# 랜덤 순열의 직렬 합성과 병렬 합성 사이의 트래이드오프에 관한 연구

정회원 이 언 경*

# On the Trade-off Between Composition and XOR of Random Permutations

Eon-kyung Lee* ***Regular Member***

요 약

직렬 합성(composition)과 병렬 합성(XOR)은 암호 스킴의 안전성을 높이기 위해 널리 사용되고 있는 방법이다. 랜덤 순열을 직렬 합성하는 회수가 많아질수록 보다 안전한 랜덤 순열이 되고, 병렬 합성하는 회수가 많아질수록 보다 안전한 랜덤 함수가 된다. 이 두 가지 방법을 결합해서, 본고는 다음과 같은 일반화된 형태의 랜덤 함수를 정의한다: $SUM^s - CMP^c = (\pi_{sc} \circ \cdots \circ \pi_{(s-1)c+1}) \oplus \cdots \oplus (\pi_c \circ \cdots \circ \pi_1)$. 여기서, $\pi_1, \cdots, \pi_{sc}$는 랜덤 순열이다. 랜덤 순열의 총 개수가 고정되어 있을 때, 직렬 합성과 병렬 합성을 각각 얼마만큼 하느냐에 따라 위 함수의 안전성은 달라질 것이다.

임의의 두 암호 스킴의 안전성을 엄밀히 비교하기 위해서는 각각의 정확한 안전성 값을 대상으로 해야 한다. 그러나, 일반적으로 정확한 값이 알려진 경우는 거의 없다. 특히, 매개변수(위 함수의 경우, s, c)의 값이 작을 경우는 밀계(tight bound)가 알려져 있는 경우가 종종 있으나, 일반적인 매개변수에 대해서는 정확한 값이나 밀계가 알려진 경우가 거의 없다. 그래서, 실제 상황에서는 두 암호 스킴의 안전성 비교는, 각각의 불안전성(insecurity)의 상계(upper bound)를 비교함으로써 이루어진다. 안전성을 중요시 하는 상황에서는 더 낮은 상계를 갖는 암호 스킴을 선호하게 된다. $SUM^s - CMP^c$의 불안전성은 기존의 여러 결과들을 조합해서 계산할 수 있다. 따라서, 특정 $(s_1, c_1), (s_2, c_2)$에 대한 두 함수의 안전성은 각각의 불안전성의 상계값을 계산함으로써 비교될 수 있다. 본고는 일반적인 $(s, c)$에 대한 $SUM^s - CMP^c$의 불안전성의 상계값의 변화를 알아보고자 한다. 그리고, 보다 낮은 상계값을 얻기 위한 직렬/병렬 합성의 최적의 개수가 무엇인지 조사한다.

**Key Words** : random function, random permutation, composition, XOR, decorrelation theory

ABSTRACT

Both composition and XOR are operations widely used to enhance security of cryptographic schemes. The more number of random permutations we compose (resp. XOR), the more secure random permutation (resp. random function) we get. Combining the two methods, we consider a generalized form of random function: $SUM^s - CMP^c = (\pi_{sc} \circ \cdots \circ \pi_{(s-1)c+1}) \oplus \cdots \oplus (\pi_c \circ \cdots \circ \pi_1)$ where $\pi_1, \cdots, \pi_{sc}$ are random permutations. Given a fixed number of random permutations, there seems to be a trade-off between composition and XOR for security of $SUM^s - CMP^c$. We analyze this trade-off based on some upper bound of insecurity of $SUM^s - CMP^c$, and investigate what the optimal number of each operation is, in order to lower the upper bound.

※ 이 논문은 2005년 정부의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임 (KRF-2005-R04-2004-000-10039-0)
* 세종대학교 응용수학과 (eonkyung@sejong.ac.kr)
논문번호 : #kics2005-10-424, 접수일자 : 2005년 10월 24일, 최종논문접수일자 : 2006년 2월 20일

## Ⅰ. Introduction

Composition and XOR operations are important tools in cryptography to enhance security. They are used either individually or together in various forms.

Since composing random functions usually weakens security, we will deal with composing random permutations. Composition of random permutations has been studied mainly related to block ciphers. One way to measure the security of a block cipher is to do its security as a random permutation. Some of the results show that composition of random permutations produces a more secure random permutation. Especially, Vaudenay[5] did by proposing the decorrelation theory. The theory has been a useful tool to measure or compare securities of block ciphers against other attacks as well as against chosen plaintext attack.

A basic form of XOR-ing random functions (resp. permutations) is $f_1(x)\oplus\cdots\oplus f_s(x)$ for independent random functions (resp. permutations) $f_1,\cdots,f_s$. This results in a random function regardless of whether its constituents are random functions or permutations. For the XOR of independent random functions, the security has not been precisely analyzed, however, it does not seem to amplify security. Myers[4] proposed its variant and proved that it amplifies security. More precisely, if $r_1,\cdots,r_s$ are independent uniform random bit strings and $f_1,\cdots,f_s$ are independent random functions, then $f_1(x\oplus r_1)\oplus\cdots\oplus f_s(x\oplus r_s)$ is a random function stronger than each component random function. As a way to build a secure random function from random permutations, Lucks[1] considered XOR-ing independent random permutations, and analyzed the security.

The more number of random permutations we compose (resp. XOR), the more secure random permutation (resp. function) we get. Considering that a random permutation itself can be used as a random function, an immediate question can be, 'Which method produces a more secure random function?' Since random permutations do not resist birthday attack, if one has to select only one method, they will probably prefer XOR. Thus, a next question can be, 'Is it more useful to combine the two methods?' This question was initially asked in view of security, however, there is another aspect: without parallel computation, using composition makes the resultant random function more efficient. There seems to be a trade-off between the two operations. Given a fixed number of random permutations, an increase in the number of compositions means XOR-ing a *smaller* number of random permutations that are *more secure* than the original ones.

Our goal is to provide as clear (and quantitative) as possible answers to the above questions by analyzing the previous results. To do so, we first define a random function

$$SUM^s - CMP^c = (\pi_{sc}\circ\cdots\circ\pi_{(s-1)c+1})\oplus \cdots\oplus(\pi_c\circ\cdots\circ\pi_1),$$

where $sc=m$ and $\pi_1,\cdots,\pi_m$ are random permutations on $\{0,1\}^n$. Note that the latest results on the composition and XOR of random permutations are Vaudenay's in 1998[5] and Luck's in 2000[1], respectively. Considering that no better result has appeared in both areas at least for the last five years, we based on their results upper bound the insecurity of $SUM^s-CMP^c$ in terms of decorrelation theory.

For a random function, its decorrelation bias represents the distinguishability from the uniform random function. The upper bound, denoted $UB-DecF^d(SUM^s-CMP^c)$, on the decorrelation bias of $SUM^s-CMP^c$ is determined by the function parameters $n$, $s$, $c$ the security of $\pi_i$, and the adversary resource $d$.

Let $f$ and $g$ be random functions such that $UB-DecF^d(f) < UB-DecF^d(g)$. Such an inequality has played an important role in many cases of comparing their securities or selecting one of them, although it does not guarantee that $f$ is more secure than $g$. For instance, Moriai and Vaudenay[3] made use of those upper bounds in order to compare several types of block ciphers. They compared the securities by the computational cost of each scheme necessary for a specific level of security, more ex-

actly, for the upper bound to be less than some value.

In this work, we find the relation between $s$ and $c$ on $UB-DecF^d(SUM^s-CMP^c)$ according to the general behavior of $n$, $d$, $m$, and the security of $\pi_i$.

## Ⅱ. Preliminaries

Let $\mathbb{R}$ be the set of all real numbers, and $\mathbb{CN}$ the set of all composite, positive integers. Let $I_n = \{0,1\}^n$ be the set of all $n$-bit strings. For reals $a<b$, let $[a,b] = \{x \in \mathbb{R} : a \le x \le b\}$, $(a,b) = \{x \in \mathbb{R} : a < x < b\}$, $[a,b) = \{x \in \mathbb{R} : a \le x < b\}$, and $(a,b] = \{x \in \mathbb{R} : a < x \le b\}$. For a sequence of random variables, i.i.d. is the abbreviation for "independent and identically distributed".

**Definition 1.** A continuous function $h : [a,b] \to \mathbb{R}$ is called *convex* if for any distinct points $x_1$ and $x_2$ in [a, b] and for any $\lambda \in (0,1)$,

$$h(\lambda x_1 + (1-\lambda)x_2) \le \lambda h(x_1) + (1-\lambda)h(x_2).$$

If the inequality is strict for all $x_1, x_2$, and $\lambda$, then $f$ is called *strictly convex*.

**Definition 2.** A *random function* $f$ from $I_n$ to $I_m$ is a random variable which takes as values functions from $I_n$ to $I_m$. If $f$ takes only permutations with $m=n$, it is called a *random permutation* on $I_n$.

**Definition 3.** If a random function (resp. random permutation) has the uniform distribution over all functions from $I_n$ to $I_m$ (resp. over all permutations on $I_n$), it is called the *uniform random function (URF)* (resp. *uniform random permutation (URP)*) and denoted by $URF_{n\to m}$ (resp. $URP_n$). $URF_n$ means $URF_{n\to n}$.

For a security model for random functions, we consider an adaptive version of the Luby-Rackoff model, in which the number of adversary's queries to an oracle is bounded.

**Definition 4.** Given two random functions $f$ and $f'$, let an oracle $O$ simulate either $f$ or $f'$. A *q-limited distinguisher* for $f$ and $f'$ is a computationally unbounded Turing machine $D^O$ that outputs either 0 or 1 after a limited number $q$ of interactive queries to $O$.

The distinguishability between two random functions, $f$ and $f'$, is quantified by the *maximal advantage* over all $q$-limited distinguishers $D$ as:

$$Adv^q(f,f') = \max_D |Pr[D^f = 1] - Pr[D^{f'} = 1]|.$$

The decorrelation theory is a set of mathematical tools which aims at studying and defining the security of block ciphers in the Luby-Rackoff model.

**Definition 5.** Given a random function $f$ from $I_n$ to $I_m$ and an integer $d$, we define the *d-wise distribution matrix* $[f]^d$ of $f$ as an $I_n^d \times I_m^d$-matrix where the $(x, y)$-entry of $[f]^d$corresponding to the multi-points $x = (x_1, \cdots, x_d) \in I_n^d$ and $y = (y_1, \cdots, y_d) \in I_m^d$ is defined as

$$[f]^d_{x,y} = Pr[f(x_i) = y_i \text{ for all } 1 \le i \le d].$$

**Definition 6.** Given two random functions $f$ and $f'$ from $I_n$ to $I_m$, a positive integer $d$, and a matrix norm $\|\cdot\|$ over the $I_n^d \times I_m^d$-matrix space $\mathbb{R}^{I_n^d \times I_m^d}$, we define the *d-wise decorrelation* $\|\cdot\|$*-distance* between $f$ and $f'$ as

$$Dec^d_{\|\cdot\|}(f,f') = \|[f]^d - [f']^d\|.$$

Here, if $f'$ is the URF, the distance is denoted by $DecF^d_{\|\cdot\|}(f)$ and called *d-wise decorrelation bias of function f*. Similarly, if $f$ is a random permutation and $f'$ is the URP, the distance is denoted by $DecP^d_{\|\cdot\|}(f)$ and called *d-wise decorrelation bias of permutation f*.

By defining a new matrix norm $\|\cdot\|_a$, Vaudeny linked the decorrelation distance between two random functions to the maximal advantage of distinguisher.

**Lemma 1**[6]. For any random functions $f$ and $f'$, and any positive integer $d$, we have

$$Dec^d_{\|\cdot\|_a}(f,f') = 2 \cdot Adv^d(f,f').$$

From now on, this paper will use only $\|\cdot\|_a$ as a matrix norm associated with decorrelation distance. Thus, we will simply write $Dec^d$, $DecF^d$, and $DecP^d$ instead of $Dec^d_{\|\cdot\|_a}$, $DecF^d_{\|\cdot\|_a}$, and $DecP^d_{\|\cdot\|_a}$, respectively.

## Ⅲ. A Random Function and Its Security

When combining XOR and composition operations, we can think in two ways: XOR-ing after composing and composing after XOR-ing. Both ways produce random functions from random permutations, but we will consider only the former because composing random functions usually diminishes security.

**Definition 7.** For positive integers $c$ and $s$, and for i.i.d. random permutations $\pi_1, \cdots, \pi_{sc}$ on $I_n$, we define a random function $SUM^s - CMP^c$ from $I_n$ to $I_n$ as follows:

$$SUM^s - CMP^c = (\pi_{sc} \circ \cdots \circ \pi_{(s-1)c+1}) \oplus \cdots \oplus (\pi_c \circ \cdots \circ \pi_1).$$

In order to get the security of $SUM^s - CMP^c$, we use the following results.

**Lemma 2**[5]. For any i.i.d. random permutations $\pi_1, \cdots, \pi_c$,

$$DecP^d(\pi_c \circ \cdots \circ \pi_1) \le DecP^d(\pi_1)^c.$$

**Lemma 3**[1]. Let $\pi_1^*, \cdots, \pi_s^*$ be independent URPs on $I_n$. For any $d \le 2^{n-1}/s$,

$$DecF^d(\pi_s^* \oplus \cdots \oplus \pi_1^*) \le \frac{2}{2^{s(n-1)}} \sum_{0 \le i < d} i^s.$$

For feasible handling, we use a simpler form of alternative to the above boundary formula:

$$\frac{2}{2^{s(n-1)}} \sum_{0 \le i < d} i^s \le \frac{2d^{s+1}}{(s+1)2^{s(n-1)}}.$$

Note that the above two terms behave almost in the same way.

In order to get the security of $\pi_s \oplus \cdots \oplus \pi_1$ when not every $\pi_i$ is uniform, the following lemma is used.

**Lemma 4.** For independent random permutations $\pi_1, \cdots, \pi_s, \pi_1', \cdots, \pi_s'$ on $I_n$,

$$Dec^d(\pi_s \oplus \cdots \oplus \pi_1, \pi_s' \oplus \cdots \oplus \pi_1') \le \sum_{i=1}^{s} Dec^d(\pi_i, \pi_i').$$

From the above three lemmas, we have the following result.

**Theorem 5.** For positive integers $c$ and $s$, let $\pi_1, \cdots, \pi_{sc}$ be i.i.d. random permutations on $I_n$. Using them, define $SUM^s - CMP^c$ as in Definition 7. Then, for any $d \le 2^{n-1}/s$,

$$DecF^d(SUM^s - CMP^c) \le s(DecP^d(\pi_1))^c + \frac{2d}{s+1}\left(\frac{d}{2^{n-1}}\right)^s.$$

## Ⅳ. Trade-off between Composition and XOR

Let $m=sc$ be the number of i.i.d. random permutations, and $\epsilon$ the $d$-wise decorrelation bias of them. Let $UB - DecF^d(SUM^s - CMP^c)$ denote the upper bound of $DecF^d(SUM^s - CMP^c)$ in Theorem 5. Then, it is expressed as $UB - DecF^d(SUM^s - CMP^c) = \frac{m}{c}\epsilon^c + \frac{2cd}{c+m} \cdot \left(\frac{d}{2^{n-1}}\right)^{\frac{m}{c}}$. Define a function $f$ as

$$f(n,d,\epsilon,m,x) = \frac{m}{x}\epsilon^x + \frac{2dx}{x+m}\left(\frac{d}{2^{n-1}}\right)^{\frac{m}{x}}.$$

The following lemma shows that $f$ has a nice property in some domain of interest.

**Lemma 6.** For any $n \in [4, \infty)$, $d \in [1, 2^{n-4}]$,

$\epsilon \in (0,1)$, and $m \in [1,\infty)$, $f(n,d,\epsilon,m,x)$ is a strictly convex function in $x \in [1,m]$.

### 4.1 Composition versus XOR

First, we compare $SUM^1 - CMP^m$ and $SUM^m - CMP^1$. By a straightforward calculation, we obtain $\epsilon_0 \in (0,1]$, determined by $(n, d, m)$, such that $DecP^d(\pi_1) < \epsilon_0$ if and only if $UB - DecF^d(SUM^m - CMP^1) < UB - DecF^d(SUM^1 - CMP^m)$.

**Theorem 7.** Define $\alpha_0$ and $\epsilon_0$ as $\alpha_0(n,d,m) = \frac{d^2}{2^{n-1}} - \frac{2d}{m+1}(\frac{d}{2^{n-1}})^m$; $\epsilon_0(n,d,m) = 1$ if $\alpha_0(n,d,m) \geq m-1$, and the root of $x^m - mx + \alpha_0(n,d,m) = 0$ in $(0,1)$ otherwise. For any $n \in [4,\infty)$, $d \in [1,2^{n-4}]$, and $m \in [1,n]$,

$$f(n,d,\epsilon,m,1) < f(n,d,\epsilon,m,m) \quad \text{for all } 0 < \epsilon < \epsilon_0(n,d,m);$$
$$f(n,d,\epsilon,m,1) = f(n,d,\epsilon,m,m) \quad \text{for } \epsilon = \epsilon_0(n,d,m);$$
$$f(n,d,\epsilon,m,1) > f(n,d,\epsilon,m,m) \quad \text{for all } \epsilon_0(n,d,m) < \epsilon < 1.$$

When $m$ is a prime number, the only comparable forms are $SUM^1 - CMP^m$ and $SUM^m - CMP^1$. From now on, we focus on composite numbers $m$. For any of such $m$'s, there exists at least one factor (other than the trivial factor 1) of $m$ not greater than $\sqrt{m}$. The following theorem shows that, in most cases of $(n, d, m)$, $UB - DecF^d(SUM^s - CMP^c) < UB - DecF^d(SUM^m - CMP^1)$ for all factors $c$ of $m$ such that $1 < c \leq \sqrt{m}$ regardless of the value of $DecP^d(\pi_1)$.

**Theorem 8.** For any $n \in [16,\infty)$, $d \in [1,2^{n/2}]$ (resp. $d \in (2^{n/2}, 2^{3n/4}]$), $\epsilon \in [2^{-n}, 2^{-2}]$, and $m \in [9,n]$ (resp. $m \in [49,n]$), $f(n,d,\epsilon,m,x) < f(n,d,\epsilon,m,1)$ for all $x \in (1,\sqrt{m}]$.

*Proof.* For $n \in [16,\infty)$, $d \in [1,2^{n-4}]$, $\epsilon \in [2^{-n}, 2^{-2}]$, and $m \in [4,n]$, define $g(n,d,\epsilon,m) = f(n,d,\epsilon,m,1) - f(n,d,\epsilon,m,\sqrt{m})$. We will show that $g(n,d,\epsilon,m) > 0$ for all $n \in [16,\infty)$, $d \in [1,2^{n/2}]$ (resp. $d \in (2^{n/2}, 2^{3n/4}]$), $\epsilon \in [2^{-n}, 2^{-2}]$, and $m \in [9,n]$ (resp. $m \in [49,n]$).

Then, to combine this with Lemma 6 gives the desired results. By a straightforward calculation, we have the slopes of $g$ for each $d$, $\epsilon$, $m$ as follows. For all $n \in [16,\infty)$, $d \in [1,2^{n-4}]$, $\epsilon \in [2^{-n}, 2^{-2}]$, and $m \in [4,n]$, (a) $\frac{\partial g}{\partial d}(n,d,\epsilon,m) < 0$; (b) $\frac{\partial g}{\partial \epsilon}(n,d,\epsilon,m) > 0$; (c) $\frac{\partial g}{\partial m}(n,d,\epsilon,m) > 0$.

Since $1 < 2^{n/2} < 2^{3n/4} \leq 2^{n-4}$ for all $n \geq 16$, the theorem statement is obtained by the following due to (a), (b), and (c): $g(n,2^{n/2},2^{-n},9) > 0$ and $g(n,2^{3n/4},2^{-n},49) > 0$ for all $n \geq 16$. ■

### 4.2 Optimal Number of Compositions

Theorem 8 says that composition helps XOR to lower $UB - DecF^d(SUM^s - CMP^c)$ either when $1 \leq d \leq 2^{n/2}$ and $9 \leq m \leq n$ or when $2^{n/2} < d \leq 2^{3n/4}$ and $49 \leq m \leq n$. Then, what is the number of compositions to obtain the minimum value for these $(d, m)$'s? This number occurs at every factor of $m$ between the second smallest one and $m$. This section analyzes concretely how the optimal number of compositions is related to $(n,d,\epsilon,m)$, from which the optimal number of XORs follows immediately due to $m=sc$.

Notation. For a positive integer $m$, let $FAC(m)$ denote the set of all factors of $m$, and let $m_2$ be the second smallest factor of $m$, $m_\ell$ the greatest factor of $m$ not greater than $\sqrt{m}$, and $m_u$ the smallest factor of $m$ not less than $\sqrt{m}$. Namely, $m_2 = \min(1, m] \cap FAC(m)$, $m_\ell = \max[1, \sqrt{m}] \cap FAC(m)$, and $m_u = \min[\sqrt{m}, m] \cap FAC(m)$.

Given $(n,d,\epsilon,m)$, the minimum of $f(n,d,\epsilon,m,x)$ occurs at a single point $x \in [1,m]$ because of Lemma 6, but can occur at more than one point $x \in FAC(m)$. Thus, we define $C_0$ as the set of all factors of $m$ where $f$ has the minimum: $C_0 = \{c_0 \in FAC(m) : f(n,d,\epsilon,m,c_0) \leq f(n,d,\epsilon,m,c) \text{ for all } c \in FAC(m)\}$. $C_0$ is determined by $(n,d,\epsilon,m)$, and the number of its elements is either one or two. The following theorem finds the

value, $\epsilon_1$, of $DecP^d(\pi_1)$ which is used to determine whether $C_0$ is inside $[1, m_u]$ or inside $[m_\ell, m]$.

**Theorem 9.** Define $\alpha_1$ and $\epsilon_1$ as $\alpha_1(n,d,m) = \frac{2d}{(\sqrt{m}+1)^2}(\frac{d}{2^{n-1}})^{\sqrt{m}}(1+(\sqrt{m}+1)\ln\frac{2^{n-1}}{d})$; $\epsilon_1(n,d,m) = 1$ if $\alpha_1(n,d,m) \geq 1$, and the root of $x^{\sqrt{m}}(\sqrt{m}\ln x - 1) + \alpha_1(n,d,m) = 0$ in $(0,1)$ otherwise. For any $n \in [4,\infty)$, $d \in [1, 2^{n-4}]$, and $m \in [1,n] \cap \mathbb{CN}$, we have $C_0 \subset [1, m_u]$ for all $0 < \epsilon \leq \epsilon_1(n,d,m)$ and $C_0 \subset [m_\ell, m]$ for all $\epsilon_1(n,d,m) < \epsilon < 1$.

*Proof.* Fix $n \in [4,\infty)$, $d \in [1, 2^{n-4}]$, and $m \in [1,n] \cap \mathbb{CN}$. Put $\alpha_1 = \alpha_1(n,d,m)$ and $\epsilon_1 = \epsilon_1(n,d,m)$. Define a function $k(\epsilon)$ on (0,1) as $k(\epsilon) = \frac{\partial f}{\partial x}(n,d,\epsilon,m,\sqrt{m}) = \epsilon^{\sqrt{m}}(\sqrt{m}\ln\epsilon - 1) + \alpha_1$. Then, $k(\epsilon)$ is decreasing on (0,1), $\lim_{\epsilon\to 0} k(\epsilon) = \alpha_1 > 0$, and $\lim_{\epsilon\to 1} k(\epsilon) = \alpha_1 - 1$. If $\alpha_1 - 1 \geq 0$, then $k(\epsilon) > 0$ for all $\epsilon \in (0,1) = (0,\epsilon_1)$. Otherwise, there exists uniquely $\epsilon'_1 \in (0,1)$ such that

$$k(\epsilon) > 0 \text{ for all } \epsilon \in (0,\epsilon'_1) = (0,\epsilon_1);$$
$$k(\epsilon) = 0 \text{ for all } \epsilon = \epsilon'_1 = \epsilon_1;$$
$$k(\epsilon) < 0 \text{ for all } \epsilon \in (\epsilon'_1, 1) = (\epsilon_1, 1).$$

Therefore, $\frac{\partial f}{\partial x}(n,d,\epsilon,m,\sqrt{m}) \geq 0$ if and only if $0 < \epsilon \leq \epsilon_1$.

*Case 1.* $0 < \epsilon \leq \epsilon_1$: Since $\frac{\partial f}{\partial x}(n,d,\epsilon,m,\sqrt{m}) \geq 0$, we have $f(n,d,\epsilon,m,m_u) < f(n,d,\epsilon,m,c)$ for all $c \in (m_u, m] \cap FAC(m)$, and hence $C_0 \subset [1, m_u]$.

*Case 2.* $\epsilon_1 < \epsilon < 1$: Since $\frac{\partial f}{\partial x}(n,d,\epsilon,m,\sqrt{m}) < 0$, we have $f(n,d,\epsilon,m,m_\ell) < f(n,d,\epsilon,m,c)$ for all $c \in [1,m_\ell) \cap FAC(m)$, and hence $C_0 \subset [m_\ell, m]$. ■

Note that $C_0$ is composed of a single element, say $c_0$, in general. Recall $f(n,d,\epsilon,m,x) = \frac{m}{x}\epsilon^x + \frac{2dx}{x+m}(\frac{d}{2^{n-1}})^{\frac{m}{x}}$. Let $x_0 \in [1,m]$ be the point where $f(n,d,\epsilon,m,\cdot)$ has the minimum. The value of $f(n,d,\epsilon,m,x)$ at $x \in [1,x_0]$ (resp. at $x \in [x_0,m]$) depends mainly on $\frac{m}{x}\epsilon^x$ (resp. on $\frac{2dx}{x+m}(\frac{d}{2^{n-1}})^{\frac{m}{x}}$). At every $x \in [1,m]$, $\frac{m}{x}\epsilon^x$ is an increasing function in $(\epsilon, m)$, and $\frac{2dx}{x+m}(\frac{d}{2^{n-1}})^{\frac{m}{x}}$ is an increasing function in $d$ and a decreasing function in $m$. Therefore, $c_0$ tends to increase as $d$ decreases, and $m$ and $\epsilon$ increase, and to decrease as $d$ increases, and $m$ and $\epsilon$ decrease.

Consider the case where we are given random permutations. In this case, $\epsilon = DecP^d(\pi_1)$ is an increasing function in $d$. This implies that $c_0$ should be observed when both $d$ and $\epsilon$ move in the same direction. Therefore, we combine Theorem 8 with Theorem 9 for relatively small $d$'s and $\epsilon$'s in the following corollary: in most cases, the optimal number of compositions occurs between $m_2$ and $m_u$ for $\pi_i$'s with $DecP^d(\pi_i) \leq \epsilon_2$. Here, $\epsilon_2$ is easier to compute than $\epsilon_1$.

**Corollary 10.** Define $\epsilon_2(n,d,m) = \min\{2^{-2}, \frac{d}{2^{n-1}}(\frac{2d(1+(\sqrt{m}+1)\ln\frac{2^{n-1}}{d})}{(n\sqrt{m}+1)(\sqrt{m}+1)^2})^{\frac{1}{\sqrt{m}}}\}$. For any $n \in [16,\infty)$, $d \in [2, 2^{n/2}]$ (resp. $d \in (2^{n/2}, 2^{3n/4}]$), $m \in [9,n] \cap \mathbb{CN}$ (resp. $m \in [49,n] \cap \mathbb{CN}$), and $\epsilon \in [2^{-n}, \epsilon_2(n,d,m)]$, we have $C_0 \subset [m_2, m_u]$.

*Proof.* Recall $\alpha_1$ and $\epsilon_1$ from Theorem 9. We will show that $2^{-n} \leq \epsilon_2(n,d,m) \leq \epsilon_1(n,d,m)$ holds for all *(n, d, m)*. Then, the conclusion follows from Theorems 8 and 9.

Fix $n \in [16,\infty)$ and $m \in [9,n]$. Note that $\frac{d}{2^{n-1}}(\frac{2d(1+(\sqrt{m}+1)\ln\frac{2^{n-1}}{d})}{(n\sqrt{m}+1)(\sqrt{m}+1)^2})^{\frac{1}{\sqrt{m}}} \geq 2^{-n}$ for all $d \in [2, 2^{3n/4}]$, which is implied by $2^{2\sqrt{m}+2}\sqrt{m} + (\sqrt{m}+1)^2 \leq (\sqrt{m}+1)(2^{2\sqrt{m}+1} -$

$\sqrt{m}(\sqrt{m}+1))m$. Therefore, we have $\epsilon_2(n,d,m) \geq 2^{-n}$ for all $d \in [2, 2^{3n/4}]$.

Fix $d \in [2, 2^{3n/4}]$. Put $\alpha_1 = \alpha_1(n,d,m)$, $\epsilon_1 = \epsilon_1(n,d,m)$, and $\epsilon_2 = \epsilon_2(n,d,m)$. Choose $\epsilon \in [2^{-n}, \epsilon_2]$. We will show that $\epsilon \in [2^{-n}, \epsilon_1]$. Since $\epsilon \geq 2^{-n}$, we have $\frac{\partial f}{\partial x}(n,d,\epsilon,m,\sqrt{m}) = -\epsilon^{\sqrt{m}}(1-\sqrt{m}\ln\epsilon)+\alpha_1 \geq -(n\sqrt{m}+1)\epsilon^{\sqrt{m}}+\alpha_1$. Note that $-(n\sqrt{m}+1)x^{\sqrt{m}}+\alpha_1 \geq 0$ for all $0 \leq x \leq (\frac{\alpha_1}{n\sqrt{m}+1})^{\frac{1}{\sqrt{m}}}$, and that $2^{-n} \leq \epsilon \leq \epsilon_2 = \min\{2^{-2}, (\frac{\alpha_1}{n\sqrt{m}+1})^{\frac{1}{\sqrt{m}}}\}$. Hence, $\frac{\partial f}{\partial x}(n,d,\epsilon,m,\sqrt{m}) \geq 0$. Since $\frac{\partial f}{\partial x}(n,d,w,m,\sqrt{m})$ is a decreasing function in $\omega \in (0,1)$, $\epsilon \in [2^{-n}, \epsilon_1]$ holds by the definition of $\epsilon_1$, from which $\epsilon_2 \leq \epsilon_1$ follows. ■

## V. Concluding Remarks

The exact securities of composition and XOR of random permutations (i.e. $DecF^d(SUM^1 - CMP^m)$, $DecF^d(SUM^m - CMP^1)$ in this paper) are not known yet. Thus, their upper bounds (i.e. $UB-DecF^d(SUM^1 - CMP^m)$, $UB-DecF^d(SUM^m - CMP^1)$) can be used as an important data when we select one of the two methods. This paper has analyzed the trade-off between $s$ and $c$ in $UB-DecF^d(SUM^s - CMP^c)$, where $sc=m$ and $SUM^s - CMP^c = (\pi_{sc} \circ \cdots \circ \pi_{(s-1)c+1}) \oplus \cdots \oplus (\pi_c \circ \cdots \circ \pi_1)$ for i.i.d. random permutations $\pi_i$'s: for most $(n, d, m)$'s under consideration, we have shown the following.

(a) $UB-DecF^d(SUM^m - CMP^1) < UB-DecF^d(SUM^1 - CMP^m)$ if and only if $DecP^d DecP^d(\pi_1) < \epsilon_0$.

(b) Regardless of the security of $\pi_i$, $UB-DecF^d(SUM^s - CMP^c) < UB-DecF^d(SUM^m - CMP^1)$ for every $c$ satisfying $1 < c \leq \sqrt{m}$.

(c) If $DecP^d(\pi_1) < \epsilon_2$, the optimal $c$ is tightly bounded above by $m_u$ (the smallest factor of $m$ not less than $\sqrt{m}$) and below by $m_2$ (the second smallest factor of $m$).

## REFERENCES


[1] S. Lucks, "The Sum of PRPs is a Secure PRF", *EUROCRYPT '00*, LNCS 1807, pp. 470-484, 2000.

[2] U. Maurer, J. Massey, "Cascade Ciphers: The Importance of Being First", *J. Cryptology*, 6, pp. 55-61, 1993.

[3] S. Moriai, S. Vaudenay, "On the Pseudorandomness of Top-Level Schemes of Block Ciphers", *ASIACRYPT '00*, LNCS 1976, pp. 289-302, 2000.

[4] S. Myers, "Efficient Amplification of the Security of Weak Pseudo-Random Function Generators", *J. Cryptology*, 16, pp. 1-24, 2003.

[5] S. Vaudenay, "Provable Security for Block Ciphers by Decorrelation", *STACS '98*, LNCS 1373, pp. 249-275, 1998.

[6] S. Vaudenay, "Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness", *SAC '99*, LNCS 1758, pp. 49-61, 2000.

[7] S. Vaudenay, "Decorrelation: A Theory for Block Cipher Security", *J. Cryptology*, 16, pp. 249-286, 2003.



**이 언 경** (Eon-kyung Lee) 정회원

1988년 3월~1992년 2월 KAIST 수학과 학사

1992년 3월~1994년 2월 KAIST 수학과 석사

1994년 2월~1997년 8월 ETRI 연구원

1997년 9월~2001년 8월 KAIST 수학과 박사

2001년 10월~2003년 8월 KISA 선임연구원

2003년 9월~현재 세종대학교 응용수학과 조교수

<관심분야> 암호론, 땋임군론