情報保護學會論文誌
第17卷 第3號, 2007. 6

랜덤 오라클 모델에서의 Even-Mansour Cipher에 대한 키 길이 최적화 방법*

성 재 철
서울시립대학교 수학과

On the Optimal Key Size of the Even-Mansour Cipher in the Random Function Oracle Model

Jaechul Sung
Department of Mathematics, University of Seoul

요 약

본 논문은 Even-Mansour 암호에 대해 안전성 약화 없이 키 사이즈를 줄이는 방법에 대해 다룬다. Even과 Mansour는 랜덤 순열 모델에서 랜덤 순열 P와 두 개의 키를 이용하여 평문 M을 암호화하는 기법($C = k_2 \oplus P(M \oplus k_1)$)을 제안하였다.[3] ASIACRYPT 2004에서 Gentry와 Ramzen은 4 라운드의 Feistel 구조를 이용하여 Even-Mansour 모델의 랜덤 순열을 랜덤 함수로 대치한 새로운 모델을 제안하고 안전성을 증명하였다. 본 논문에서는 Gentry-Ramzen 모델에 필요한 키 사이를 반으로 줄이는 방법을 살펴보고 제안한 방법에 대한 안전성을 랜덤 함수 모델에서 증명한다.

ABSTRACT

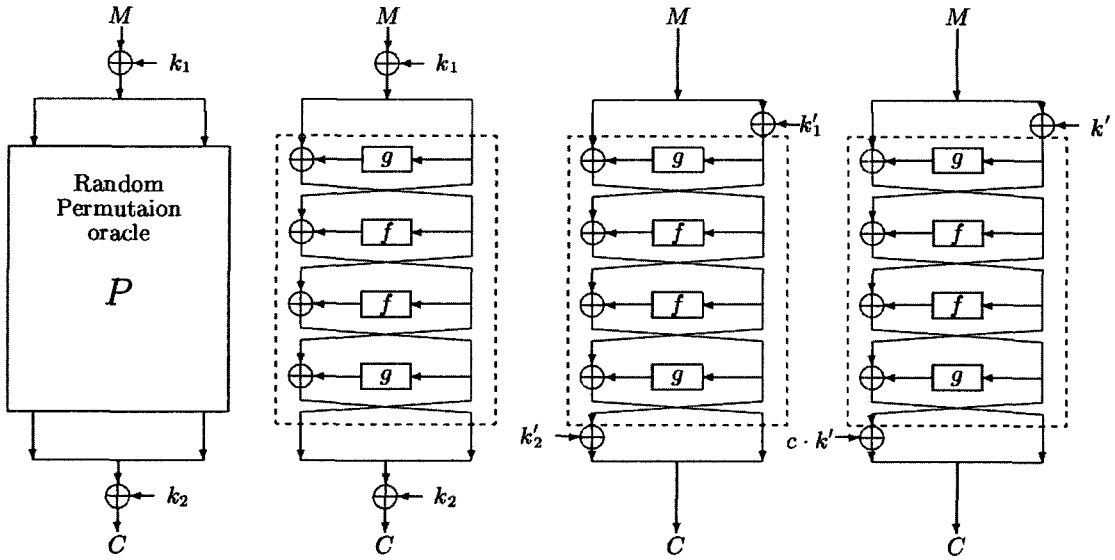
We describe the problem of reducing the key material in the Even-Mansour cipher without security degradation. Even and Mansour proposed a block cipher based on XORing secret key material just prior to and after applying random oracle permutation P such that $C = k_2 \oplus P(M \oplus k_1)$.[3] Recently, Gentry and Ramzan showed that this scheme in the random permutation oracle can be replaced by the four-round Feistel network construction in the random function oracle and also proved that their scheme is super-pseudorandom.[4] In this paper we reduce the key size from 2n to n, which is the optimal key size of Even-Mansour cipher in the random function oracle model and also give almost the same level of security.

Keywords : *Block Cipher, Provable Security, Feistel Scheme, Even-Mansour Cipher, Pseudorandomness, Random Oracle.*

I. Introduction

Luby and Rackoff[7] suggested the formal definitions for pseudorandomness and super-pseudorandomness(*or* strong-pseudorandomness) and also showed a method for constructing a pseudorandom permutation from a pseudorandom function. A block cipher is called pseudorandom if it is indistinguishable from a random permutationunder the chosen plaintext attack model. Furthermore, it is called super-pseudoran-

접수일: 2006년 12월 5일; 채택일: 2007년 2월 22일
* 이 논문은 2006년도 서울시립대학교 학술연구조성비에 의하여 연구되었음
† 주저자, ‡ 교신저자 : jcsung@uos.ac.kr



(a) Even-Mansour (b) Gentry-Ramzen I (c) Gentry-Ramzan II (d) Our construction

[Fig. 1] Even-Mansour cipher and its variants

dom if it is indistinguishable from a random permutation under the chosen plaintext and ciphertext attack model.

Even and Mansour[3] proposed a block cipher based on XORing secret key material just prior to and after applying random oracle permutation[2] P such that $C = k_2 \oplus P(M \oplus k_1)$ where M is the plaintext, C is the ciphertext, and k_1, k_2 are the key materials. In the random permutation oracle model, the permutation P and its inverse are computable by all parties. The only secrete components are k_1 and k_2, which is XORed at the beginning and the end. Except this key XORing operation, every component is publicly accessible in this model.

In 2004, Gentry and Ramzan gave the formal proof of the Even-Mansour cipher recently.[4] This implies that the scheme is super-pseudorandom. Furthermore, they replaced the random permutation oracle by random function oracle, which does not need bijective anymore. They just replaced the random permutation P by the four-round Feistel permutation $\psi(g,f,f,g)$, where ψ is the Feistel permutation and f, g are random function oracles. We will define the formal definitions of these in the following section.

The advantage of the construction of Gentry and Ramzan over that of Even-Mansour is that the random permutation oracle is replaced by the random function model. Also they permit to access publicly not only to an inner four-round Feistel permutation oracle $\psi(g,f,f,g)$ but also two random oracles f and g. This model comes from the security notion of [12], which is called the round security.

However, in two generic models, it is required that the size of key materials is $4n$-bit, where the message space is $\{0,1\}^{2n}$ (See the Fig. 1). We do concentrate to reduce the key size in the random oracle model without security degradation. It means that we hope to prove super-pseudorandomness for the constructions of Even-Mansour and Gentry-Ramzan without security degradation just by reducing the key size. Actually, the full paper of [4], they proposed some methods to reduce the key materials as the followings;

(i) In (b) of Fig.1, set $k_1 = k_2$.

(ii) Two key materials are XORed into the right

half of the input to the Feistel Networks ((c) of Fig. 1).

(iii) By replacing XOR operation by '+' and '−' group operations in the (c) of Fig. 1, set $k'_1 = k'_2$.

The first two methods already needs *2n*-bit key material. The third method which uses the technique in Patel et al.[11] seems to have an optimal key size. However, it needs other group operations rather than an XOR operation, which is not a bit-wise operation. Can we reduce the key size up to n-bit without replacing XOR operation by others?

In this paper we give an answer of it. We reduce the key size only by replacing k'_2 by $c \cdot k'_1$, where $c(\neq \{0,1\})$ is publicly known constant (such as 2 or 3) and $\cdot$ means the multiplication in $GF(2^n)$. We know that the multiplication with the fixed constant can be calculated by some shift operations and XOR operations. In the random function oracle model of the Even-Mansour cipher, our construction has optimal key size. Also we give an explicit proof of ours using the almost same way in [4].

RELATED WORKS : Luby and Rackoff provided a construction of (super) pseudorandom permutations from pseudorandom functions with the three(four)-round Feistel construction. Later there were many approaches to obtain more efficient construction of super-pseudorandom permutation than that of Luby and Rackoff.[5,6,8,9,10,11,12] Among them, Naor and Reingold gave an formal model of this construction and simplified its proof of security. In 2000, Ramzan and Reyzin introduced a new security model, which is called round security. In this model, the adversary can access to some of internal round primitives.

ORGANIZATIONS : In Section 2 we give some preliminary definitions and security notions. In Section 3 we survey the generic model of [4] and its proof skill. In section 4 we proved that our construction is super-pseudorandom without security degradation in comparison with that of [4] and this construction has an optimal key size in random function oracle model of the Even-Mansour cipher.

Ⅱ. Notations and Standard Definitions

For $x \in \{0,1\}^{2n}$, x^L means the left n-bit of x and x^R means the right n-bit of x. We denote all functions from $\{0,1\}^n$ to $\{0,1\}^n$ by F_n and the set of all permutations on $\{0,1\}^{2n}$ by P_{2n}. For a set S, $s \leftarrow^R S$ means the process of picking an element s from S uniformly at random. For two functions f and g, $g \circ f$ denotes the composition of f and g.

We call a function family keyed if every function in it can be specified by a key a. We denote the function given by a as f_a. For a given keyed function family, a key can be any string from $\{0,1\}^s$ where s is known as key length. For a function $f \in F_n$, we define basic Feistel permutation $\psi_f \in P_{2n}$ as $\psi_f(x^L, x^R) = (x^R, x^L \oplus f(x^R))$. Also define the r-round Feistel permutation $\psi(f_1, \cdots, f_r) = \psi_{f_r} \circ \cdots \circ \psi_{f_1}$.

Let Φ be a permutation family on $\{0,1\}^{2n}$. Then we say that Φ is *pseudorandom* if it is indistinguishable from P_{2n}, where the adversary is allowed adaptive chosen plaintext attacks. Moreover, we call that Φ is *super-pseudorandom* if it is indistinguishable from P_{2n}, where the adversary is allowed adaptive chosen plaintext and ciphertext attacks. In this paper we will only consider super-pseudorandomness. Other definitions and notations follows that of [1, 4].

In the general super-pseudorandomness attack model, the adversary have two oracles, the forward direction of the permutation and the backward direction of the permutation. The adversary A is a program for RAM(Random Access Machine) with black-box access to some number two oracles. We assume that the adversary's computational power is unlimited, but the total number of oracle calls is limited to q. After making at most q queries to the oracles, A outputs 0 or 1.

Now let us define an advantage of the adversary in the general super-pseudorandomness attack model.

〔Definition 1〕 (SPRP)

Let Φ be a permutation family on $\{0,1\}^{2n}$. For an adversary A with two-oracles, we define A's advantage as the following;

$$Adv_{\Phi}^{sprp}(A) =$$

$$\left| \Pr[\phi \leftarrow^{R} \Phi : A^{\phi,\phi^{-1}} = 1] - \Pr[p \leftarrow^{R} P_{2n} : A^{p,p^{-1}} = 1] \right|.$$

For any integer $q,t(\geq 0)$, we define $Adv_{\Phi}^{sprp}(q,t) = Adv_{\Phi}^{sprp}(A)$, as an insecurity function, where the maximum is taken over choices of adversary A such that A makes at most q oracle queries, and the running time of A, plus the time necessary to select $\phi \leftarrow^{R} \Phi$ and answer A's queries, is at most t.

The notion of round security[12] is an extension of the general definition of pseudorandomness. Let $\Phi, F^1, \cdots, F^r$ be permutation family on $\{0,1\}^{2n}$, such that for a function $\phi \in \Phi$, $\phi = f^r \circ \cdots \circ f^1$. Then $F^1, \cdots, F^r$ is called r-round decomposition for Φ. The adversary A is a program for RAM(Random Access Machine) with black-box access to some number $r+2$ oracles. In this model the adversary can access to r oracles $f^1, \cdots, f^r$ and two oracles ϕ, ϕ^{-1}.

Since we will consider the Even-Mansour cipher in the random function oracle, we do not consider $i \rightarrow j$ in〔12〕, which means being able to give inputs to round i of the forward direction of a block cipher and view outputs after round j. We simplify the definition of 〔12〕.

〔Definition 2〕 (*Round Security*)

Let Φ be a permutation family on $\{0,1\}^{2n}$ with r-round decomposition $F^1, \cdots, F^r$. For an adversary A with $(r+2)$-oracles, we define A's advantage as the following;

$$Adv_{\Phi,F^1,\cdots,F^r}^{sprp}(A) =$$

$$\left| \Pr[\phi \leftarrow^{R} \Phi : A^{\phi,\phi^{-1},f^1,\cdots,f^r} - \Pr[p \leftarrow^{R} P_{2n} : A^{p,p^{-1},f^1,\cdots,f^r} = 1] \right|.$$

For any integer $q,t(\geq 0)$, we define $Adv_{\Phi}^{sprp}(q,t)$ specifies our insecurity function analogous to Definition 1.

Ⅲ. Gentry-Ramzan's Generic Model vs. Ours

In this section we briefly consider the frame of 〔4, 12〕. We denote $\Psi_{k_1,k_2}^{f,g}$ the Gentry-Ramzan construction when the internal permutation is replaced by a four-round Feistel network with outer round g and inner round f, i.e., $\Psi_{k_1,k_2}^{f,g} = k_2 \oplus \psi(g,f,f,g)(x \oplus k_1)$ where k_1, k_2 are the key materials and f, g are modeled as random function oracles.

The main theorem of the Gentry and Ramzan in the round-security is as the following.

〔Theorem 1〕〔4〕

Let f an g be modeled as random function oracles, let k_1 and k_2 be pricked randomly and independently from $\{0,1\}^{2n}$. Let $\Psi_{k_1,k_2}^{f,g} = k_2 \oplus \psi(g,f,f,g)(x \oplus k_1)$, and R be a random element in P_{2n}. Then, for any four-oracle adversary A that makes at most q_c queries to its first two oracle queries (either Ψ, Ψ^{-1} or R, R^{-1}) and at most q_f and q_g queries to its f and g oracles respectively, it follows that :

$$\left| \Pr[A^{\Psi,\Psi^{-1},f,g} = 1] - \Pr[A^{R,R^{-1},f,g} = 1] \right|$$

$$\leq (q_c^2 + 2q_f q_c + 2q_g q_c + q_c^2 - q_c)\, 2^{-n} + \frac{q_c(q_c-1)}{2}(2^{-n+1} + 2^{-2n+1}).$$

Actually, though the theorem is true itself, we can improve the upper bound. The upper bound can be replaced by as the following ;

$$\left| \Pr[A^{\Psi,\Psi^{-1},f,g} = 1] - \Pr[A^{R,R^{-1},f,g} = 1] \right|$$

$$\leq (q_c^2 + 2q_f q_c + 2q_g q_c + q_c^2 - q_c)\, 2^{-n} + \frac{q_c(q_c-1)}{2} 2^{-2n+1}.$$

Let $x = (x^L, x^R)$ be in $\{0,1\}^{2n}$ and k' be a key in $\{0,1\}^{n}$. Let $\Psi_{k_1,k_2}^{f,g}$ be the generic Gentry-Ramzan construction. Then our modification can be defined as the following :

$$\Psi_{k'}^{f,g}(x_L x_R) = (c \cdot k' \oplus (\psi(g,f,f,g)(x^R, x^L \oplus k'))^L,$$

$$\psi(g,f,f,g)(x^R, x^L \oplus k'))^R),$$

where $c(\neq \{0,1\})$ is be an fixed known constant and $\cdot$ means the multiplication in $GF(2^n)$(See the

Fig. 1). Then we have the following main result.

〔Theorem 2〕 (*Main Result*)

Let f an g be modeled as random function oracles, let k' be picked randomly and independently from $\{0,1\}^n$. Let $\Psi^{f,g}_{k_1,k_2}$ means our construction which is defined above, and R be a random element in P_{2n}. Then, for any four-oracle adversary A that makes at most q_c queries to its first two oracle queries(either Ψ, Ψ^{-1} or R, R^{-1}) and at most q_f and q_g queries to its f and g oracles respectively, it follows that :

$$\left|\Pr[A^{\Psi,\Psi^{-1},f,g}=1]-\Pr[A^{R,R^{-1},f,g}=1]\right| \le (q_c^2+2q_fq_c+2q_gq_c+q_c^2-q_c)\,2^{-n} + \frac{q_c(q_c-1)}{2}(2^{-n+1}+2^{-2n+1}).$$

Our upper bound is as same as the previous one, even though we only use one fourth of that of Gentry-Ramzan's construction. We think that this key size is optimal in the random function model of the Even-Mansour cipher. Also this result reduce the sizable gap between the best known key-recovery attack and the security bound in the above.

Ⅳ. Proof of the Main Results

Our construction is almost same as that of the Gentry-Ramzan except the key materials. Therefore, we can directly apply the frame of proof in 〔4〕 to our construction. The only different part is the definition of the BAD events and their probabilities.

To begin with, let P be the permutation oracle, which is either Ψ or R. Let O^f and O^g be the oracles that compute the functions f and g, respectively. The adversary A can makes two types of queries to the oracle P; $(+,x)$ which asks to obtain the value $P(x)$, $(-,x)$ which asks to obtain the value $P^{-1}(x)$, where $x,y\in\{0,1\}^{2n}$. This is called the cipher queries. We assume that A makes q_c queries such that $<x_1,y_1>,\cdots,<x_{q_c},y_{q_c}>_P$. We also denote oracle queries f and g as (O^f,x') and (O^g,x'') which ask to obtain $f(x')$ and $g(x'')$ respectively, where $x',x''\in\{0,1\}^n$. Let $\{<x'_1,y'_1>,\cdots,<x'_{q_f},y'_{q_f}>\}_{O^f}$ be f-oracle-transcript of A and $\{<x''_1,y''_1>,\cdots,<x''_{q_g},y''_{q_g}>\}_{O^g}$ be g-oracle -transcript of A. For the formal definitions, see 〔4, 8〕.

We denote the $(i+j+k+1)^{st}$ query A makes as a function of the first $(i+j+k)$ query-answer pairs in A's cipher and oracle transcripts by $C_A[\alpha_i,\beta_j,\gamma_k]$, where $\alpha_i=\{<x_1,y_1>,\cdots,<x_i,y_i>\}_P$, $\beta_j=\{<x'_1,y'_1>,\cdots,<x'_j,y'_j>\}_{O^f}$, $\gamma_k=\{<x''_1,y''_1>,\cdots,<x''_k,y''_k>\}_{O^g}$ and either $i<q_c$ or $j<q_f$ or $k<q_g$.

Let $\tilde{\Psi}$ denote the process in which the cipher queries and f-oracle queries answered as they would be Ψ, however the g-oracle queries are answered by another independent random function oracle h. Furthermore, $\tilde{R}$ denote the process that answers all oracle queries as Ψ would, but answers the i^{th} cipher query of A as follows:

1. If A's query is $(+,x_i)$ and for some $1\le j<i$ the j^{th} query-answer pair is $<x_i,y_i>$, then $\tilde{R}$ answers y_i.
2. If A's query is $(-,y_i)$ and for some $1\le j<i$ the j^{th} query-answer pair is $<x_i,y_i>$, then $\tilde{R}$ answers x_i.
3. If neither of the above happens, then $\tilde{R}$ answers with a uniformly chosen element in $\{0,1\}^{2n}$.

Note that $\tilde{R}$ may be inconsistent. However, if $\tilde{R}$ is consistent, it behaves as same as R which is uniformly chosen from the set of random permutations. Now we give the formal definition of these.

〔Definition 3〕 *Let $\sigma=<x_1,y_1>,\cdots,<x_{q_c},y_{q_c}>_P$ be any A-cipher transcript. Then we say that σ is inconsistent if for some $1\le j<i<q_c$ the corresponding query-answer pairs satisfy $x_i=x_j$ but $y_i\neq y_j$, or $x_i\neq x_j$ but $y_i=y_j$. Otherwise σ is consistent.*

〔Definition 4〕 *The random variables T_Ψ, $T_{\tilde{\Psi}}$, T_R, and $T_{\tilde{R}}$ denote that the cipher and oracle transcripts seen by A when its cipher queries are answered by Ψ, $\tilde{\Psi}$, R, $\tilde{R}$ respectively, and its oracle queries are*

answered by O^f and O^g.

Using the above definitions and the definition of $C_A(T_{\tilde{\Psi}'})$, we can obtain $A^{\Psi',\Psi'^{-1},f,g}$ and $C_A(T_{\tilde{\Psi}'})$ denote the same random variable. The same is true for the other random variables. Then we have the followings.

〔Proposition 1〕

$$|\Pr[C_A(T_{\tilde{R}})=1]-\Pr[C_A(T_R)=1]| \le \left(\binom{q_c}{2}\right)\cdot 2^{-2n}.$$

The proof of the proposition can be seen in [4, 8]. Now we want to have an upper bound of the advantage between $T_{\tilde{\Psi}'}$ and $T_{\tilde{\Psi}'}$.

〔Definition 5〕 *For any $k' \in \{0,1\}^n$, we define $BAD(k')$ to be the set of all possible and consistent transcripts $\sigma=(T_P,T_f,T_g)$, with $T_P=<x_1,y_1>,\cdots,<x_{q_c},y_{q_c}>_P$, $T_f=\{<x'_1,y'_1>,\cdots,<x'_{q_f},y'_{q_f}>\}_{O^f}$, and $T_g=\{<x''_1,y''_1>,\cdots,<x''_{q_g},y''_{q_g}>\}_{O^g}$ satisfying at least one of the following events:*

- *BG1* : there exist $1\le i\le q_c$ and $1\le j\le q_g$ s.t. $x_i^R\oplus k'=x_j''$, or
- *BG2* : there exist $1\le i\le q_c$ and $1\le j\le q_g$ s.t. $y_i^L\oplus c\cdot k'=x_j''$.

〔Proposition 2〕 *Let k' be randomly chosen from $\{0,1\}^n$. Then, for any possible and consistent A-transcripts $\sigma=(T_P,T_f,T_g)$, with $T_P=<x_1,y_1>,\cdots,<x_{q_c},y_{q_c}>_P$, $T_f=\{<x'_1,y'_1>,\cdots,<x'_{q_f},y'_{q_f}>\}_{O^f}$, and $T_g=\{<x''_1,y''_1>,\cdots,<x''_{q_g},y''_{q_g}>\}_{O^g}$, we have the following;*

$$\Pr_{k'}[\sigma\in BAD(k')] \le 2q_gq_c\cdot 2^{-n}.$$

Proof. Since k' is randomly chosen from $\{0,1\}^n$, for any fixed i and j, *BG1* and *BG2* happens with probability 2^{-n}. So we can have the desired result directly.

Using the above the proposition, we now can show that $T_{\tilde{\Psi}'}$ and $T_{\tilde{\Psi}'}$ are identically distributed if the following $BAD(k')$ does not happen.

〔Lemma 1〕 *Let σ be any possible and consistent transcripts defined as proposition 2. Then we have the following.*

$$\Pr_{\tilde{\Psi}'}[T_{\tilde{\Psi}'}=\sigma \mid \sigma\notin BADG(k')]=\Pr_{\tilde{\Psi}'}[T_{\tilde{\Psi}'}=\sigma].$$

The proof of this lemma is identical to that of [4]. Now, in order to have a bound of the advantage that A in distinguishing between $T_{\tilde{\Psi}'}$ and $T_{\tilde{R}'}$, we need to define another bad event $BAD(k',g)$.

〔Definition 6〕 *For any $k'\in\{0,1\}^n$ and random function oracle g, we define $BAD(k',g)$ to be the set of all possible and consistent transcripts $\sigma=(T_P,T_f,T_g)$, with $T_P=<x_1,y_1>,\cdots,<x_{q_c},y_{q_c}>_P$, $T_f=\{<x'_1,y'_1>,\cdots,<x'_{q_f},y'_{q_f}>\}_{O^f}$, and $T_g=\{<x''_1,y''_1>,\cdots,<x''_{q_g},y''_{q_g}>\}_{O^g}$ satisfying at least one of the following events:*

- *B1 : there exist $1\le i<j\le q_c$ s.t. $g(x_i^R\oplus k')\oplus x_i^L=g(x_j^R\oplus k')\oplus x_j^L$, or*
- *B2 : there exist $1\le i<j\le q_c$ s.t. $y_i^R\oplus g(y_i^L\oplus c\cdot k')=y_j^R\oplus g(y_j^L\oplus c\cdot k')$, or*
- *B3 : there exist $1\le i,j\le q_c$ s.t. $g(x_i^R\oplus k')\oplus x_i^L=y_j^R\oplus g(y_j^L\oplus c\cdot k')$, or*
- *B4 : there exist $1\le i\le q_c$ and $1\le j\le q_f$ s.t. $g(x_i^R\oplus k')\oplus x_i^L=x_j'$, or*
- *B4 : there exist $1\le i\le q_c$ and $1\le j\le q_f$ s.t. $y_i^R\oplus g(y_i^L\oplus c\cdot k')=x_j'$.*

〔Proposition 3〕 *Let k' be randomly chosen from $\{0,1\}^n$. Then, for any possible and consistent A-transcripts $\sigma=(T_P,T_f,T_g)$, with $T_P=<x_1,y_1>,\cdots,<x_{q_c},y_{q_c}>_P$, $T_f=\{<x'_1,y'_1>,\cdots,<x'_{q_f},y'_{q_f}>\}_{O^f}$, and $T_g=\{<x''_1,y''_1>,\cdots,<x''_{q_g},y''_{q_g}>\}_{O^g}$, we have the following;*

$$\Pr_{k',g}[\sigma\in BAD(k',g)] \le (q_c^2+2q_fq_c+q_c(q_c-1))\cdot 2^{-n}.$$

Proof. For each *B1* and *B2*, the probability is bounded by $\left(\binom{q_c}{2}\right)\cdot 2^{-n}$. since k' is randomly chosen from $\{0,1\}^n$. Similarly, For each *B4* and *B5*, the probability is bounded by $q_cq_f\cdot 2^{-n}$ since k' is ran-

domly chosen from $\{0,1\}^n$ For the case of $B3$, since k' is randomly chosen from $\{0,1\}^n$, we can not distinguish the two functions, $g(x \oplus k')$ and $g(x \oplus c \cdot k')$. So the probability is bounded by $q_c^2 \cdot 2^{-n}$.

Furthermore, if $BAD(k',g)$ does not happen, then $T_{\tilde{\Psi}}$ and $T_{\tilde{R}}$ are identical. So, we have the following lemma.

〔**Lemma 2**〕 *Let σ be any possible and inconsistent transcript as defined Proposition 3. Then*

$$\Pr_{\tilde{\Psi}}[T_{\tilde{\Psi}} = \sigma \mid \sigma \notin BAD(k',g)] = \Pr_{\tilde{\Psi}}[T_{\tilde{\Psi}} = \sigma].$$

With the above lemma, the rest of the proof of our construction can identically follow that of Gentry-Ramzan. The followings are the brief summary of our proof.

$$\begin{aligned}
&\left|\Pr[A^{\Psi,\Psi^{-1},f,g}=1]-\Pr[A^{R,R^{-1},f,g}=1]\right| \\
&=\left|\Pr[C_A(T_{\Psi})=1]-\Pr[C_A(T_R)=1]\right| \\
&\le \left|\Pr[C_A(T_{\Psi})=1]-\Pr[C_A(T_{\tilde{\Psi}})=1]\right| \\
&\quad+\left|\Pr[C_A(T_{\tilde{\Psi}})=1]-\Pr[C_A(T_{\tilde{R}})=1]\right| \\
&\quad+\left|\Pr[C_A(T_{\tilde{R}})=1]-\Pr[C_A(T_R)=1]\right| \\
&\le \Pr_{k'}[\sigma\in BADG(k')]+\Pr_{k',g}[\sigma\in BAD(k',g)] \\
&\qquad+2\cdot\left(\binom{q_c}{2}\right)\cdot 2^{-2n} \\
&\le 2q_cq_c\cdot 2^{-n}+(q_c^2+2q_fq_c+2\cdot\left(\binom{q_c}{2}\right))\cdot 2^{-n} \\
&\qquad+2\cdot\left(\binom{q_c}{2}\right)\cdot 2^{-2n} \\
&\le (q_c^2+2q_fq_c+2q_gq_c+q_c^2-q_c)\,2^{-n} \\
&\qquad+\frac{q_c(q_c-1)}{2}(2^{-n+1}+2^{-2n+1}).
\end{aligned}$$

This completes the proof of our main theorem. So we proved that our construction is as secure as that of Gentry-Ramzan.

V. Conclusion

We considered how to reduce the key size of the Even-Mansour cipher in the random function model. With compared to generic model of Gentry and Ramzan, we reduce the key size from 4n to n, which is the optimal key size of Even-Mansour cipher in the random function oracle model. Also this work reduce sizable gap between the best known key recovery attack and the security bound in the Even-Mansour cipher.

참고문헌(References)

〔1〕 M. Bellare, J. Kilian, and P. Rogaway, "The Security of Cipher Block Chaining," *Advances in Cryptology - CRYPTO'94*, LNCS 839, Springer-Verlag, pp. 341-358, 1994.

〔2〕 M. Bellare and P. Rogaway, "Random Oracles are Practical : A Paradigm for Designing Efficient Protocols," *First ACM Conference on Computer and Communications Security*, Fairfax, pp. 62-73, 1993.

〔3〕 S. Even and Y. Mansour, "A Construction of a Cipher from a Single Pseudorandom Permutation," *Journal of Cryptology*, vol. 10, no. 3, pp. 151-162, 1997. Earlier version in ASIACRYPT'91, LNCS 739, Springer-Verlag, pp. 210-224, 1991.

〔4〕 C. Gentry and Z. Ramzen, "Eliminating Random Permutation Oracles in the Even-Mansour Cipher," *Advances in Cryptology - ASIACRYPT 2004*, LNCS 3329, Springer-Verlag, pp. 32-47, 2004. Full version can be available in IACR *Cryptology ePrint archive*(or available from the author), 2004.

〔5〕 T. Iwata and K. Kurosawa, "How to Re-use Round Function in Super-Pseudorandom Permutation," *The 9th Austalasian Conference on Information Seucurity and Privacy(ACISP 2004)*, LNCS 3108, Springer-Verlag, pp. 224-235, 2004.

〔6〕 T. Iwata, T. Yoshino, and K. Kurosawa, "Non-cryptographic Primitive for Pseudorandom Permutation," *The 9th Fast Software Encryption*

Worksop (FSE 2002), LNCS 2365, Springer-Verlag, pp. 149-163, 2004.

[7] M. Luby and C. Rackoff, "How to Construct Pseudorandom Permutations from Pseudorandom Functions," *SIAM J. Comput.*, vol. 17, pp. 373-386, 1988.

[8] M. Naor and O. Reingold, "On the Construction of Pseudorandom Permutations : Luby-Rackoff Revisited," *Journal of Cryptology*, vol. 12, pp. 29-66, 1999.

[9] J. Patarin, " New Results of Pseudorandom Permutation Generators based on the DES Scheme," *Advances in Cryptology - CRYPTO'91*, LNCS 576, Springer-Verlag, pp. 301-312, 1991.

[10] J. Patarin, "How to Construct Pseudorandom and Super Pseudorandom Permutations from One Single Pseudorandom Function," *Advances in Cryptology - EUROCRYPT'92*, LNCS 658, Springer-Verlag, pp. 256-266, 1992.

[11] S. Patel, Z. Ramzan, and G. S. Sundaram, "Luby-Rackoff Ciphers : Why XOR is not Exclusive," *Selected Areas in Cryptography: 9th Annual International Workshop(SAC 2002)*, LNCS 2595, Springer-Verlag, pp. 271-290, 2002.

[12] Z. Ramzan and L. Reyzin, "On the Round Security of Symmetric-Key Cryptographic Primitives," *Advances in Cryptology - CRYPTO 2000*, LNCS 1880, Springer-Verlag, pp. 376-393, 2000.

〈著者紹介〉

성 재 철 (Jaechul Sung) 종신회원

1997년 8월 : 고려대학교 수학과 학사
1999년 8월 : 고려대학교 수학과 석사
2002년 8월 : 고려대학교 수학과 박사
2002년 8월~2004년 1월 : 한국정보보호진흥원 선임연구원
2004년 2월~현재 : 서울시립대학교 수학과 조교수
<관심분야> 암호 알고리즘 설계 및 분석