Impossibility and Optimality Results on Constructing Pseudorandom Permutations

(Extended Abstract)

Yuliang Zheng, Tsutomu Matsumoto and Hideki Imai

Division of Electrical and Computer Engineering
Yokohama National University
156 Tokiwadai, Hodogaya, Yokohama, 240 Japan

Summary Let $I_n = \{0,1\}^n$, and H_n be the set of all functions from I_n to I_n. For $f \in H_n$, define the *DES-like transformation* associated with f by $F_{2n,f}(L,R) = (R \oplus f(L), L)$, where $L, R \in I_n$. For $f_1, f_2, \ldots, f_s \in H_n$, define $\psi(f_s, \ldots, f_2, f_1) = F_{2n,f_s} \circ \cdots \circ F_{2n,f_2} \circ F_{2n,f_1}$. Our main result is that $\psi(f^k, f^j, f^i)$ is *not* pseudorandom for any positive integers i, j, k, where f^i denotes the i-fold composition of f. Thus, as immediate consequences, we have that (1) none of $\psi(f,f,f)$, $\psi(f,f,f^2)$ and $\psi(f^2,f,f)$ are pseudorandom and, (2) Ohnishi's constructions $\psi(g,g,f)$ and $\psi(g,f,f)$ are optimal. Generalizations of the main result are also considered.

1. Introduction

Random generation is of supreme importance for cryptography, and has recently received extensive investigation by many computer scientists [GGM] [S] [Y]. As mentioned in [LR], if polynomial-time computable pseudorandom invertible permutations are available, then we can design ideal secret-key block ciphers that are provably secure against the chosen plaintext attack. This paper also deals with the construction of pseudorandom (invertible) permutations.

The set of positive integers is denoted by $\mathcal{N}$. For each $n \in \mathcal{N}$, let $I_n = \{0,1\}^n$. Denote by $s_1 \oplus s_2$ the bit-wise XOR of two strings $s_1, s_2 \in I_n$, and by H_n the set of all

2^{n2^n} functions from I_n to I_n. The *composition* of two functions f and g in H_n, denoted by $f \circ g$, is defined by $f \circ g(x) = f(g(x))$ where $x \in I_n$. And in particular, $f \circ f$ is denoted by f^2, $f \circ f \circ f$ by f^3, and so on.

Associate with $f \in H_n$ a function $F_{2n,f} \in H_{2n}$ defined by $F_{2n,f}(L, R) = (R \oplus f(L), L)$ for all $L, R \in I_n$. (Note that our definition for $F_{2n,f}$ is *notationally* different from that given in [LR] and [S]. However, the difference is *not* essential, and does *not* affect the results to be proved below.) $F_{2n,f}$ is a permutation in H_{2n}, and called the *DES-like transformation* associated with f [NBS] [FNS]. Furthermore, for $f_1, f_2, \ldots, f_s \in H_n$, define $\psi(f_s, \ldots, f_2, f_1) = F_{2n,f_s} \circ \cdots \circ F_{2n,f_2} \circ F_{2n,f_1}$. We say that $\psi(f_s, \ldots, f_2, f_1)$ consists of s rounds of DES-like transformations.

In their wonderful paper [LR], Luby and Rackoff showed that permutations $\psi(h, g, f)$, where $f, g, h \in_{\mathrm{R}} H_n$, cannot be efficiently distinguished from an $r \in_{\mathrm{R}} H_{2n}$, here by $x \in_{\mathrm{R}} X$ we mean that x is drawn randomly and uniformly from a finite multi-set X. In other words, from *three* independent random functions $f, g, h \in H_n$, one can construct, by three applications of DES-like transformations, a permutation in H_{2n} which cannot be efficiently distinguished from a truly random function in H_{2n}.

Ohnishi [O] observed that *two* independent random functions are sufficient in Luby and Rackoff's construction. In particular, he showed that both $\psi(g, f, f)$ and $\psi(g, g, f)$, where $f, g \in_{\mathrm{R}} H_n$, cannot be efficiently distinguished from an $r \in_{\mathrm{R}} H_{2n}$. See Appendix for more information on the proof of it.

In the thesis, Ohnishi also showed that neither $\psi(f, f, f)$ nor $\psi(f, g, f)$ are pseudorandom. This result was independently obtained by Rueppel in [R].[1] However, it still remains open whether or not permutations like $\psi(f, f, f^2)$ and $\psi(f^2, f, f)$ are pseudorandom. The technique used in [O] and [R], which is described in the final section of this paper, is not applicable to these cases.

In the remaining part of this paper, we first introduce the notion of pseudorandomness, then show that for any f and for any $i, j, k \in \mathcal{N}$, there is a circuit that distinguishes $\psi(f^k, f^j, f^i)$ from an $r \in_{\mathrm{R}} H_{2n}$. Thus, as immediate consequences, we have that (1) none of $\psi(f, f, f)$, $\psi(f, f, f^2)$ and $\psi(f^2, f, f)$ are pseudorandom and, (2) Ohnishi's constructions $\psi(g, f, f)$ and $\psi(g, g, f)$ are optimal among the pseudorandom

[1] At Eurocrypt'88, Schnorr [S] *erroneously* claimed that $\psi(f, f, f)$, where $f \in_{\mathrm{R}} H_n$, cannot be efficiently distinguished from an $r \in_{\mathrm{R}} H_{2n}$.

permutations $\psi(f_3^k, f_2^j, f_1^i)$ where $i, j, k \in \mathcal{N}$ and $f_1, f_2, f_3 \in H_n$ such that for any $1 \leq s, t \leq 3$, either $f_s = f_t$ or f_s is independent of f_t. We also investigate generalizations of our main result.

2. Notion of Pseudorandomness

Let $n \in \mathcal{N}$. An *oracle circuit* T_n is an acyclic circuit which contains, in addition to ordinary AND, OR, NOT and constant gates, also a particular kind of gates — *oracle gates*. Each oracle gate has an n-bit input and an n-bit output, and it is evaluated using some function from H_n. The output of T_n, a single bit, is denoted by $T_n[f]$ when a function $f \in H_n$ is used to evaluate the oracle gates. The size of T_n is the total number of connections in it. Note that one can view an oracle circuit as a circuit with no inputs or as a circuit with inputs to which constants are assigned.

A family of circuits $T = \{T_n \mid n \in \mathcal{N}\}$ is called a *statistical test for functions* if each T_n is an oracle circuit whose size is bounded by some polynomial in n.

Assume that S_n is a multi-set consisting of functions from H_n. Let $S = \{S_n \mid n \in \mathcal{N}\}$ and $H = \{H_n \mid n \in \mathcal{N}\}$. We say that T is a *distinguisher* for S if for some polynomial P and for infinitely many n, we have $|Pr\{T_n[s] = 1\} - Pr\{T_n[h] = 1\}| \geq 1/P(n)$, where $s \in_{\mathrm{R}} S_n$ and $h \in_{\mathrm{R}} H_n$. We say that S is *pseudorandom* if there is no distinguisher for it. (See also [GGM], [LR] and [Y].)

In this paper we are only concerned with pseudorandom permutations, i.e., pseudorandom functions $S = \{S_n \mid n \in \mathcal{N}\}$ where each S_n consists of permutations from H_n. It is convenient to say that an $s \in_{\mathrm{R}} S_n$ is pseudorandom whenever S is pseudorandom, and not pseudorandom (or can be distinguished from an $r \in_{\mathrm{R}} H_n$) otherwise.

3. Main Result

This section proves our main result on permutations $\psi(f^k, f^j, f^i)$ where $f \in H_n$ and $i, j, k \in \mathcal{N}$. For $i, j, k \in \mathcal{N}$, let $\Psi_{2n}(i, j, k)$ be the multi-set consisting of all functions $\psi(f^k, f^j, f^i) \in H_{2n}$ where $f \in H_n$, and let $\Psi(i, j, k) = \{\Psi_{2n}(i, j, k) \mid n \in \mathcal{N}\}$.

[Theorem 1] *For any $i, j, k \in \mathcal{N}$, there is a distinguisher $T = \{T_{2n} \mid n \in \mathcal{N}\}$ for $\Psi(i, j, k)$, i.e., $\Psi(i, j, k)$ is not pseudorandom. Each T_{2n} has $(m_1 + m_2 + 1)$ oracle gates, where $m_1 = (i + j)/d$, $m_2 = (j + k)/d$ and $d = \gcd(i + j, j + k)$.*

Proof: Denote by $O_0, O_1, \ldots, O_{m_1+m_2}$ the (m_1+m_2+1) oracle gates, by (X_{s1}, X_{s2}) and (Y_{s1}, Y_{s2}) the input to and output of O_s respectively, and by 0^n the all-0 string in I_n. The structure of T_{2n} is as follows. (See also Figure 1.)

DESCRIPTION OF T_{2n} :

(1) The input to O_0 is $(X_{01}, X_{02}) = (0^n, 0^n)$.

(2) The input to O_1 is $(X_{11}, X_{12}) = (0^n, Y_{01})$. And if $m_1 > 1$, then for each $1 < p \leq m_1$, the input to O_p is $(X_{p1}, X_{p2}) = (0^n, X_{(p-1)2} \oplus Y_{(p-1)1})$.

(3) The input to O_{m_1+1} is $(X_{(m_1+1)1}, X_{(m_1+1)2}) = (Y_{02}, 0^n)$. And if $m_2 > 1$, then for each $m_1 + 1 < t \leq m_1 + m_2$, the input to O_t is $(X_{t1}, X_{t2}) = (X_{(t-1)1} \oplus Y_{(t-1)2}, 0^n)$.

(4) Finally, T_{2n} outputs a bit 1 iff $Y_{m_1 2} = X_{(m_1+m_2)1} \oplus Y_{(m_1+m_2)2}$.

Obviously, the size of T_{2n} is of polynomial in n. Now we analyze the behavior of T_{2n} in the following two cases: CASE-1, where a function $\psi(f^k, f^j, f^i) \in \Psi_{2n}(i,j,k)$ is used to evaluate the oracle gates, and CASE-2, where a function drawn randomly and uniformly from H_{2n} is used to evaluate the oracle gates. We show that in the former case, the probability that T_{2n} outputs a bit 1 is 1 and, in the latter case, the probability is less than $1/2^{n-1}$. Thus $T = \{T_{2n} \mid n \in \mathcal{N}\}$ is a distinguisher for $\Psi(i,j,k)$.

CASE-1: Notice that $\psi(f^k, f^j, f^i)(L,R) = (R \oplus f^i(L) \oplus f^k(L \oplus f^j(R \oplus f^i(L))), L \oplus f^j(R \oplus f^i(L)))$. Thus the output of O_0 is $(Y_{01}, Y_{02}) = (f^i(0^n) \oplus f^{k+j+i}(0^n), f^{j+i}(0^n))$.

Denote by $\sim$ a string which we do not care. The inputs to and outputs of $O_1, O_2, \ldots, O_{m_1}$ are as follows:

$$\begin{aligned}
O_1 :\ (X_{11}, X_{12}) &= (0^n, f^i(0^n) \oplus f^{k+j+i}(0^n)),\\
(Y_{11}, Y_{12}) &= (f^{k+j+i}(0^n) \oplus f^{2k+2j+i}(0^n), \sim);\\
O_2 :\ (X_{21}, X_{22}) &= (0^n, f^i(0^n) \oplus f^{2k+2j+i}(0^n)),\\
(Y_{21}, Y_{22}) &= (f^{2k+2j+i}(0^n) \oplus f^{3k+3j+i}(0^n), \sim);
\end{aligned}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\begin{aligned}
O_{m_1} :\ (X_{m_1 1}, X_{m_1 2}) &= (0^n, f^i(0^n) \oplus f^{m_1 k + m_1 j + i}(0^n)),\\
(Y_{m_1 1}, Y_{m_1 2}) &= (\sim, f^{m_1 k + (m_1+1) j + i}(0^n)).
\end{aligned}$$

Similarly, for $O_{m_1+1}, O_{m_1+2}, \ldots, O_{m_1+m_2}$, we have:

$$\begin{aligned}
O_{m_1+1} :\ (X_{(m_1+1)1}, X_{(m_1+1)2}) &= (f^{j+i}(0^n), 0^n),\\
(Y_{(m_1+1)1}, Y_{(m_1+1)2}) &= (\sim, f^{j+i}(0^n) \oplus f^{2j+2i}(0^n));\\
O_{m_1+2} :\ (X_{(m_1+2)1}, X_{(m_1+2)2}) &= (f^{2j+2i}(0^n), 0^n),\\
(Y_{(m_1+2)1}, Y_{(m_1+2)2}) &= (\sim, f^{2j+2i}(0^n) \oplus f^{3j+3i}(0^n));
\end{aligned}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\begin{aligned}
O_{m_1+m_2} :\ (X_{(m_1+m_2)1}, X_{(m_1+m_2)2}) &= (f^{m_2 j + m_2 i}(0^n), 0^n),\\
(Y_{(m_1+m_2)1}, Y_{(m_1+m_2)2}) &= (\sim, f^{m_2 j + m_2 i}(0^n) \oplus f^{(m_2+1)j + (m_2+1)i}(0^n)).
\end{aligned}$$

Thus

$$\begin{aligned}
Y_{m_1 2} &= f^{m_1 k + (m_1+1) j + i}(0^n) = f^{m_1(k+j)+j+i}(0^n)\\
&= f^{\frac{i+j}{d}(k+j)+j+i}(0^n) = f^{j\frac{k+j}{d}+i\frac{k+j}{d}+j+i}(0^n)\\
&= f^{jm_2+im_2+j+i}(0^n) = f^{(m_2+1)j+(m_2+1)i}(0^n)\\
&= X_{(m_1+m_2)1} \oplus Y_{(m_1+m_2)2},
\end{aligned}$$

and the probability that T_{2n} outputs a bit 1 is 1.

CASE-2: There are two sub-cases to be analyzed: $(Y_{01}, Y_{02}) = (0^n, 0^n)$ and $(Y_{01}, Y_{02}) \neq (0^n, 0^n)$.

1) When $(Y_{01}, Y_{02}) = (0^n, 0^n)$, we have $Y_{m_1 2} = X_{(m_1+m_2)1} \oplus Y_{(m_1+m_2)2}$. But $Pr\{(Y_{01}, Y_{02}) = (0^n, 0^n)\} = 1/2^{2n}$.

2) When $(Y_{01}, Y_{02}) \neq (0^n, 0^n)$, we have $(X_{11}, X_{12}) \neq (X_{(m_1+1)1}, X_{(m_1+1)2})$, and hence $(X_{11}, X_{12}) \neq (0^n, 0^n)$ or $(X_{(m_1+1)1}, X_{(m_1+1)2}) \neq (0^n, 0^n)$. Suppose that $(X_{11}, X_{12}) \neq (0^n, 0^n)$. (The other case is similar.) Then (Y_{11}, Y_{12}), and hence (Y_{21}, Y_{22}), (Y_{31}, Y_{32}), $\ldots$, $(Y_{m_1 1}, Y_{m_1 2})$ are all random strings in I_{2n}. These strings are independent of $(X_{(m_1+1)1}, X_{(m_1+1)2})$, and hence of $(Y_{(m_1+1)1}, Y_{(m_1+1)2}), (Y_{(m_1+2)1}, Y_{(m_1+2)2}), \ldots, (Y_{(m_1+m_2)1}, Y_{(m_1+m_2)2})$. So when $(Y_{01}, Y_{02}) \neq (0^n, 0^n)$, the probability that $Y_{m_1 2} = X_{(m_1+m_2)1} \oplus Y_{(m_1+m_2)2}$, i.e., T_{2n} outputs a bit 1, is $1/2^n$.

Thus, for CASE-2, we have

$$\begin{aligned}
&Pr\{T_{2n}[f] = 1\} \\
&\quad = Pr\{T_{2n}[f] = 1 \mid (Y_{01}, Y_{02}) = (0^n, 0^n)\} \cdot Pr\{(Y_{01}, Y_{02}) = (0^n, 0^n)\} \\
&\qquad + Pr\{T_{2n}[f] = 1 \mid (Y_{01}, Y_{02}) \neq (0^n, 0^n)\} \cdot Pr\{(Y_{01}, Y_{02}) \neq (0^n, 0^n)\} \\
&\quad = 1 \cdot 1/2^{2n} + 1/2^n \cdot (1 - 1/2^{2n}) \\
&\quad < 1/2^{n-1}.
\end{aligned}$$

This completes the proof. ▮

As a consequence of Theorem 1, we know that none of $\psi(f, f, f)$, $\psi(f, f, f^2)$ and $\psi(f^2, f, f)$, where $f \in_{\mathrm{R}} H_n$, are pseudorandom.

Next we discuss the optimality of $\psi(g, g, f)$ and $\psi(g, f, f)$ where $f, g \in_{\mathrm{R}} H_n$. Apparently, $F_{2n,f}$ can be distinguished from an $r \in_{\mathrm{R}} H_{2n}$. It was proved in [LR] that *two* applications of DES-like transformations cannot obtain a pseudorandom permutation. In particular, Luby and Rackoff showed that $\psi(g, f)$, where $f, g \in H_n$, can be easily distinguished from an $r \in_{\mathrm{R}} H_{2n}$.

Thus, by putting together Theorem 1 and Ohnishi's observations mentioned above, we see that to get a pseudorandom permutation in H_{2n}, *two* independent random functions from H_n and three applications of DES-like transformations are not only *sufficient* but also *necessary*, as far as our construction is restricted to the permutations

$\psi(f_3^k, f_2^j, f_1^i)$, where $i, j, k \in \mathcal{N}$ and $f_1, f_2, f_3 \in H_n$ such that for any $1 \leq s, t \leq 3$, either $f_s = f_t$ or f_s is independent of f_t. In other words, under the above condition, pseudorandom permutations $\psi(g, f, f)$ and $\psi(g, g, f)$ proposed by Ohnishi [O], where $f, g \in_{\mathrm{R}} H_n$, are *optimal* in the sense that they consist of the minimal rounds of DES-like transformations, and "consume" the minimal number of independent random functions from H_n.

4. Generalizations

This section extends in two directions Theorem 1 to the case of *generalized DES-like transformations*.

Let $\ell \in \mathcal{N}$ with $\ell \geq 2$. Following [FNS, pp.1547-1549] and [S], we associate with an $f \in H_n$ a function $F_{\ell n,f} \in H_{\ell n}$ defined by $F_{\ell n,f}(B_1, B_2, \ldots, B_\ell) = (B_2 \oplus f(B_1), B_3, \ldots, B_\ell, B_1)$, where $B_i \in I_n$. Call $F_{\ell n,f}$ the *generalized DES-like transformation* associated with f.

For $f_1, f_2, \ldots, f_s \in H_n$, define $\theta(f_s, \ldots, f_2, f_1) = F_{\ell n,f_s} \circ \cdots \circ F_{\ell n,f_2} \circ F_{\ell n,f_1}$. It is easy to show that when $s < 2\ell - 1$, $\theta(f_s, \ldots, f_2, f_1)$ can be distinguished from an $r \in_{\mathrm{R}} H_{\ell n}$. By modifying the proof for the Main Lemma of [LR], it can be shown that when $s = 2\ell - 1$, $\theta(f_s, \ldots, f_2, f_1)$ is pseudorandom where $f_1, f_2, \ldots, f_s \in_{\mathrm{R}} H_n$.

Now we prove an impossibility result on $\theta(f_{2\ell-1}, \ldots, f_2, f_1)$. For $(2\ell - 1)$ integers $i_1, i_2, \ldots, i_{2\ell-1} \in \mathcal{N}$, let $\Theta_{\ell n}(i_1, i_2, \ldots, i_{2\ell-1})$ be the multi-set consisting of all functions $\theta(f^{i_{2\ell-1}}, \ldots, f^{i_2}, f^{i_1}) \in H_{\ell n}$ where $f \in H_n$, and let $\Theta(i_1, i_2, \ldots, i_{2\ell-1}) = \{\Theta_{\ell n}(i_1, i_2, \ldots, i_{2\ell-1}) \mid n \in \mathcal{N}\}$.

[Theorem 2] *For any $i_1, i_2, \ldots, i_{2\ell-1} \in \mathcal{N}$, there is a distinguisher $T = \{T_{\ell n} \mid n \in \mathcal{N}\}$ for $\Theta(i_1, i_2, \ldots, i_{2\ell-1})$. Each $T_{\ell n}$ has $(m_1 + m_2 + 1)$ oracle gates, where $m_1 = (i_1 + i_2 + \cdots + i_\ell)/d$, $m_2 = (i_2 + i_3 + \cdots + i_{\ell+1})/d$ and $d = \gcd(i_1 + i_2 + \cdots + i_\ell, i_2 + i_3 + \cdots + i_{\ell+1})$.*

Proof: There are two cases to be treated: $\ell = 2$ and $\ell > 2$. The former has been proved in Theorem 1. The proof for the latter is similar to that for the former.

As in the proof of Theorem 1, denote by $O_0, O_1, O_2, \ldots, O_{m_1+m_2}$ the $(m_1 + m_2 + 1)$ oracle gates, by $(X_{s1}, X_{s2}, \ldots, X_{s\ell})$ and $(Y_{s1}, Y_{s2}, \ldots, Y_{s\ell})$ the input to and output of O_s respectively, and by 0^n the all-0 string in I_n.

DESCRIPTION OF $T_{\ell n}$:

(1) The input to O_0 is $(X_{01}, X_{02}, \ldots, X_{0\ell}) = (0^n, 0^n, \ldots, 0^n)$.

(2) The input to O_1 is $(X_{11}, X_{12}, \ldots, X_{1\ell}) = (0^n, Y_{03}, 0^n, \ldots, 0^n)$. And if $m_1 > 1$, then for each $1 < p \leq m_1$, the input to O_p is $(X_{p1}, X_{p2}, \ldots, X_{p\ell}) = (0^n, X_{(p-1)2} \oplus Y_{(p-1)3}, 0^n, \ldots, 0^n)$.

(3) The input to O_{m_1+1} is $(X_{(m_1+1)1}, X_{(m_1+1)2}, \ldots, X_{(m_1+1)\ell}) = (Y_{02}, 0^n, \ldots, 0^n)$. And if $m_2 > 1$, then for each $m_1 + 1 < t \leq m_1 + m_2$, the input to O_t is $(X_{t1}, X_{t2}, \ldots, X_{t\ell}) = (X_{(t-1)1} \oplus Y_{(t-1)2}, 0^n, \ldots, 0^n)$.

(4) $T_{\ell n}$ outputs a bit 1 iff $Y_{m_1 2} = X_{(m_1+m_2)1} \oplus Y_{(m_1+m_2)2}$.

See also Figure 2 for the structure of $T_{\ell n}$. Analysis necessary is also similar to Theorem 1, and omitted here. ∎

Further analysis of the proof for Theorem 2 reveals that even given $(\ell - 1)$ independent random functions from H_n, it is not guaranteed that one can always obtain pseudorandom permutations in $H_{\ell n}$, by $(2\ell - 1)$ applications of generalized DES-like transformations. This is formally stated below.

Let $i_1, i_2, \ldots, i_{\ell+1} \in \mathcal{N}$, and let $\widetilde{\Theta}_{\ell n}(i_1, i_2, \ldots, i_{\ell+1})$ be the multi-set consisting of all functions $\theta(f_{\ell-1}, \ldots, f_3, f_2, f_1^{i_{\ell+1}}, \ldots, f_1^{i_2}, f_1^{i_1}) \in H_{\ell n}$ where $f_1, f_2, \ldots, f_{\ell-1} \in H_n$, and let $\widetilde{\Theta}(i_1, i_2, \ldots, i_{\ell+1}) = \{\widetilde{\Theta}_{\ell n}(i_1, i_2, \ldots, i_{\ell+1}) \mid n \in \mathcal{N}\}$.

[Theorem 3] *For any $i_1, i_2, \ldots, i_{\ell+1} \in \mathcal{N}$, $\widetilde{\Theta}(i_1, i_2, \ldots, i_{\ell+1})$ is not pseudorandom.*

5. Concluding Remarks

Our consideration has been restricted to the case of $\psi(f_3^k, f_2^j, f_1^i)$ where $i, j, k \in \mathcal{N}$ and $f_1, f_2, f_3 \in H_n$ such that for any $1 \le s, t \le 3$, either $f_s = f_t$ or f_s is independent of f_t. It is worth while examining other cases, such as $\psi(\hat{f}, f, f)$ and $\psi(f, f, \hat{f})$ where $\hat{f}$ is constructed from f with $\hat{f} \neq f^m$ for any $m \in \mathcal{N}$.

Also, it is not clear to us whether or not *one* independent random function $f \in H_n$ can be used to construct a pseudorandom permutation, by more than three applications of DES-like transformations such as $\psi(f, f, f, f^2)$ and $\psi(f^2, f, f, f)$.

Some partial impossibility results were implied in [O], where Ohnishi showed that both $\psi(f_s, \ldots, f_2, f_1, f_0, f_1, f_2, \ldots, f_s)$ and $\psi(f_s, \ldots, f_2, f_1, f_1, f_2, \ldots, f_s)$, where $f_i \in H_n$, can be distinguished from an $r \in_{\mathrm{R}} H_{2n}$ by an oracle circuit $\bar{T}_{2n}$ with two oracle gates O_1 and O_2. The structure of $\bar{T}_{2n}$ is as follows: (1) Choose $X_1, X_2 \in I_n$. (2) Input (X_1, X_2) to O_1. Assume that the output of O_1 is (Y_1, Y_2). (3) Input (Y_2, Y_1) to O_2. Assume that the output of O_2 is (Z_1, Z_2). (4) $\bar{T}_{2n}$ outputs a bit 1 iff $(X_1, X_2) = (Z_2, Z_1)$.

To the end, we pose an open problem: Prove or disprove that from *one* random function in H_n, one can obtain in some way a pseudorandom (invertible) permutation in H_{2n}.[2]

Acknowledgment

This work was motivated by [LR], [O] and [S] as well as the Dec.1988 communication with Professor C. P. Schnorr. The authors also would like to thank Professor A. Maruoka of Tohoku University for making the reference [O] available.

[2] Schnorr believed that the answer to the problem would be affirmative. (private conversation at Eurocrypt'89, April 1989.)

References

[FNS] H. Feistel, W. A. Notz and J. L. Smith: “Some cryptographic techniques for machine-to-machine data communications,” *Proceedings of IEEE* , Vol. 63, No. 11, (1975), pp.1545-1554.

[GGM] O. Goldreich, S. Goldwasser and S. Micali: “How to construct random functions,” *Journal of ACM*, Vol. 33, No. 4, (1986), pp.792-807.

[LR] M. Luby and C. Rackoff: “How to construct pseudorandom permutations from pseudorandom functions,” *SIAM Journal on Computing*, Vol. 17, No. 2, (1988), pp.373-386. (A preliminary version including other results appeared in *Proceedings of the 18th ACM Symposium on Theory of Computing*, (1986), pp.356-363.)

[NBS] *Data Encryption Standard*, Federal Information Processing Standards (FIPS) Publication 46, National Bureau of Standards, U.S. Department of Commerce, (1977).

[O] Y. Ohnishi: “A study on data security,” *Master Thesis* (in Japanese), Tohoku University, Japan, (March, 1988).

[R] R. A. Rueppel: “On the security of Schnorr’s pseudorandom generator,” *Abstracts of EUROCRYPT’89*, Houthalen, (April 10-13, 1989).

[S] C. P. Schnorr: “On the construction of random number generators and random function generators,” *Advances in Cryptology — EUROCRYPT’88*, LNCS Vol. 330, Springer-Verlag, (1988), pp.225-232.

[Y] A.C. Yao: “Theory and applications of trapdoor functions,” *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science*, (1982), pp.80-91.

Appendix

In [O], Ohnishi showed that both $\psi(g,f,f)$ and $\psi(g,g,f)$, where $f,g\in_{\mathrm{R}} H_n$, cannot be efficiently distinguished from an $r\in_{\mathrm{R}} H_{2n}$. He obtained the result by carefully modifying the proof for the Main Lemma of [LR]. The major modification begins with the definition of B-gate$_i$ [LR,p.382]. Now we describe the definition for the case of $\psi(g,g,f)$. The case of $\psi(g,f,f)$ is similar.

Let $\Omega = \{0,1\}^{3nm}$, and $\omega = \omega_1,\cdots,\omega_{3nm} \in \Omega$. For $1 \le i \le m$, define $X_i(\omega), Y_{2i-1}(\omega)$ and $Y_{2i}(\omega)$ as follows:

$$X_i(\omega) = \omega_{(i-1)n+1} \bullet \cdots \bullet \omega_{(i-1)n+n},$$

$$Y_{2i-1}(\omega) = \omega_{mn+(2i-2)n+1} \bullet \cdots \bullet \omega_{mn+(2i-2)n+n},$$

$$Y_{2i}(\omega) = \omega_{mn+(2i-1)n+1} \bullet \cdots \bullet \omega_{mn+(2i-1)n+n}.$$

Also let

$$X(\omega) =< X_1(\omega),\ldots,X_m(\omega) >,$$

$$Y(\omega) =< Y_1(\omega),\ldots,Y_{2m}(\omega) > .$$

The ith oracle gate is computed as follows:

```
$B$-gate$_i$:
    The input is $L_i(\omega) \bullet R_i(\omega)$,
    $\ell \leftarrow \min\{j : 1 \le j \le i, R_i(\omega) = R_j(\omega)\}$,
      $\alpha'_i(\omega) \leftarrow L_i(\omega) \oplus X_\ell(\omega)$,
    $\ell \leftarrow \min\{\{2j-1 : 1 \le j \le i, \alpha'_i(\omega) = \alpha'_j(\omega)\} \bigcup$
                $\{2j : 1 \le j \le i-1, \alpha'_i(\omega) = \beta'_j(\omega)\}\}$,
      $\beta'_i(\omega) \leftarrow R_i(\omega) \oplus Y_\ell(\omega)$,
    $\ell \leftarrow \min\{\{2j-1 : 1 \le j \le i, \beta'_i(\omega) = \alpha'_j(\omega)\} \bigcup$
                $\{2j : 1 \le j \le i, \beta'_i(\omega) = \beta'_j(\omega)\}\}$,
      $\gamma'_i(\omega) \leftarrow \alpha'_i(\omega) \oplus Y_\ell(\omega)$,
    The output is $\beta'_i(\omega) \bullet \gamma'_i(\omega)$.
```

Note that the same function g is applied in both the second and the third rounds of DES-like transformations of $\psi(g,g,f)$. So the key point is that each input to g should be compared with *all* previous inputs to it, no matter which round they appear in.

The remaining portion of the proof proceeds in the same way as [LR], with some obvious modifications introduced by the above defined B-gate$_i$.

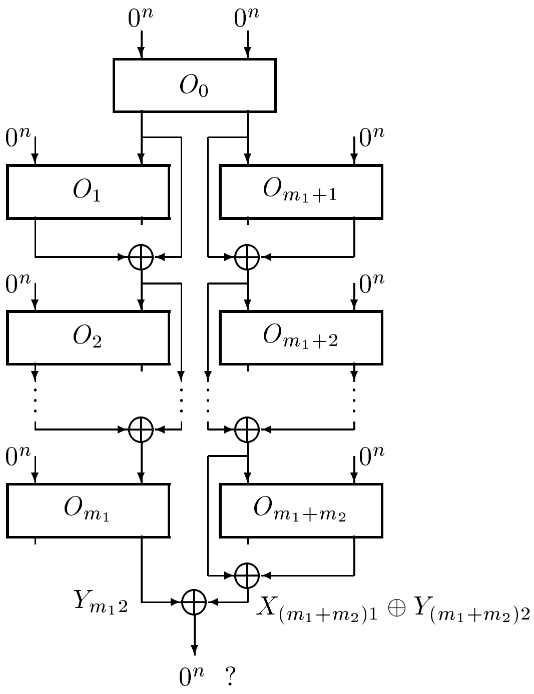

Figure 1: Structure of Oracle Circuit T_{2n}

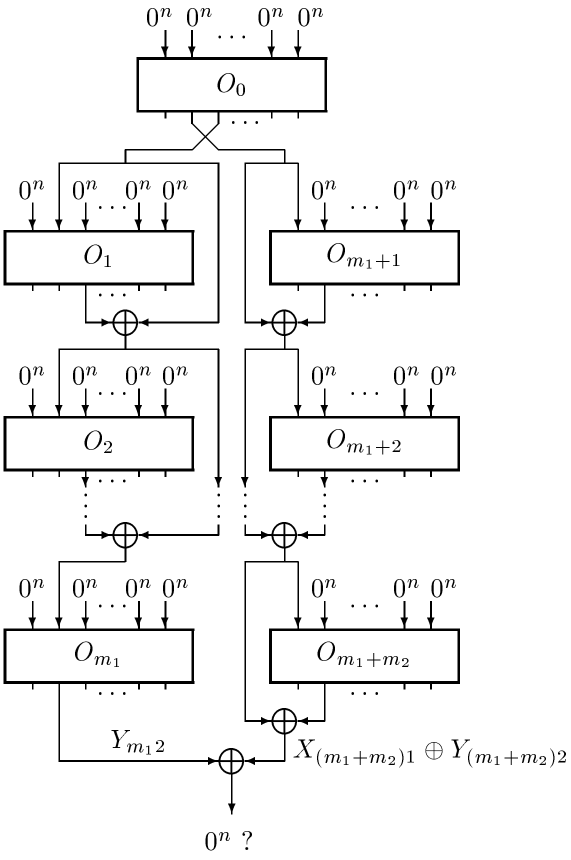

Figure 2: Structure of Oracle Circuit $T_{\ell n}$