NEW RESULTS ON PSEUDORANDOM PERMUTATION GENERATORS BASED ON THE DES SCHEME

Jacques PATARIN
INRIA Domaine de Voluceau BP 105 78153 Le Chesnay Cedex France

J. Feigenbaum (Ed.): Advances in Cryptology - CRYPTO '91, LNCS 576, pp. 301-312, 1992.

NEW RESULTS ON PSEUDORANDOM PERMUTATION GENERATORS BASED ON THE DES SCHEME

Abstract

We denote by ψ^k the permutation generator based on the DES Scheme with k rounds where the S boxes are replaced by random independant functions. We denote by $|P_1 - P_1^*|$, (respectively $|P_1 - P_1^{**}|$), the probability of distinguishing such a permutation from a random function (respectively from a random permutation) by means of a distinguishing circuit that has m oracle gates.
In 1988, M. Luby and C. Rackoff [1] proved that

$$\forall k \geq 3, |P_1 - P_1^*| \leq \frac{m(m-1)}{2^n}.$$

At Eurocrypt 90, J. Pieprzyk wondered at the end of his paper [4] if that inequality could be improved. This is the problem we consider here. In particular, such an improvement could greatly reduce the length of the keys used in a "direct" application of these theorems to a cryptosystem.

Our main results will be :

1. For ψ^3 and ψ^4 there is no really tighter inequality than $|P_1 - P_1^*| \leq \frac{m(m-1)}{2^n}$.
2. However for ψ^5 (and then for $\psi^k, k \geq 5$), there is a much tighter inequality than Luby - Rackoff's one. For example for ψ^6, $|P_1 - P_1^*|$ and $|P_1 - P_1^{**}|$ are $\leq \frac{12m}{2^n} + \frac{18m^3}{2^{2n}}$.
3. When m is very small ($m = 2$ or 3 for example) it is possible to have an explicit evaluation of the effects of the number of rounds k on the "better and better pseudorandomness" of ψ^k.

1 Notations and definitions

Definitions 1

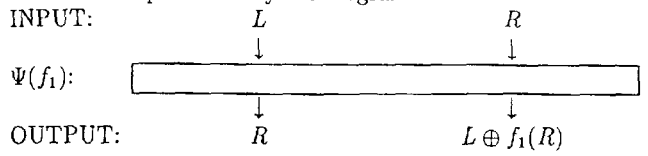
- I_n is the set $\{0,1\}^n, n \in \mathbf{N}$.
- For $a, b \in I_n$, $[a, b]$ will be the string of length $2n$ of I_{2n} which is the concatenation of a and b.
- If A and B are two sets, A^B will be the set of all functions from B to A.
- The set of all functions from I_n to I_n is F_n. So $F_n = I_n^{I_n}$.
- The set of all permutations from I_n to I_n is B_n, so $B_n \subset F_n$.
- $\circ$ is the composition of functions.
- E_0 is the number of elements of F_n. So $E_0 = (2^n)^{2^n} = 2^{n \cdot 2^n}$.
- f^2 is $f \circ f$.

Definition 2 Let f_1 be a function from I_n to I_n, and let L, R, S, and T be elements of I_n.
Then by definition : $\Psi(f_1)$ is the function from $I_{2n} \rightarrow I_{2n}$ such that:

$$\forall (L,R) \in I_n^2,\ \Psi(f_1)[L,R] = [S,T] \iff \begin{cases} S = R \\ T = L \oplus f_1(R) \end{cases},$$

where $\oplus$ is the bitwise addition modulo 2.

This can be represented by the diagram

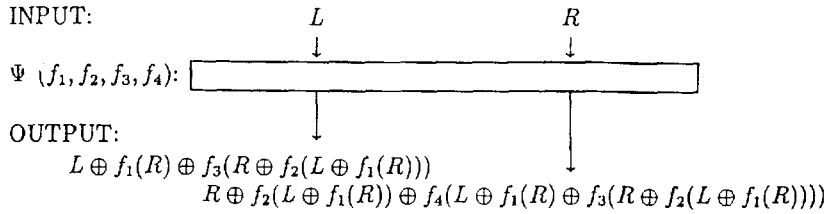


Note that $\Psi(f_1)$ is a permutation $I_{2n} \rightarrow I_{2n}$.

Definition 3 Let $f_1, f_2, \ldots, f_k$ be k functions from I_n to I_n. $\Psi(f_1, \ldots, f_k)$ is the permutation from I_{2n} to I_{2n} defined by:

$$\Psi(f_1, \ldots, f_k) = \Psi(f_k) \circ \cdots \circ \Psi(f_2) \circ \Psi(f_1),$$

where $\circ$ is the composition of functions. For example we have for $\psi(f_1, f_2, f_3, f_4)$:



Remark:
$\Psi(f_1, \ldots, f_k)$ is in fact a *k iteration DES Scheme* where the S-boxes are replaced by the functions $f_1, \ldots, f_k$.

Definition 4 We will use the notation ψ^k to say that we are considering a permutation $\psi(f_1, \ldots, f_k)$, where $f_1, \ldots, f_k$ are k independant function randomly chosen in F_n.

We will assume that the definitions of permutation generator, distinguishing circuit, random oracle, pseudorandom permutation generator, and super pseudorandom permutation generator are known. These definitions can be found in [1] for example.

Definition 5 Let ϕ be a distinguishing circuit. We will denote by $\phi(f)$ its output (1 or 0) when its oracle gates are given the values of the function f.
We will denote by P_1 the probability that $\phi(f) = 1$ when $f_1, \ldots, f_k$ are k functions randomly chosen in F_n, and $f = \psi(f_1, \ldots, f_k)$.

So : $P_1 = \dfrac{\text{Number of } (f_1, \ldots, f_k) \text{ such that } \phi(\psi(f_1, \ldots, f_k)) = 1}{E_0^k}$.

We will denote by P_1^* the probability that $\phi(f) = 1$ when f is randomly chosen in F_{2n}.

Then : $P_1^* = \dfrac{\text{Number of functions } f \in F_{2n} \text{ such that } \phi(f) = 1}{(2^{2n})^{(2^{2n})}}$.

And we will denote by P_1^{**} the probability that $\phi(f) = 1$ when f is randomly chosen in B_{2n}.

Then : $P_1^{**} = \dfrac{\text{Number of permutations } f \in B_{2n} \text{ such that } \phi(f) = 1}{(2^{2n})!}$.

Notice that P_1 depends on k and ϕ, and that P_1^* depends on ϕ.
A distinguishing circuit has only normal oracle gates. To insist on this, we will use sometimes the expression "normal distinguishing circuit" for "distinguishing circuit". A "super distinguishing circuit" has normal and inverse oracle gates. (See [1] for precise definitions).

Definition 6 Let ϕ be a super distinguishing circuit.
We will define $\phi(f), P_1$ and P_1^{**} exactly as for normal distinguishing circuit.

Notice that here P_1^* is not defined. This is because an inverse oracle gate is just defined with permutations.

Definition 7 Let σ be the permutation such that :
$\forall (L, R) \in I_n^2, \sigma[L, R] = [R, L]$. ($\sigma$ "swaps" the left and the right parts). $\sigma \in B_{2n}$.
Then for all functions $f_1, \ldots, f_k$ of F_n we have : $\psi(f_1)^{-1} = \sigma \circ \psi(f_1) \circ \sigma$.
And : $\psi(f_1, \ldots, f_k)^{-1} = \sigma \circ \psi(f_k, \ldots, f_1) \circ \sigma$.

In [1], M. Luby and C. Rackoff proved that for ψ^3 (or for $\psi^k, k \geq 3$), for any normal distinguishing circuit ϕ with m oracle gates, $|P_1 - P_1^*| \leq \dfrac{m(m-1)}{2^n}$.

The aim of this paper is to find conditions on k under which such an inequality can significantly be improved. In paragraph 6 we will give an example of J. Pieprzyk which shows why such an improvement can be interesting.

2 The case $m = 2$

Here we will just consider distinguishing circuits with two oracle gates. Of course this case is less important than the cases where m is large. (m large will be subject of paragraphs 3,4 and 5). But when m is very small ($m = 0, 1, 2$ or 3) it is possible to study the problem completely, and to obtain the exact maximum values of $|P_1 - P_1^*|$ and $|P_1 - P_1^{**}|$, and this is done for each k. Then this case will show with high precision how our generator of permutations "better and better pseudorandom" becomes when the number of rounds increases.

Remark:
For $m = 0$ and $m = 1$ we have $|P_1 - P_1^*| = 0$ if $k \geq 2$. So the real problem begins when $m \geq 2$.

Let $L_1, R_1, L_2, R_2, S_1, T_1, S_2, T_2$ be elements of I_n such that $(L_1, R_1) \neq (L_2, R_2)$ and $(S_1, T_1) \neq (S_2, T_2)$.
The key property is that, we are able to find the exact number H of k -tuples of functions $(f_1, \ldots, f_k)$ such that :
$\forall i, 1 \leq i \leq m, \psi^k(f_1, \ldots, f_k)[L_i, R_i] = [S_i, T_i]$ when m is very small ($m = 2$ here). Then, the values H will give us the maximum of $|P_1 - P_1^*|$ and $|P_1 - P_1^{**}|$.

For $m = 2$ an explicit calculation gives the values H. (The proof is by induction on k). For an even k these values are :

Theorem 2.1 *Let* $a_0 = \dfrac{1}{1 - \frac{1}{2^{2n}}} \cdot \dfrac{E_0^k}{2^{4n}}$, *where* $E_0 = 2^{n.2^n}$.
Then when k *is even and* $k \geq 2$, *we have :*

Case 1 : $R_1 \neq R_2$ **and** $S_1 \neq S_2$. Then $H = a_0 \left(1 - \dfrac{1}{2^{kn}}\right)$.

Case 2 : $R_1 \neq R_2, S_1 = S_2$ **and** $R_1 \oplus R_2 \neq T_1 \oplus T_2$.
or : $R_1 = R_2, S_1 \neq S_2$ **and** $S_1 \oplus S_2 \neq L_1 \oplus L_2$

Then $H = a_0 \left(1 - \dfrac{1}{2^{(\frac{k}{2}-1)n}} - \dfrac{1}{2^{(\frac{k}{2})n}} + \dfrac{1}{2^{(k-1)n}}\right)$.

Case 3 : $R_1 \neq R_2, S_1 = S_2$ **and** $R_1 \oplus R_2 = T_1 \oplus T_2$
or : $R_1 = R_2, S_1 \neq S_2$ **and** $S_1 \oplus S_2 = L_1 \oplus L_2$

Then $H = a_0 \left(1 + \dfrac{1}{2^{(\frac{k}{2}-2)n}} - \dfrac{1}{2^{(\frac{k}{2}-1)n}} - \dfrac{2}{2^{\frac{kn}{2}}} + \dfrac{1}{2^{(k-1)n}}\right)$.

Case 4 : $R_1 = R_2$ **and** $S_1 = S_2$

Then $H = a_0 \left(1 - \dfrac{1}{2^{(k-2)n}}\right)$.

When k is odd and $k \geq 3$, calculation of H is also possible. There are then five cases. (See [3] for details).

The values of H will give us the maximum of $|P_1 - P_1^*|$ and the maximum of $|P_1 - P_1^{**}|$.
We will denote this numbers by $|P_1 - P_1^*|_{\max}$ and $|P_1 - P_1^{**}|_{\max}$.

We find (for $m = 2$) :

	$\lvert P_1 - P_1^* \rvert_{\max}$	approximate value of $\lvert P_1 - P_1^{**} \rvert_{\max} \simeq$
ψ^1	$1 - \frac{1}{2^{3n}}$	$1 - \frac{1}{2^{3n}}$ (The exact value is : $1 - \frac{1}{2^{3n} - 2^n}$)
ψ^2	$1 - \frac{1}{2^n}$	$1 - \frac{1}{2^n}$
ψ^3	$\frac{1}{2^n} - \frac{1}{2^{2n}}$	$\frac{1}{2^n}$
ψ^4	$\frac{1}{2^n} - \frac{1}{2^{2n}}$	$\frac{1}{2^n}$
ψ^5	$\frac{2}{2^{2n}} - \frac{2}{2^{3n}}$	$\frac{1}{2^{2n}}$
ψ^6	$\frac{1}{2^{2n}} + \frac{1}{2^{3n}} - \frac{2}{2^{4n}}$	$\frac{1}{2^{2n}}$
ψ^7	$\frac{1}{2^{2n}} + \frac{1}{2^{4n}} - \frac{2}{2^{5n}}$	$\frac{1}{2^{3n}}$
ψ^8	$\frac{1}{2^{2n}}$	$\frac{1}{2^{3n}}$
$\psi^k, k \geq 8$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{(\frac{k}{2}-1)n}}$ for k even $\frac{1}{2^{(\frac{k}{2}-\frac{1}{2})n}}$ for k odd

$\forall k \geq 8$, $|P_1 - P_1^*|_{\max} = \frac{1}{2^{2n}}$.

$|P_1 - P_1^*|_{\max} \not\to 0$ because $\psi^k(f_1, \ldots, f_k)$ is a permutation so $(L_1, R_1) \neq (L_2, R_2) \Rightarrow (S_1, T_1) \neq (S_2, T_2)$.

But we have :

$$|P_1 - P_1^{**}| \overset{k \to +\infty}{\longrightarrow} 0.$$

Conclusion

When $m = 2$ we can obtain the exact values of $|P_1 - P_1^*|_{\max}$ and $|P_1 - P_1^{**}|_{\max}$ for all k. (See [3] for the exact values of $|P_1 - P_1^{**}|_{\max}$).

For $m = 2$, the result of M. Luby and C. Rackoff says that $\forall k \geq 3, |P_1 - P_1^*|_{\max} \leq \frac{2}{2^n}$.

This gives us a good minoration for ψ^3 and ψ^4 (because then the exact value of $|P_1 - P_1^*|_{\max}$ is $\frac{1}{2^n}$), but for $k \geq 5$, $|P_1 - P_1^*|_{\max} \leq \frac{2}{2^{2n}}$. So, for $k \geq 5$ and $m = 2$, it is indeed possible to improve the result of M. Luby and C. Rackoff.

This lets us hope that we can improve this result for other values of m as well.

Another important result that we obtain is that $|P_1 - P_1^{**}| \overset{k \to +\infty}{\longrightarrow} 0$, and when k is large the rate of convergence is about $2^{\frac{kn}{2}}$. (It is possible to see this directly in the expressions of H that we have given). So we have an explicit evaluation of the effects of the number of rounds k on the "better and better pseudorandomness" of ψ^k, when $m = 2$.

3 General properties of P_1, P_1^* and P_1^{**}

We will always denote by m the number of oracle gates, by k the number of rounds ψ that we use in ψ^k, and by n the integer such that the permutations that we are considering are in B_{2n}.

Definition 8 When m, k and n are fixed, we will denote by $|P_1 - P_1^*|_{\max}$ the smallest real number such that :
for all normal distinguishing circuit that has m oracle gates, we have : $|P_1 - P_1^*| \leq |P_1 - P_1^*|_{\max}$.
So $|P_1 - P_1^*|_{\max}$ is less or equal than 1, and it depends on m, k and n.
And we will define $(P_1 - P_1^*)_{\max}$ and $(P_1^* - P_1)_{\max}$ in the same way.

Definition 9 When m, k and n are fixed, we will denote by $|P_1 - P_1^{**}|_{\max}$ the smallest real number such that :
for all super distinguishing circuits that have m oracle gates, we have : $|P_1 - P_1^{**}| \leq |P_1 - P_1^{**}|_{\max}$.
We define $(P_1 - P_1^{**})_{\max}$ and $(P_1^{**} - P_1)_{\max}$ in the same way.
Now we will see some example of the properties of these values.
(See [3] for the proofs).

Theorem 3.1 *There is always a distinguishing circuit such that* $|P_1 - P_1^*| = |P_1 - P_1^*|_{\max}$ *and there is always a super distinguishing circuit such that* $|P_1 - P_1^{**}| = |P_1 - P_1^{**}|_{\max}$.

Theorem 3.2 $(P_1 - P_1^*)_{\max} = (P_1^* - P_1)_{\max} = |P_1 - P_1^*|_{\max}$.

Theorem 3.3 $(P_1 - P_1^{**})_{\max} = (P_1^{**} - P_1)_{\max} = |P_1 - P_1^{**}|_{\max}$.

Theorem 3.4 *When m increases (and k and n are fixed),* $|P_1 - P_1^*|_{\max}$ *and* $|P_1 - P_1^{**}|_{\max}$ *increase.*

Theorem 3.5 *When k increases (and m and n are fixed),* $|P_1 - P_1^*|_{\max}$ *and* $|P_1 - P_1^{**}|_{\max}$ *decrease.*

Remarks

1. Theorem 3.5 is very important because it shows that when the number of rounds k increases, the random properties of ψ^k can just be better. But notice that this is due to the fact that all the $f_1, \ldots, f_k$ are **independant** function randomly chosen in F_n. For example $\psi(f, f, f, f^2)$ is pseudo-random (as claimed in [4]), but if one adds a round $\psi(f^2)$, we obtaint $G = \psi(f^2, f, f, f, f^2)$. And this one is not pseudo-random. This is because it is its own inverse if left and right halves of inputs and outputs are swapped : $G^{-1} = \sigma \circ G \circ \sigma$. So if g is a permutation such that $g[L, R] = [S, T]$ by testing if $g[T, S] = [R, L]$ it is possible to know if g is probably a permutation of G or not.

2. The decrease is not necessarily strict for $|P_1 - P_1^*|_{\max}$ as we have seen for $m = 2$.

Theorem 3.6 *For all normal distinguishing circuit with m oracle gates, $|P_1^* - P_1^{**}| \leq \frac{m(m-1)}{2.2^{2n}}$.*

Remark:
This shows that if m is not of order 2^n, it is not possible to distinguish a random permutation from a random function with a high probability. The converse of this property is well known : it is indeed possible to distinguish with a high probability a random permutation of B_{2n} from a random function of F_{2n} when m is of order 2^n. (This is "the birthday paradox").

Theorem 3.7 *It is possible to distinguish a random permutation from a permutation ψ^k with a high probability when m is of order 2^n. (k is fixed here, the number of oracle gates is limited by m, but the number of computations to analyse these m values is not limited).*

Idea of the proof

There are a lot of different ways to prove this theorem 3.7. The simplest is perhaps to see that it is a consequence a Shannon's theorem : the secret key should be at least as great as that of the known plaintext.
It is possible to use this theorem here because we suppose that there is no limit on the amount of computation that a circuit can do to analyse its m values.
Then, if real random functions $f_1, \ldots, f_k$ of F_n are the secret key, the length of the key is about $k.n.2^n$ bits. And with m oracle gates, $m.2n$ bits will be known.
So if $m > \frac{k.2^n}{2}$, it is possible to find a circuit ϕ with m normal oracle gates such that $|P_1 - P_1^{**}|$ is not negligible. (But ϕ will eventually do a lot of computations).

Theorem 3.8 *If m, n and k are ≥ 2, then $|P_1 - P_1^*|_{\max} \neq 0$ and $|P_1 - P_1^{**}|_{\max} \neq 0$.*
This a consequence of theorem 3.4 and of the values that we have found for $m = 2$ in paragraph 2.

Conclusion

When m is small compared to $\sqrt{2^n}$, and $k \geq 3$, Luby and Rackoff's property shows that it is not possible to distinguish a permutation ψ^k from a random function (or a random permutation) with m normal oracle gates and with a high probability. But when m is of order 2^n, it is possible to distinguish a permutation ψ^k from a random permutation and from a random function, and to distinguish a random permutation from a random function.
So the problem is now : what will happen when m is between $\sqrt{2^n}$ and 2^n ? This is what we will try to see now.

4 ψ^3 and ψ^4 when $m \geq 0(2^{\frac{n}{2}})$

We will see that when $m \geq 0(2^{\frac{n}{2}})$, it is possible to distinguish the permutations ψ^3 and ψ^4 from random permutations.

Proof for ψ^3

Let ϕ be the following distinguishing circuit : ϕ will analyse a function f of F_{2n} like this :

1. ϕ chooses m distinct $R_i, 1 \leq i \leq m$, and chooses m values L_i arbitrarily in I_n, $1 \leq i \leq m$.
2. ϕ asks for the values $[S_i, T_i] = f([L_i, R_i]), 1 \leq i \leq m$.
3. ϕ counts the number N of equalities of the form $R_i \oplus S_i = R_j \oplus S_j, i < j$.
4. Let N_0 be the expectation of N when f is a random permutation, and N_1 be the expectation of N when f is a $\psi^3(f_1, f_2, f_3)$.
   Then $N_1 \simeq 2N_0$, because when f is a $\psi^3(f_1, f_2, f_3)$, $R_i \oplus S_i = f_2(L_i \oplus f_1(R_i))$ so $f_2(L_i \oplus f_1(R_i)) = f_2(L_j \oplus f_1(R_j)), i < j$, if $L_i \oplus f_1(R_i) \neq L_j \oplus f_1(R_j)$ and $f_2(L_i \oplus f_1(R_i)) = f_2(L_j \oplus f_1(R_j))$ or if $L_i \oplus f_1(R_i) = L_j \oplus f_1(R_j)$.

So if ϕ gives 1 as output when N is closer to N_1 and 0 as output when N is closer to N_0, ϕ will have a $|P_1 - P_1^{**}|$ close to 1 when N_0 is greater than 1, that is to say when $m \geq 0(2^{\frac{n}{2}})$.

Conclusion : For ψ^3, there is a converse to Luby-Rackoff's property. It is possible to distinguish with a good probability the permutations ψ^3 from random permutations with m oracle gates, if and only if m is of order $\sqrt{2^n}$.

Notice also that here the m values $[R_i, L_i]$ chosen can be chosen randomly in I_n. In terms of cryptography this means that it is possible to use a "known plaintext attack" (we don't have to use a "chosen plaintext attack").

Proof for ψ^4

This time, we take $R_i = 0$ (or R_i constant), and we count the number N of equalities of the form $S_i \oplus L_i = S_j \oplus L_j$, $i < j$. In fact, when $f = \psi(f_1, f_2, f_3, f_4)$, then $S_i \oplus L_i = f_3(f_2(L_i \oplus f_1(0))) \oplus f_1(0)$. So the probability of such an equality is about the double in this case than in the case where f is a random permutation (because if $f_2(L_i \oplus f_1(0)) = f_2(L_j \oplus f_1(0))$ this equality holds, and if $\beta_i = f_2(L_i \oplus f_1(0)) \neq f_2(L_j \oplus f_1(0)) = \beta_j$ but $f_3(\beta_i) = f_3(\beta_j)$, this equality also holds).

Conclusion : For ψ^4, as for ψ^3, there is a converse to Luby-Rackoff's property.
It is possible to distinguish with a good probability the permutations ψ^3 and ψ^4 from random permutations with m oracle gates, if and only if m is of order $\sqrt{2^n}$. We will see that this will not be true for $\psi^k, k \geq 5$.

Notice that for ψ^4 we have used a "chosen plaintext attack" (because all the R_i are constant). And it is possible to prove that this is necessary if m is of order $\sqrt{2^n}$. (See [3]).

5 Properties of ψ^5 and ψ^6

For ψ^6, we have proved the following theorem. (See [3] for the demonstration).

Theorem 5.1 *For ψ^6 and for all super distinguishing circuit with m oracles gates, we have :* $|P_1 - P_1^{**}| \leq \frac{18m}{2^n} + \frac{12m^3}{2^{2n}}$.

The main idea in proving this theorem is to evaluate the number H of k-tuples of functions $(f_1, \ldots, f_k)$ such that : $\forall i, 1 \leq i \leq m, \psi^k(f_1, \ldots, f_k)[L_i, R_i] = [S_i, T_i]$. Here $k = 5$ or 6, the $[L_i, R_i], 1 \leq i \leq m$, are m pairwise distinct elements of I_{2n}, and the $[S_i, T_i], 1 \leq i \leq m$ are also m pairwise distinct elements of I_{2n}. ("Pairwise distinct" means that if $i \neq j$, then $L_i \neq L_j$ or $R_i \neq R_j$).(See [3] for a complete proof).

This theorem shows that it is not possible to distinguish with a good probability a random permutation from a permutation $\psi^k, k \geq 6$, if m is not at least of order $2^{\frac{2n}{3}}$. We will give in the next paragraph an exemple of an application of this result.

For ψ^5, we have just proved the following theorem.

Theorem 5.2 *For ψ^5 and for all normal distinguishing circuit with m oracles gates, $|P_1 - P_1^*|$ is negligible when n is large if m is not at least of order $2^{\frac{2n}{3}}$.*

Remark:
The theorems 5.1 and 5.2 show that ψ^5 and ψ^6 are really sensibly better permutation generators than ψ^3 and ψ^4. And we have strong presumption (see [3]) that the properties of ψ^5 and ψ^6 are even better.
For example, it is probable that this conjecture holds :

Conjecture
For ψ^5, or perhaps ψ^6 or ψ^7, and for any distinguishing circuit with m oracle gates we have : $|P_1 - P_1^*| \leq \frac{30m}{2^n}$. (The number 30 is just an example).
If this conjecture is true (and it is probably true), it shows that in fact when $k \geq 5$, m should be of order 2^n to distinguish a permutation ψ^k from a random function (or a random permutation).

6 Example of application

We will now see an example given by J. Pieprzyk at the end of his talk at Eurocrypt'90.
This is just an example and there are a lot of different (and clever) ways to use the results on pseudorandom permutations. (In general a pseudorandom function generator is used and not real random functions as we will do). But this example is instructive, and this was the example that we had in mind when we decided to work in an improvement of the inequalities.

The problem

Suppose that you want to use the results in a direct way, that is to say with k real random functions $f_1, \ldots, f_k$ of F_n which are the secret key. Then your secret key will be $k.n.2^n$ bits long. And suppose that you want that the permutation $\psi(f_1, \ldots, f_k)$ is not distinguishable from a random permutation with a good probability for all distinguishing circuit with $m \leq 10^9$. Notice that if this property holds, then to distinguish $\psi(f_1, \ldots, f_k)$ from a random permutation with a good probability it is necessary to do at least 10^9 computations. Then, what will be the length of the secret key ?

• If you use Luby-Rackoff's property : for $\psi^3, |P_1 - P_1^*| \leq \frac{m^2}{2^n}$, then since $m \simeq 2^{30}$, you will take $n \simeq 64$, so the length of the key is $3.64.2^{64}$ bits. This is of course too much !

• If you use Pieprzyk's property : $\psi(f, f, f, f^2)$ is pseudorandom, then you will divided "at best" the length of the key by 3, and the length is of course still too much. (We say "at best" because in fact the inequality of $|P_1 - P_1^*|$ is worse in this case : see the paragraph 7).

• If you use our property for ψ^6 : $|P_1 - P_1^*| \leq \frac{12m}{2^n} + \frac{18m^3}{2^{2n}}$, then since $m \simeq 2^{30}$, you will take $n \simeq 48$, so the length of the key is $6.48.2^{48}$ bits. This is still too much ! But ... we have divided the length of the key by 40000.

• And in fact, if the conjecture of paragraph 5 is true, it is probably possible to take $n \simeq 32$ for ψ^6.
Then the length of the key will be $6.32.2^{32}$ bits. Of course this is still a lot, but because of Shannon's theorem there is no hope to reduce the length of the key by much more (if you are considering that the distinguishing circuits are not limited in the amount of computation that they can perform to analyse their m values).

7 Remark for $\psi(f, f, f, f^2)$

When f is a random function of F_n, $\psi(f, f, f, f^2)$ is a pseudo random permutation of B_{2n}. But there is a little mistake in one of the the proofs of J. Pieprzyk : his lemma 4.1 page 145 of [4] is wrong. (And then the inequality obtained for this generator is worse).
For example, let ϕ be this normal distinguishing circuit, which has only one oracle gate. ϕ will test like this a function F of $I_{2n} \to I_{2n}$.

1. ϕ chooses an element R of I_n (for example $R = 0$) and take $L = 0$.
2. ϕ asks for the value $F[0, R] = [S, T]$.
3. If $R = S = T$, then ϕ gives the output 1. If not, ϕ gives the output 0.

Evaluation of $P_1 = P_r[C_{2n}(\psi(f, f, f, f^2))]$. (This is the notation of J. Piepzryk).
If $F = \psi(f, f, f, f^2)$, we have : $\begin{cases} S = f(R) \oplus f(R \oplus f^2(R)) \\ T = R \oplus f^2(R) \oplus f^2(S). \end{cases}$

P_1 is the probability that $R = S = T$ when f is randomly chosen in F_n.
But here (this will not be the case for $\psi^4(f,f,f,g)$) if $R = S$ we will have necessarily $T = R$.
So $P_1 = \frac{1}{2^n}$.

Evaluation of $Q_1 = P_r[C_{2n}(\psi(f,f,f,g))]$ (This is the notation of J. Pieptryk).
If $F = \psi(f,f,f,g)$, we have : $\begin{cases} S = f(R) \oplus f(R \oplus f^2(R)) \\ T = R \oplus f^2(R) \oplus g(S). \end{cases}$

Q_1 is the probability that $R = S = T$ when f and g are randomly and independently chosen in F_n.
So $Q_1 = \frac{1}{2^{2n}}$.
Then, $|P_1 - Q_1| = \frac{1}{2^n} - \frac{1}{4^n}$, which is not smaller than $\frac{9}{4^n}$ for all n, as was mentioned in lemma 4.1. of [4].
An other problem of $\psi(f,f,f,f^2)$ is that this generator is not super pseudo random. (see [3]).

8 Conclusion

We have seen that ψ^k, for $k \geq 5$, is an "exponentially" better pseudorandom permutation generator than ψ^3 and ψ^4. This improvement of the properties of ψ^k when $k \geq 5$ is a new result, and it holds for small values of m as for great values of m.

References

[1] M. Luby and Ch. Rackoff, *How to construct pseudorandom permutations from pseudorandom functions*, SIAM Journal and Computing, 17(2) : 373-386, April 1988.

[2] J. Patarin, *Pseudorandom permutations based on the DES Scheme*, Proceedings of EUROCODE'90.

[3] J. Patarin, *Etude des générateurs de permutations basés sur le Schéma du D.E.S.*, Thèse. To be publish in September 1991, INRIA, Domaine de Voluceau, Le Chesnay, France.

[4] J. Pieprzyk, *How to construct pseudorandom permutations from Single Pseudorandom Functions*, EUROCRYPT'90, Århus, Denmark, May 1990.

[5] Y. Zheng, T. Matsumoto and H. Imai, *Impossiblility and optimality results on constructing pseudorandom permutations*, Abstract of EUROCRYPT'89, Houthalen, Belgium, April 1989.