# HOW TO CONSTRUCT PSEUDORANDOM AND SUPER PSEUDORANDOM PERMUTATIONS FROM ONE SINGLE PSEUDORANDOM FUNCTION

Jacques PATARIN
Bull CP8, 68 route de Versailles - B.P.45 - 78430 Louveciennes - France

**Abstract**

In this paper we will solve two open problems concerning pseudorandom permutations generators.

1. We will see that it is possible to obtain a pseudorandom permutation generator with only three rounds of DES - like permutation and a single pseudorandom function. This will solve an open problem of [6].
2. We will see that it is possible to obtain a super pseudorandom permutation generator with a single pseudorandom function. This will solve an open problem of [5]. For this we will use only four rounds of DES - like permutation.

For example, we will see that if $\zeta$ denotes the rotation of one bit, $\psi(f, f, f \circ \zeta \circ f)$ is a pseudorandom function generator. And $\psi(f, f, f, f \circ \zeta \circ f)$ is a super pseudorandom function generator.

Here the number of rounds used is optimal. It should be noted that here we introduce an important new idea in that we do not use a composition of $f$, $i$ times, but $f \circ \zeta \circ f$ for the last round, where $\zeta$ is a fixed and public function.

## 1 Introduction

In their important paper [1], M. Luby and C. Rackoff showed how to construct a pseudorandom permutation generator from a pseudorandom function generator and the application of three rounds of DES - like permutations. (This structure is notated as $\psi(f, g, h)$). Later, Zheng, Matsumoto and Imai [6] showed that it is impossible to make a pseudorandom permutation with some composition of a single pseudorandom function $f$ and three rounds of DES - like permutations, i.e. $\psi(f^i, f^j, f^k)$ is not pseudorandom for any $i, j, k$. At the end of their article, they raised two open problems :

R.A. Rueppel (Ed.): Advances in Cryptology - EUROCRYPT '92, LNCS 658, pp. 256-266, 1993.

a) Whether it is possible to use one single function $f$ to construct a pseudorandom permutation, by more than three applications of DES - like transformation.

b) Whether it is possible that $\psi(f,f,\hat{f})$ be a pseudorandom permutation, where $\hat{f}$ is constructed from $f$ with $\hat{f} \neq f^m$ for any $m \in \mathbb{N}$.

The problem a) was solve by J. Pieprzyk in [4] where he explains that $\psi(f,f,f,f^2)$ is a pseudorandom permutation (but not a super pseudorandom permutation as we will see).

But problem b) remained open. Recently, we have solved this problem b) and will explain our results in this paper.

Another open problem was :

c) How to construct super pseudorandom permutations from one single pseudorandom function.

This notion of super pseudorandomness was introduced by M. Luby and C. Rackoff. It means that the block cryptosystem is secure against a chosen plaintext / ciphertext attack. They said that $\psi(f,g,h,e)$ is super pseudorandom, where $f,g,h$, and $e$ are four independent pseudorandom functions. (A proof of this property is given in [3]).

If only one pseudorandom function is used, we (in [3]), and J. Pieprzyk and S. Sadeghiyan (in [5]), have independently found that $\psi(f,f,f,f^2)$ is not super pseudorandom. So an open problem is how to construct a super pseudorandom permutation from a single pseudorandom function. This problem c) is the second problem that we have solved.

# 2 Notations

The notation we use, is similar to [2] and [4].

- $I_n = \{0,1\}^n$ is the set of all $2^n$ binary strings of length $n$.
- 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 $b$.
- For $a,b \in I_n$, $a \oplus b$ stands for bit-by-bit exclusive- or of $a$ and $b$.
- $\circ$ is the composition of function.
- $f^2$ is $f \circ f$.
- The set of all functions from $I_n$ to $I_n$ is $F_n$. It consists of $|F_n| = 2^{n.2^n}$ elements.
- The set of all permutations from $I_n$ to $I_n$ is $B_n$, so $B_n \subset F_n$. And $|B_n| = (2^n)!$.
- Let $f$ be a function of $F_n$. Let $L, R, S$, and $T$ be elements of $I_n$. Then by definition $\psi(f_1)$ is the permutation from $I_{2n}$ to $I_{2n}$ such that :

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

- Let $f_1, f_2, \dots, f_k$, be $k$ functions of $F_n$. $\psi(f_1, \dots, f_k)$ is the permutation from $I_{2n}$ to $I_{2n}$ defined by :
$$\psi(f_1, \dots, f_k) = \psi(f_k) \circ \dots \circ \psi(f_2) \circ \psi(f_1).$$
For example, we have :
$$\psi(f_1, f_2, f_3)[L, R] = [S, T] \quad \Leftrightarrow \quad \left\{ \begin{array}{lcl} S & = & R \oplus f_2(L \oplus f_1(R)) \\ T & = & L \oplus f_1(R) \oplus f_3(S) \end{array} \right.$$
$$\psi(f_1, f_2, f_3, f_4)[L, R] = [S, T] \quad \Leftrightarrow \quad \left\{ \begin{array}{lcl} S & = & L \oplus f_1(R) \oplus f_3(R \oplus f_2(L \oplus f_1(R))) \\ T & = & R \oplus f_2(L \oplus f_1(R)) \oplus f_4(S) \end{array} \right.$$

### Remark :

$\psi(f_1, \dots, f_k)$ is in fact a $k$ iteration DES Scheme where the S-boxes are replaced by the functions $f_1, \dots, f_k$.

We will assume that the definitions of permutation generator, distinguishing circuit, normal and inverse oracle gates, pseudorandom permutation generator and super pseudorandom permutation generator are known. These definitions, may be found in [1] for example.
In all this article the number of computations that can perform a distinguishing circuit is not bounded. But the number of oracle gates of a distinguishing circuit is a fixed integer $m$.

## 3 Definition of the "spreading" of a permutation $\zeta$

To explain the results that we obtained, we will need to define the notion of the "spreading" of a permutation. This notion will be useful to formulate our results in general.

**Definition 1** *Let $\zeta$ be a permutation of $I_n$. (Then, $\zeta \in B_n$). By definition, the "spreading" of $\zeta$ is the smallest integer $\lambda$ such that :*
*$\forall L \in I_n$, the equation $x \oplus \zeta(x) = L$ has at most $\lambda$ solutions in $I_n$.*

### Examples

1. If $\zeta$ is the identity function, then $\lambda = 2^n$. This is because for $L = 0$ the equation $x \oplus x = L$ has $2^n$ solutions.

2. Let $\zeta$ be the rotation of one bit, such that the first bit becomes the second bit, the second bit the third, ..., and the last bit becomes the first bit.

So if $x = x_1 x_2 \dots x_n$, where $x \in I_n$, $\zeta(x) = x_n x_1 x_2 \dots x_{n-1}$.

Then we will see that $\lambda = 2$.
Let $L = \ell_1 \ell_2 \dots \ell_n$.

Then $x \oplus \zeta(x) = L$ if and only if : $\left\{ \begin{array}{lcl} x_1 & \oplus & x_n = \ell_1 \\ x_2 & \oplus & x_1 = \ell_2 \\ & \vdots & \\ x_n & \oplus & x_{n-1} = \ell_n \end{array} \right.$ $(I)$

where $\forall i, 1 \leq i \leq n, \ell_i = 0$ or 1, and $x_i = 0$ or 1.

## First case : $x_n = 0$

Then the $(n-1)$ first equations of (I) give us $x_1, x_2, \ldots, x_{n-1}$. And then if $\ell_n = x_n \oplus x_{n-1}$ the last equation is true. If not, $x_n = 0$ is not possible.

## Second case : $x_n = 1$

In the same way, the system (I) then has zero or one solution if $x_n = 1$.

## Conclusion :

Let $\zeta$ be the rotation of one bit. Then we have seen that for all $L \in I_n$, the equation $x \oplus \zeta(x) = L$ has at most two solutions. (And for $L = 0$ it has exactly two solutions). So the "spreading" of the function rotation of one bit is $\lambda = 2$, as claimed.

## Remark :

It is possible to find some permutations with $\lambda = 1$. As pointed out by Mr Lothrop Mittenthal after my presentation of this paper, in this case a permutation $\zeta$ is call "Complete Mappings". Complete Mappings have been studied for differents raisons before, and more details about them are given in [7].

In this paper, we will present two theorems that will use our notion of "spreading". These theorems are :

**Theorem 3.1** *Let $\zeta = (\zeta_n)_{n \in N}$ be a sequence of permutations, $\zeta_n \in B_n$.
Let $\lambda_n$ be the spreading of $\zeta_n$.
If for all polynomial $P(n)$ we have :*

$$\frac{\lambda_n P(n)}{2^n} \quad \overrightarrow{n \rightarrow +\infty} \quad 0 \quad \textit{then :}$$

*$\psi(f, f, f \circ \zeta \circ f)$ is a pseudo-random function generator, where $f$ is a single pseudo-random function.
(When $f \in F_n$, the notation $f \circ \zeta \circ f$ means $f \circ \zeta_n \circ f$).*

**Theorem 3.2** *With the same notations, and the same condition on $\zeta$, we have :
$\psi(f, f, f, f \circ \zeta \circ f)$ is a super pseudo-random function generator.*

These two theorems solve the two open problems b) and c) discussed in paragraph 1. Theorem 3.1. solves problem b) and Theorem 3.2 solves problem c).

For example, if $\zeta$ is the function rotation of one bit, $\lambda_n = 2$ and by Theorem 3.2 we have found a super pseudorandom permutation generator by using only one single pseudorandom function $f$. Moreover we have found many of these super pseudorandom permutation generators :
each $\zeta$ such that $\frac{\lambda_n P(n)}{2^n} \overset{\longrightarrow}{n \to +\infty} 0$ (for all polynomial $P(n)$) will give us such a generator.

We will now see the ideas that we have used to prove these two new theorems. Paragraphs 4 and 5 discuss about theorem 3.1, and paragraph 6 and 7 will deal with theorem 3.2. And in paragraph 8 we will compare our results with one single pseudorandom function with what can be obtained with two pseudorandom functions.

## 4 A "basic property" of $\psi(f, f, f \circ \zeta \circ f)$

To prove Theorem 3.1, we have first proved a "basic property" of $\psi(f, f, f \circ \zeta \circ f)$.

**Theorem 4.1** *Basic property of $\psi(f, f, f \circ \zeta \circ f)$.*

*Let $\zeta$ be a permutation of $I_n$. Let $\lambda$ be the spreading of $\zeta$.*
*Let $[L_i, R_i], 1 \leq i \leq m$, be a sequence of m distinct elements of $I_{2n}$. (Distinct means that $i \neq j \Rightarrow R_i \neq R_j$ or $L_i \neq L_j$).*
*And let $[S_i, T_i], 1 \leq i \leq m$, be a sequence of m distinct elements of $I_{2n}$ such that if $i \neq j$, then $S_i \neq S_j$.*
*Then the number $H$ of functions $f$ of $F_n$ such that*

$$\forall i, 1 \leq i \leq m, \psi(f, f, f \circ \zeta \circ f)[L_i, R_i] = [S_i, T_i]$$

*is* $H \geq \frac{|F_n|}{2^{2nm}} \left(1 - \frac{6m^2}{2^n} - \frac{\lambda m}{2^n}\right)$.

The proof of this theorem 4.1 is not very difficult : it is just a combinatorial evaluation. In [3] a complete proof of this Theorem is given.

## 5 $\psi(f, f, f \circ \zeta \circ f)$ is pseudorandom, if $\zeta$ is well chosen

Let $\phi$ be a distinguishing circuit.

- We will denote by $\phi(F)$ its output (1 or 0) when its oracle gates are given the values of a function $F$.
  Let $\zeta$ be a fixed permutation.
- We will denote by $P_1$ the probability that $\phi(F) = 1$ when $f$ is a function randomly chosen in $F_n$, and $F = \psi(f, f, f \circ \zeta \circ f)$.

  So $P_1 = \frac{\text{Number of } f \in F_n \text{ such that } \phi(\psi(f, f, f \circ \zeta \circ f)) = 1}{|F_n|}$.

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

So $P_1^* = \dfrac{\text{Number of function } F \in F_{2n} \text{ such that } \phi(F) = 1}{|F_{2n}|}$.

From Theorem 4.1, it is possible to prove this theorem :

**Theorem 5.1** *For every distinguishing circuit $\phi$ with $m$ oracle gates, we have :*

$$|P_1 - P_1^*| \leq \frac{6m^2}{2^n} + \frac{\lambda m}{2^n} + \frac{m(m-1)}{2.2^n},$$

*where $\lambda$ is the spreading of $\zeta$.*
*And then : $|P_1 - P_1^*| \leq \dfrac{6.5m^2}{2^n} + \dfrac{\lambda m}{2^n}$.*

(See [3] for the complete proof).In the APPENDIX we will give a general result (Theorem A1) which shows that Theorem 5.1 is just a consequence of Theorem 4.1.
And theorem 3.1 is an easy consequence of this theorem 5.1.

## Remarks

1. Let $Q_1$ be the probability that $\phi(F) = 1$ when $f, g, h$ are three independant functions randomly chosen in $F_n$ and $F = \psi(f, g, h)$. Then, in [1] M. Luby et C. Rackoff have proved that : for every distinguishing circuit $\phi$ whith $m$ oracle gates, we have :
   $|Q_1 - P_1^*| \leq \dfrac{m^2}{2^n}$.
   It is useful to compare this property with our property of theorem 5.1 :
   $|P_1 - P_1^*| \leq \dfrac{6.5m^2}{2^n} + \dfrac{\lambda m}{2^n}$.
   In theorem 5.1 the inequality is a little worse, but the important thing is that we use only one function $f$ randomly chosen in $F_n$. When these theorems are used in order to obtain a cryptosystem, the functions $f$,$g$,$h$ will generally be generated by a pseudorandom functions generator. So by using $\psi(f, f, f \circ \zeta \circ f)$ instead of $\psi(f, g, h)$ the lenght of the secret key will generaly be divided by three (because we need to generate only one pseudorandom function instead of three).

2. Theorem 5.1 is true because it concerns a distinguishing circuit. These circuits have only normal oracle gate. If we use super distinguishing circuit, with normal and inverse oracle gates, then the property of theorem 5.1 will not be true. This is because here we use only three rounds of DES - like permutations. And in [1] M. Luby and C. Rackoff have proved that in this case a generator is never super pseudorandom.

# 6 A basic "property" of $\psi(f, f, f, f \circ \zeta \circ f)$

We will now present the ideas that we have used to prove Theorem 3.2. The proof is very similar to the proof of theorem 3.1. First, we proved this theorem :

**Theorem 6.1** *basic property of $\psi(f,f,f,f\circ\zeta\circ f)$.*

*Let $\zeta$ be a permutation of $I_n$. Let $\lambda$ be the spreading of $\zeta$.
Let $[L_i,R_i], 1\leq i\leq m$, be a sequence of $m$ distinct elements of $I_{2n}$. (Distinct means that $i\neq j\Rightarrow R_i\neq R_j$ or $L_i\neq L_j$).
Let $[S_i,T_i], 1\leq i\leq m$, be also a sequence of $m$ distinct elements of $I_{2n}$. (Distinct means that $i\neq j\Rightarrow S_i\neq S_j$ or $T_i\neq T_j$).
Then the number $H$ of functions $f$ of $F_n$ such that*

$$\forall i, 1\leq i\leq m, \psi(f,f,f,f\circ\zeta\circ f)[L_i,R_i]=[S_i,T_i]$$

*is* $H\geq\dfrac{|F_n|}{2^{2nm}}\left(1-\dfrac{10.5m^2}{2^n}-\dfrac{\lambda m}{2^n}\right)$.

See [3] for the complete proof.

# 7 $\psi(f,f,f,f\circ\zeta\circ f)$ is super pseudorandom, if $\zeta$ is well chosen

Let $\zeta$ be a fixed and public permutation. (For example a rotation of one bit).
Let $\phi$ be a super distinguishing circuit. (This is a circuit with normal and inverse oracle gates. See [1] for precise definitions).

- We will denote by $\phi(F)$ its output (1 or 0) when its normal oracle gates are given the values of a permutation $F$, and its inverse oracle gates are given the values of $F^{-1}$.
- We will denote by $P_1$ the probability that $\phi(F)=1$ when $f$ is a function randomly chosen in $F_n$, and $F=\psi(f,f,f,f\circ\zeta\circ f)$.
- We will denote by $P_1^{**}$ the probability that $\phi(F)=1$ when $F$ is randomly chosen in $B_{2n}$.

From theorem 6.1, it is possible to prove this theorem :

**Theorem 7.1** *For every super distinguishing circuit $\phi$ with $m$ oracle gates, we have :*

$$|P_1-P_1^{**}|\leq\frac{10.5m^2}{2^n}+\frac{\lambda m}{2^n}+\frac{m(m-1)}{2.2^{2n}}.$$

*And then :*

$$|P_1-P_1^{**}|\leq\frac{11m^2}{2^n}+\frac{\lambda m}{2^n}.$$

(See [3] for the proof). In the APPENDIX we will give a general result (Theorem A2) which shows that Theorem 7.1 is just a consequence of Theorem 6.1.
And theorem 3.2 is an easy consequence of this theorem 7.1.

### Remark

If for $\zeta$ we take the identity function, then $\lambda = 2^n$ (see paragraph 3).
Then $\frac{\lambda P(n)}{2^n}$ does not tend to 0 for any polynomial $P$.
So the theorem 3.2 can not conclude in this case that $\psi(f, f, f, f^2)$ is super pseudorandom.
And in fact it is possible to show that $\psi(f, f, f, f^2)$ is not super pseudorandom.
(See [5] or [3]).

## 8 Generators with two functions

Although that it is not exactly the thema of this article, we will now briefly survey the properties of the generators with two independant functions $f$ and $g$ randomly chosen in $F_n$. All these properties can be proved with the "coefficient $H$ technique" which is given in Appendix. Most of these properties have been find before this article. With these properties we will then comment a result claimed in [5], and we will explain why we think that this result is wrong.

### The properties

1. $\psi(f, f, g)$ and $\psi(f, g, g)$ are pseudorandom, but not super pseudo-random. They are not super pseudo-random beacause here there is only three rounds.

2. $\psi(f, g, f)$ is not pseudorandom. This is easy to see because this permutation is its own inverse if left and right halves of inputs and outputs are swapped.

   **Remark** : These results on 1. and 2. have first been find by Ohnishi (see [6]).

3. $\psi(f, f, f, g)$ and $\psi(f, g, g, g)$ are super pseudorandom.

4. $\psi(f, f, g, g)$ is also super pseudorandom.

5. $\psi(f, g, g, f)$ is not pseudorandom. This is easy to see because this permutation is its own inverse if left and right halves are swapped.

6. $\psi(f, g, f, g)$ is super pseudorandom.

7. $\psi(f, f, g, f)$ and $\psi(f, g, f, f)$ are super pseudorandom.

Because of these results, we think that the "Corollary 1" of [5] is wrong.
This "Corollary 1" claim :

*Let $(f_1, f_2, \ldots, f_i)$ be $i$ functions of $F_n$ such that $G_1 = \psi(f_i, \ldots, f_1)$ be a pseudorandom permutation.*
*Then $G_1$ is super pseudorandom if and only if $G_2 = \psi(f_i, \ldots, f_2)$ and $G_3 = \psi(f_1, \ldots, f_{i-1})$ are pseudorandom permutations.*
But we have just seen that :

1. $\psi(f,f,f,g)$ is super pseudorandom and $\psi(f,f,f)$ is not pseudorandom.
2. $\psi(f,g,f,g)$ is super pseudorandom, but $\psi(f,g,f)$ and $\psi(g,f,g)$ are not pseudorandom. Notice here that $f_2$ and $f_{i-1}$ are independant.

So this is why we think that this "Corollary 1" of [5] is wrong.

# 9 Conclusion

In this paper we have explained the ideas that we have used to solve two open problems about pseudorandom permutation generators. We have presented a notion of "spreading" for a permutation, and this notion is very useful for our results. Another new idea was to use functions $f \circ \zeta \circ f$, where $\zeta$ is a fixed and public permutation with small "spreading", and $f$ a pseudorandom function.
Using this sort of function give us very different results from those obtained when using only compositions of $f$.
Our main result is that it is possible to construct super pseudorandom permutations from a single pseudorandom function. Such permutations give block cryptosystems secure against chosen plaintext / ciphertext attack. Finally, we have explained that there are many such permutations : any $\psi(f,f,f,f\circ\zeta\circ f)$, where $\zeta$ is a fixed and public permutation with small "spreading" will be a super pseudorandom permutation constructed from the pseudorandom function $f$. And here the number of rounds used (four) is also optimal.

# References

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

[2] J. Patarin, *New results on pseudorandom permutation generators based on the DES Scheme*, Abstracts of Crypto'91, p. 7-2, 7-7.

[3] J. Patarin, *Etude des générateurs de permutations basés sut le schéma du DES*, Thèse, November 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] B. Sadeghiyan and J. Pieprzyk, *On necessary and sufficient conditions for the construction of super pseudorandom permutations*, Abstracts of Asiacrypt'91, November 1991, p. 117-123.

[6] Y. Zheng, T. Matsumoto and H. Imai, *Impossiblility and optimality results on constructing pseudorandom permutations*, Abstract of EUROCRYPT'89, Houthalen, Belgium, April 1989, p. 412-421.

[7] L. J. Paige, *Complete Mappings of finite groups*, J. Math. 1, 111-116, 1951.

# APPENDIX

## The "coefficients $H$ technique" for proving pseudorandomness and super-pseudorandomness

We will formulate here the two main Theorems that we generally used in order to prove some pseudorandom or super-pseudorandom properties.
These theorems show a technique (we call it the "coefficient $H$ technique") for proving such properties. More details and variants of these technique (some generalisations exist) are given in [3] with the proof of these theorems.

### Theorem A1 ("coefficient $H$ technique for pseudorandomness")

*Let $\Lambda$ be a pseudorandom permutation generator such that if $(f_1,\ldots,f_p)$ are $p$ functions of $F_n$, $\Lambda(f_1,\ldots,f_p) \in B_{2n}$.*
*Let $\alpha$ be a real, $\alpha > 0$.*
*If :*

*(1) For all sequence $[L_i, R_i], 1 \leq i \leq m$, of $m$ distinct elements of $I_{2n}$ (distinct means that $i \neq j \Rightarrow R_i \neq R_j$ or $L_i \neq L_j$) and for all sequences $[S_i, T_i], 1 \leq i \leq m$, of $m$ elements of $I_{2n}$ such that if $i \neq j$ then $S_i \neq S_j$, we have :*
*the number $H$ of $p$-tuple of functions $(f_1,\ldots,f_p)$ such that*

$$\forall i, 1 \leq i \leq m, \Lambda(f_1,\ldots,f_p)[L_i,R_i] = [S_i,T_i]$$

*is $H \geq \dfrac{|F_n|^p}{2^{2nm}}(1-\alpha)$.*

*Then :*

*(2) For all distinguishing circuit $\phi$ with $m$ oracle gates, we have :*

$$|P_1 - P_1^*| \leq \alpha + \frac{m(m-1)}{2.2^n}.$$

*Where $P_1$ is the probability that $\phi(F) = 1$ when $F = \Lambda(f_1,\ldots,f_p)$ and $(f_1,\ldots,f_p)$ are $p$ functions randomly (and independantly) chosen in $F_n$.*
*And $P_1^*$ is the probability that $\phi(F) = 1$ when $F$ is randomly chosen in $F_{2n}$.*

Notice that here there is no limitation in the number of computations that can perform the distinguishing circuits in order to analyse the $m$ values given by its oracle gates.

### Example

With this Theorem A1 we can obtain a new proof of the result of M. Luby and C. Rackoff about $\psi^3(f_1,f_2,f_3)$, for example.
First, it is possible to prove this property :

## Property of $\psi(f_1, f_2, f_3)$

*For all sequence $[L_i, R_i], 1 \leq i \leq m$, of $m$ distinct elements of $I_{2n}$ and for all sequence $[S_i, T_i], 1 \leq i \leq m$, of $m$ elements of $I_{2n}$ such that if $i \neq j$ then $S_i \neq S_j$, we have :*
*the number $H$ of 3-tuple of functions $(f_1, f_2, f_3)$ such that*

$$\forall i, 1 \leq i \leq m, \psi^3(f_1, f_2, f_3)[L_i, R_i] = [S_i, T_i]$$

*is* $H \geq \frac{|F_n|^3}{2^{2nm}}\left(1 - \frac{m(m-1)}{2.2^n}\right)$.
Then, from Theorem A1 we obtain :

$$|P_1 - P_1^*| \leq \frac{m(m-1)}{2^n} \quad \text{as claimed.}$$

## Theorem A2 ("coefficient $H$ technique for super-pseudorandomness")

*If :*

*(1) For all sequence $[L_i, R_i], 1 \leq i \leq m$, of $m$ distinct elements of $I_{2n}$, and for all sequences $[S_i, T_i], 1 \leq i \leq m$, of $m$ distinct elements of $I_{2n}$ the number $H$ of p-tuple of functions $(f_1, \ldots, f_p)$ such that*

$$\forall i, 1 \leq i \leq m, \Lambda(f_1, \ldots, f_p)[L_i, R_i] = [S_i, T_i]$$

*is* $H \geq \frac{|F_n|^p}{2^{2nm}}(1 - \alpha)$.

*Then :*

*(2) For all super distinguishing circuit $\phi$ with $m$ super oracle gates (normals or inverses), we have :*

$$|P_1 - P_1^{**}| \leq \alpha + \frac{m(m-1)}{2.2^{2n}}.$$

*Where $P_1$ is the probability that $\phi(F) = 1$ when $F = \Lambda(f_1, \ldots, f_p)$ and $(f_1, \ldots, f_p)$ are randomly (and independantly) chosen in $F_n$.*
*And $P_1^{**}$ is the probability that $\phi(F) = 1$ when $F$ is randomly chosen in $B_{2n}$.*

Notice that here there is also no limitation in the number of computations that can perform the super distinguishing circuits in order to analyse the $m$ values given by its super oracle gates.