The "Coefficients H" Technique

Jacques Patarin

Université de Versailles
45 avenue des Etats-Unis, 78035 Versailles Cedex, France
jacques.patarin@prism.uvsq.fr

Abstract. The "coefficient H technique" is a tool introduced in 1991 and used to prove various pseudo-random properties from the distribution of the number of keys that sends cleartext on some ciphertext. It can also be used to find attacks on cryptographic designs. We can like this unify a lot of various pseudo-random results obtained by different authors. In this paper we will present this technique and we will give some examples of results obtained.

1 Introduction

The "coefficient H technique" was introduced in 1990 and 1991 in [11], [12]. Since then, it has been used many times (by myself , Henri Gilbert, Gilles Piret, Serge Vaudenay, etc.) to prove various results on pseudo-random functions and pseudo-random permutations. In this paper we will present in a self content way the "coefficient H technique", with different formulations when we study different cryptographic attacks (known plaintext attacks, chosen plaintext attacks, etc.). We will give proofs of some of these theorems and we will give some simple examples.

2 Notation - Definition of H

In all this paper, we will use these notations.

- KPA: Known Plaintext Attack
- CPA-1: Non-adaptive Chosen Plaintext Attack
- CPA-2: Adaptive Chosen Plaintext Attack
- CPCA-1: Non-adaptive Chosen Plaintext and Chosen Ciphertext Attack
- CPCA-2: Adaptive Chosen Plaintext and Chosen Ciphertext Attack
- $I_N = \{0,1\}^N$ (N is any integer)
- F_N will be the set of all applications from I_N to I_N
- B_N will be the set of all permutations from I_N to I_N
- ψ^k will denote the Feistel scheme of F_{2n} with k rounds with k random round functions randomly chosen in F_n (n is any integer). ψ^k is also called a random Feistel scheme or a Luby-Rackoff construction.
- $a \in_R A$ means that a is randomly chosen in A with a uniform distribution

R. Avanzi, L. Keliher, and F. Sica (Eds.): SAC 2008, LNCS 5381, pp. 328–345, 2009.

- K will denote a set of values that we will sometimes call "keys". In this paper we will consider that K is a set of k-uples of functions $(f_1, \ldots, f_k)$ of F_n. (However generally only $|K|$ will be important, not the nature of the elements of K).
- G is an application of $K \to F_N$. (Therefore, G is a way to design a function of F_N from k-uples $(f_1, \ldots, f_k)$ of functions of F_n of K).

Let m be an integer (m will be the number of queries). Let $a = (a_i)_{1 \le i \le m}$ be a sequence of pairwise distinct elements of I_N. Let $b = (b_i)_{1 \le i \le m}$ be a sequence of elements of I_N. By definition, we will denote by $H(a, b)$ or simply by H if the context of the a_i and b_i is clear, the number of $(f_1, \ldots, f_k) \in K$ such that:

$$\forall i,\ 1 \le i \le m,\ G(f_1, \ldots, f_k)(a_i) = b_i$$

Therefore, H is the number of "keys" (i.e. elements of K) that send all the a_i inputs to the exact values b_i.

3 Five Basic "coefficient H" Theorems

In this section we will formulate five theorems. These theorems are the basis of a general proof technique called the "coefficient H technique", that allows to prove security results for function generators and permutation generators (and thus applies for random and pseudo-random Feistel ciphers).

These theorems were mentioned in [12] (with proofs in french) and in [16]. Since no proof in english was easily available so far we will present in this paper, in Appendices, a proof of some of these theorems.

Theorem 1. [Coefficient H technique, sufficient condition for security against KPA] *Let α and β be real numbers, $\alpha > 0$ and $\beta > 0$. If:*

(1) *For random values $a_i, b_i,\ 1 \le i \le m$ of I_N such that the a_i are pairwise distinct, with probability $\ge 1 - \beta$ we have:*

$$H \ge \frac{|K|}{2^{Nm}}(1 - \alpha)$$

Then

(2) *For every KPA with m (random) known plaintexts we have: $Adv^{KPA} \le \alpha + \beta$, where Adv^{KPA} denotes the advantage to distinguish $G(f_1, \ldots, f_k)$ when $(f_1, \ldots, f_k) \in_R K$ from a function $f \in_R F_N$*

(By "advantage" we mean here, as usual, for a distinguisher the absolute value of the difference of the two probabilities to output 1).

Theorem 2. [Coefficient H technique, sufficient condition for security against CPA-1] *Let α and β be real numbers, $\alpha > 0$ and $\beta > 0$. If:*

(1) *For all sequences $a = (a_i)$, $1 \leq i \leq m$ of m pairwise distinct elements of I_N there exists a subset $E(a)$ of I_N^m such that $|E(a)| \geq (1-\beta) \cdot 2^{Nm}$ and such that for all sequences $b = (b_i)$, $1 \leq i \leq m$ of $E(a)$ we have:*

$$H \geq \frac{|K|}{2^{Nm}}(1-\alpha)$$

Then

(2) *For every CPA-1 with m chosen plaintexts we have: $Adv^{PRF} \leq \alpha + \beta$ where Adv^{PRF} denotes the advantage to distinguish $G(f_1, \ldots, f_k)$ when $(f_1, \ldots, f_k) \in_R K$ from a function $f \in_R F_N$.*

Theorem 3. [Coefficient H technique, sufficient condition for security against CPA-2] *Let α and β be real numbers, $\alpha > 0$ and $\beta > 0$. Let E be a subset of I_N^m such that $|E| \geq (1-\beta) \cdot 2^{Nm}$.*

If:

(1) *For all sequences a_i, $1 \leq i \leq m$, of pairwise distinct elements of I_N and for all sequences b_i, $1 \leq i \leq m$, of E we have:*

$$H \geq \frac{|K|}{2^{Nm}}(1-\alpha)$$

Then

(2) *For every CPA-2 with m chosen plaintexts we have: $Adv^{PRF} \leq \alpha + \beta$ where Adv^{PRF} denotes the probability to distinguish $G(f_1, \ldots, f_k)$ when $(f_1, \ldots, f_k) \in_R K$ from a function $f \in_R F_N$.*

Theorem 4. [Coefficient H technique, sufficient condition for security against CPCA-2] *Let α be a real number, $\alpha > 0$. If:*

(1) *For all sequences of pairwise distinct elements a_i, $1 \leq i \leq m$, and for all sequences of pairwise distinct elements b_i, $1 \leq i \leq m$, we have:*

$$H \geq \frac{|K|}{2^{Nm}}(1-\alpha)$$

Then

(2) *For every CPCA-2 with m chosen plaintexts we have: $Adv^{PRF} \leq \alpha + \frac{m(m-1)}{2 \cdot 2^N}$ where Adv^{PRF} denotes the probability to distinguish $G(f_1, \ldots, f_k)$ when $(f_1, \ldots, f_k) \in_R K$ from a function $f \in_R B_N$.*

Theorem 5. [Coefficient H technique, a more general sufficient condition for security against CPCA-2]

Let α and β be real numbers, $\alpha > 0$ and $\beta > 0$

If there exists a subset E of $(I_N^m)2$ such that

(1a) *For all $(a, b) \in E$, we have:*

$$H \geq \frac{|K|}{2^{Nm}}(1-\alpha)$$

(1b) *For all CPCA-2 acting on a random permutation f of B_N, the probability that $(a, b) \in E$ is $\geq 1 - \beta$ where (a, b) denotes here the successive $b_i = f(a_i)$ or $a_i = f^{-1}(b_i)$, $1 \leq i \leq m$ that will appear.*
Then

(2) *For every CPCA-2 with m chosen plaintexts we have: $Adv^{PRF} \leq \alpha + \beta$ where Adv^{PRF} denotes the probability to distinguish $G(f_1, \ldots, f_k)$ when $(f_1, \ldots, f_k) \in_R K$ from a function $f \in_R B_N$.*

Remark. There are a lot of variants, and generalizations of these theorems. For example, in all these theorems 1, 2, 3, 4, 5, the results are also true if we change $H \geq \frac{|K|}{2^{Nm}}(1 - \alpha)$ by $H \leq \frac{|K|}{2^{Nm}}(1 + \alpha)$. However, for cryptographic uses $H \geq$ is much more practical since often it will be easier to evaluate the exceptions where H is $\ll$ average than the exceptions when H is $\gg$ average.

4 How to Use the "Coefficient H Technique"

We have used the "coefficient H technique" to obtain proofs of security (cf sections 5 and 6 below), generic attacks (cf section 7 below) and to obtain new cryptographic designs (cf section 8 below). For proofs of security, very often, the aim is to prove that a cryptographic construction A is not distinguishable from an ideal object B. For example, in the Luby-Rackoff original result of [6], A is a 3 or 4 round Feistel scheme with round functions generated from a small key k by a pseudo-random function generator, and B is a perfectly random permutation. For the proof, we introduce another ideal construction C, where all the pseudorandom functions are replaced by truly random functions (or other pseudo-random objects are replaced by truly random ones). Now the idea is that

$$Adv(A \to B) \leq Adv(A \to C) + Adv(C \to B)$$

i.e. the advantage to distinguish A from B is always smaller or equal to the advantage to distinguish A from C plus the advantage to distinguish C from B. To prove that $Adv(A \to C)$ is small is generally very easy: it comes from the hypothesis that the function generator is secure, for example. To prove that $Adv(C \to B)$ is small is sometimes more difficult. However, in A the only secret values are generally contained in a small secret cryptographic k (of 128 bits for example) while in C the secret values are much bigger since they are generally truly random secret functions. The "coefficient H" technique is very often a powerful tool to get a proof that $Adv(C \to B)$ is small (and therefore that $Adv(A \to B)$ is small, as wanted since $Adv(A \to C)$ is small). For this, we "just" have to compute some values H, as stated in Theorem 1,2,3,4,5. When the computations of these values H are easy, the proofs will be easy. (Very often these values are easy to compute when we are below a "birthday bound value", i.e. when the analysis of collisions in equations are easy since the probability to get such collisions is small). However, sometimes, the computations of the values

H are not easy. For these cases, I have developed two techniques of computations that I have called H_w and H_σ techniques.

H_w Technique

H_w stands for H "worst case" technique. The set of parameters on which we want to compute H is generally fixed from the beginning. For these computations, I sometimes use the "Theorem $P_i \oplus P_j$" (or variants of it) that I will present below. (See section 6.1 for an example of this technique).

H_σ Technique

H_σ stands for H "standard deviation" technique. The set of parameters on which we want to compute H is not fixed from the beginning, but it will automatically be fixed from the computation of the standard deviation of H. We will generally use the covariance formula to compute this standard deviation. (See section 6.2 for an example of this technique).

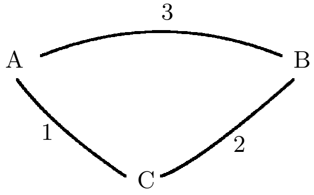

Fig. 1. Three cryptographic objects A,B,C

"Theorem $P_i \oplus P_j$"

The "Theorem $P_i \oplus P_j$" was proved in [17]. We use it sometimes to compute some difficult values H. Let us recall here what this theorem is.

Definition 1. *Let (A) be a set of equations $P_i \oplus P_j = \lambda_k$, with $P_i, P_j, \lambda_k \in I_n$. If by linearity from (A) we cannot generate an equation in only the λ_k, we will say that (A) has "no circle in P", or that the equations of (A) are "linearly independent in P".*

Let a be the number of equations in (A), and α be the number of variables P_i in (A). So we have parameters $\lambda_1, \lambda_2, \cdots, \lambda_a$ and $a + 1 \leq \alpha \leq 2a$.

Definition 2. *We will say that two indices i and j are "in the same block" if by linearity from the equations of (A) we can obtain $P_i \oplus P_j =$ an expression in $\lambda_1, \lambda_2, \cdots, \lambda_a$.*

Definition 3. *We will denote by ξ_{max} the maximum number of indices that are in the same block.*

Example 1. If $A = \{P_1 \oplus P_2 = \lambda_1, P_1 \oplus P_3 = \lambda_2, P_4 \oplus P_5 = \lambda_3\}$, here we have two blocks of indices $\{1, 2, 3\}$ and $\{4, 5\}$, and $\xi_{max} = 3$.

Definition 4. *For such a system (A), when $\lambda_1, \lambda_2, \cdots, \lambda_a$ are fixed, we will denote by h_α the number of $P_1, P_2, \cdots, P_\alpha$ solutions of (A) such that: $\forall i, j$, $i \neq j \Rightarrow P_i \neq P_j$. We will also denote $H_\alpha = 2^{na} h_\alpha$.*

Remark h_α and H_α are a concise notations for $h_\alpha(A)$ and $H_\alpha(A)$. For a given value α, h_α and H_α can have different values for different systems A.

Definition 5. *We will denote by J_α the number of $P_1, P_2, \cdots, P_\alpha$ in I_n such that: $\forall i, j$, $i \neq j \Rightarrow P_i \neq P_j$. So $J_\alpha = 2^n \cdot (2^n - 1) \cdots (2^n - \alpha + 1)$.*

Theorem 6 ("Theorem $P_i \oplus P_j$" when ξ_{max} is fixed). *Let ξ_{max} be a fixed integer, $\xi_{max} \geq 2$. Let (A) be a set of equations $P_i \oplus P_j = \lambda_k$ with no circle in P, with α variables P_i, such that:*

1. *We have no more than ξ_{max} indices in the same block.*
2. *The $\lambda_1, \lambda_2, \cdots, \lambda_k$ have any fixed values such that: for all i and j in the same block, $i \neq j$, the equation of $P_i \oplus P_j$ in $\lambda_1, \lambda_2, \cdots, \lambda_\alpha$ is $\neq 0$ (i.e. by linearity from (A) we cannot generate an equation $P_i = P_j$ with $i \neq j$).*

Then we have for sufficient large n: $H_\alpha \geq J_\alpha$. (This means: for all fixed ξ_{max}, there exists $n_0 \in \mathbb{N}$ such that, for all $n \geq n_0$, for all system A that satisfies 1. and 2., we have: $H_\alpha(A) \geq J_\alpha$).

Remark This theorem was proved in [16] if we add the condition $\alpha^3 \ll 2^{2n}$ (and also $\xi_{max}\alpha^3 \ll 2^{2n}$ since ξ_{max} is here a fixed integer).

Theorem 7 ("Theorem $P_i \oplus P_j$" when $\xi_{max}\alpha \ll 2^n$). *With the same notations, we have the same result, with the hypothesis $\xi_{max}\alpha \ll 2^n$ (instead of ξ_{max} a fixed integer).*

Remark. For cryptographic use, weaker version of this theorem will be enough. For example, instead of $H_\alpha \geq J_\alpha$ for sufficiently large n, $H_\alpha \geq J_\alpha \left(1 - f(\frac{\xi\alpha}{2^n})\right)$, where f is a function such that $f(x) \to 0$ when $x \to 0$, is enough.

Another variant of this Theorem $P_i \oplus P_j$ is:

Theorem 8 ("Theorem $P_i \oplus P_j$ when $\xi_{max} \leq O(n)$ and $\xi_{average} \leq 3$). *Let $\xi_{average}$ be the average value of ξ, where ξ is the number of variables P_j that are fixed from the equations (A) when we fix a variable P_i. If $\xi_{max} \leq O(n)$ and $\xi_{average} \leq 3$, then for sufficient large n, $H_\alpha \geq J_\alpha$.*

Generalizations of the "Theorem $P_i \oplus P_j$". This theorem may have many generalizations. For example:

- Generalization 1: the theorem is still true in any group G (instead of I_n).
- Generalization 2: we have a similar property for equations with 3, 4, $\cdots$, or k variables, i.e. each equation is $P_{i_1} \oplus P_{i_2} \cdots P_{i_k} = \lambda_l$ with pairwise distinct P_i variables.

However in this paper we will only study the original "Theorem $P_i \oplus P_j$" (i.e. theorems 6 and 7) since it is this one that is needed to study random Feistel schemes.

5 First Simple Examples

5.1 ψ^2

For ψ^2 (Feistel scheme with the round functions $(f_1, f_2) \in_R F_n^2$) let $[L_i, R_i]$, $1 \leq i \leq m$ denotes the inputs, and $[S_i, T_i]$, $1 \leq i \leq m$ denotes the outputs. We have: $S_i = L_i \oplus f_1(R_i)$ and $T_i = R_i \oplus f_2(S_i)$ (*)

For random values $[L_i, R_i], [S_i, T_i]$, $1 \leq i \leq m$ (such that $i \neq j \rightarrow L_i \neq L_j$ or $R_i \neq R_j$) with probability $> 1 - \frac{m2}{2^n}$ we have that all the R_i values are pairwise distinct and all the S_i values are pairwise distinct. Moreover, if this occurs, we have exactly $H = \frac{|F_n|^2}{2^{2nm}}$ (since (*) then fix f_1 exactly on m points and f_2 exactly on m points).

So from Theorem 1 (with $\alpha = 0$ and $\beta = \frac{m^2}{2^n}$) we get:

Theorem 9. *For every KPA with m random known plaintexts, we have*

$$Adv^{KPA} \leq \frac{m^2}{2^n}$$

where Adv^{KPA} denotes the advantage to distinguish ψ^2 when $(f_1, f_2) \in_R F_n^2$ from a function $f \in_R F_{2n}$. So when $m \ll 2^{n/2}$, ψ^2 will resit all known plaintext attacks.

Remark. This result is tight, since when m^2 becomes not negligible compared with 2^n then by counting the number $\mathcal{N}$ of $(i,j)/S_i \oplus L_i = S_j \oplus L_j$ we will be able to distinguish ψ^2 from a random permutation with a known plaintext attack.

5.2 Involutive Permutations

Let assume that G is a generator of permutations that generates involutive permutations f (i.e. $f = f^{-1}$). Then we can distinguish such f from random permutations of B_N with $m = 2$ queries in CPA-2 and $m = 2$ queries in CPCA-1.

CPA-2

In CPA-2 we ask $f(a_1) = b_1$ and $f(b_1) = b_2$, and we test if $b_2 = a_1$. This gives a CPA-2 with $m = 2$ queries. It is not in contradiction with Theorem 3 since in Theorem 3, we need property (1) on **all** sequences a_i, $1 \leq i \leq m$ (and not necessary on **all** sequences b_i). Here if we have $a = (a_1, a_2)$, $b = (b_1, b_2)$ with $a_2 = b_1$ and $b_2 \neq a_1$, we will have $H = 0$. Therefore we will not be able to prove from Theorem 3 that G is secure in CPA-2 (in fact G is not secure in CPA-2) since for most (b_1, b_2) there exists (a_1, a_3) (take $a_2 = b_1$) such that $H = 0$.

CPCA-1

In CPCA-1 we ask $f(a_1) = b_1$ and $f^{-1}(a_1) = a_2$ and we test if $a_2 = b_1$. This gives a CPCA-1 distinguisher with $m = 2$ queries. We will not be able to prove

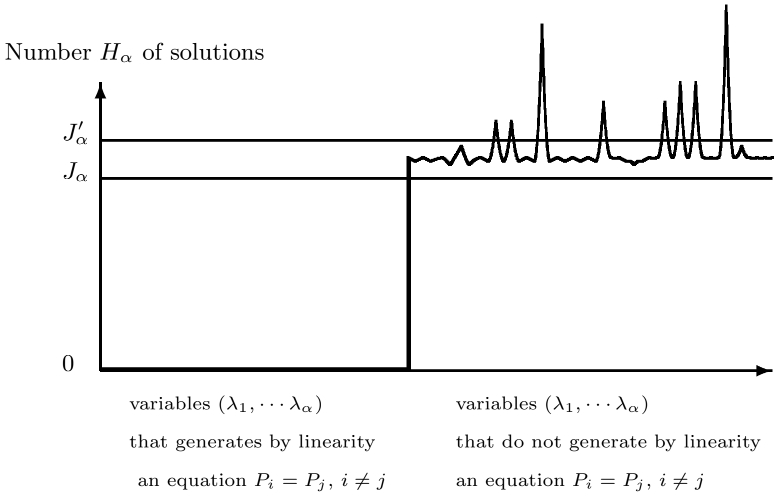

Fig. 2.

from Theorem 4 or Theorem 5 that G is secure in CPCA-1 (in fact G is not secure in CPCA-1) since in a non-adaptive chosen plaintext/ciphertext attack we can impose that $b_2 = a_1$ and if we have $a = (a_1, a_2)$, $b = (b_1, b_2)$ with $b_2 = a_1$ and $a_2 \neq b_1$ we will have $H = 0$.

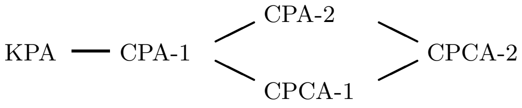

Fig. 3. Hierarchy of the attacks in secret key cryptography

5.3 Secret Key Security Hierarchy

In Figure 1, we have the well known hierarchy of attacks in secret key cryptography (cf [2], [4], [5]). With coefficients H technique we can easily prove on small examples this hierarchy, i.e. for example that there are some scheme secure in CPA-2 and not in CPCA-1, that some schemes are secure in CPA-1 and not in KPA etc. For example, we can easily prove that for a random involutive permutation of B_N we will have KPA and CPA-1 security in $O(\sqrt{2^N})$. Therefore the example of Section 6.2 shows that CPA-1 < CPA-2 and that CPA-1 < CPCA-1.

With f such that $f(0) = 0$ we will have that KPA < CPA-1.

With ψ^2 we will have KPA < CPA-1.

With ψ^3 we will have CPA-2 < CPCA-2 and CPCA-1 < CPCA-2.

With a random permutation such that $f^3 = \text{Id}$ we see that sometimes CPA-2 > CPCA-1

With a random permutation, such that $f^{-1}(x) = f(x) \oplus k$ where k is a secret constant we see that sometimes CPCA-1 > CPA-2.

6 Proofs with Coefficient H

6.1 Feistel Schemes ψ^k

I have proved many security results on ψ^k generators with coefficient H. For example, in [17], the security of ψ^5 when $m \ll 2^n$ was proved (with the H_w technique and "Theorem $P_i \oplus P_j$").

6.2 Xor of Two Random Permutations

Xoring two permutations is a simple very way to construct pseudorandom functions from pseudorandom permutations (this problem is sometimes called "Luby-Rackoff backwards"). In [19] we have proved this result:

Theorem 10. *For every CPA-2 on a function G of F_n with m chosen plaintexts, we have*

$$Adv^{PRF} \leq O(\frac{m}{2^n})$$

where Adv^{PRF} denotes the advantage to distinguish $f \oplus g$ with $f, g \in_R B_n$ from $h \in_R F_n$.

How to Get Theorem 10 from Theorem 3

A sufficient condition is to prove that for "most" (most since β must be small) sequences of values $b_i, 1 \leq i \leq m$, we have: the number H of $(f, g) \in B_n^2$ such that $\forall i, 1 \leq i \leq m, f \oplus g(a_i) = b_i$ satisfies: $H \geq \frac{|B_n^2|}{2^{nm}}(1 - \alpha)$ for a small value α (more precisely $\alpha \ll O(\frac{m}{2^n})$). One way to do this is to evaluate $E(H)$ and $\sigma(H)$, i.e. the mean value and the standard deviation of H when the b_i values are randomly chosen in I_n^m. (We call this technique, the "H_σ technique").

We can see that the result wanted to prove Theorem 10 exactly says that $\sigma(H) \ll E(H)$ when $m \ll 2^n$. To prove this, we can use the "covariance formula"

$$V(\sum_i N_i) = \sum_i (V(N_i)) + \sum_{i \neq j} [E(N_i N_j) - E(N_i)E(N_j)]$$

By definition, let λ_m be the number of sequences of values of I_n^3, $(f_i, g_i, h_i), 1 \leq i \leq m$ such that:

1. The m values f_i are pairwise distinct.
2. The m values g_i are pairwise distinct.
3. The m values h_i are pairwise distinct.
4. The m values $f_i \oplus g_i \oplus h_i$ are pairwise distinct.

After a change of variables we get finally that the property wanted in Theorem 10 means that

$$\lambda_m = \frac{(2^n(2^n-1)\dots(2^n-m+1))^4}{2^{nm}}(1+O(\frac{m}{2^n}))$$

(This is what was proved in [19])

I have also conjectured this property:

$$\forall f \in F_n,\ \text{if} \bigoplus_{x\in I_n} f(x)=0,\ \text{then}\ \exists (g,h)\in B_n2,\ \text{such that}\ f=g\oplus h.$$

Just one day after paper [19] was put on eprint, J.F. Dillon pointed to us that in fact this was proved in 1952 in [3]. We thank him a lot for this information. (This property was proved again independently in 1979 in [24]).

A New Conjecture

However I conjecture a stronger property. Conjecture:

$$\forall f \in F_n,\ \text{if} \bigoplus_{x\in I_n} f(x)=0,\ \text{then the number}\ H\ \text{of}\ (g,h)\in B_n2,$$

$$\text{such that}\ f=g\oplus h\ \text{satisfies}\ H \geq \frac{|B_n|^2}{2^{n2^n}}.$$

Variant: I also conjecture that this property is true in any group, not only with Xor.

Remark: In this paper, I have proved weaker results involving m equations with $m \ll O(2^n)$ instead of all the 2^n equations. These weaker results were sufficient for the cryptographic security wanted.

6.3 Benes Schemes

In [18] the security of Benes schemes when $m \ll 2^n$ was finally obtained (after the beginning of some proof ideas in [1]).

7 Attacks with Coefficient H

By using the coefficient values we were able to find many generic attacks. We give here some examples.

7.1 For Feistel Schemes ψ^k

From [15] we have the results of Table 1.

Table 1. Minimum number λ of computations needed to distinguish a generator Ψ^k (with one or many such permutations available) from random permutations with an even signature of $I_n \to I_n$. For simplicity we denote α for $O(\alpha)$. $\leq$ means best known attack.

	KPA	CPA-1	CPA-2	CPCA-1	CPCA-2
Ψ	1	1	1	1	1
$\Psi 2$	$2^{n/2}$	2	2	2	2
$\Psi 3$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	3
$\Psi 4$	2^n	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
$\Psi 5$	$\leq 2^{3n/2}$	2^n	2^n	2^n	2^n
$\Psi 6$	$\leq 2^{2n}$	$\leq 2^{2n}$	$\leq 2^{2n}$	$\leq 2^{2n}$	$\leq 2^{2n}$
$\Psi 7$	$\leq 2^{3n}$	$\leq 2^{3n}$	$\leq 2^{3n}$	$\leq 2^{3n}$	$\leq 2^{3n}$
$\Psi 8$	$\leq 2^{4n}$	$\leq 2^{4n}$	$\leq 2^{4n}$	$\leq 2^{4n}$	$\leq 2^{4n}$
$\Psi^k, k \geq 6$ *	$\leq 2^{(k-4)n}$	$\leq 2^{(k-4)n}$	$\leq 2^{(k-4)n}$	$\leq 2^{(k-4)n}$	$\leq 2^{(k-4)n}$

* If $k \geq 7$ these attacks analyze about $2^{(k-6)n}$ permutations of the generator and if $k \leq 6$ only one permutation is needed.

7.2 For Feistel Schemes ψ'^k with k Random Permutations for the Rounds Functions (Instead of Round Functions)

From [26] we have the results of Table 2.

Table 2. Maximum number of computations needed to get an attack on a k-round Feistel network with internal *permutations* (+) is shown when the values are larger than the corresponding values with internal functions.

number k of rounds	KPA	CPA-1	CPA-2	CPCA-1	CPCA-2
1	1	1	1	1	1
2	$2^{n/2}$	2	2	2	2
3	$2^n(+)$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	3
4	2^n	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
5	$2^{3n/2}$	2^n	2^n	2^n	2^n
6	$2^{3n}(+)$	$2^{3n}(+)$	$2^{3n}(+)$	$2^{3n}(+)$	$2^{3n}(+)$
7	2^{3n}	2^{3n}	2^{3n}	2^{3n}	2^{3n}
8	2^{4n}	2^{4n}	2^{4n}	2^{4n}	2^{4n}
9	$2^{6n}(+)$	$2^{6n}(+)$	$2^{6n}(+)$	$2^{6n}(+)$	$2^{6n}(+)$
10	2^{6n}	2^{6n}	2^{6n}	2^{6n}	2^{6n}
11	2^{7n}	2^{7n}	2^{7n}	2^{7n}	2^{7n}
12	$2^{9n}(+)$	$2^{9n}(+)$	$2^{9n}(+)$	$2^{9n}(+)$	$2^{9n}(+)$
$k \geq 6,\ k = 0\ mod\, 3$	$2^{(k-3)n}(+)$	$2^{(k-3)n}(+)$	$2^{(k-3)n}(+)$	$2^{(k-3)n}(+)$	$2^{(k-3)n}(+)$
$k \geq 6,\ k = 1$ or $2\ mod\, 3$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$

7.3 For Unbalanced Feistel Schemes with Contracting Functions

From [21] we have the results of Table 3.

Table 3. Results on G_k^d for any $k \geq 4$. For more than $2k$ rounds more that one permutation is needed or more than $2^{(2k-4)n}$ computations are needed in the best known attacks to distinguish from a random permutation with an even signature.

	KPA	CPA-1[a]
G_k^d, $1 \leq d \leq k-1$	1	1
G_k^k	$2^{\frac{n(k-1)}{2}}$	2
G_k^{k+1}	$2^{\frac{n(k-1)}{2}}$	$2^{\frac{n}{2}}$
G_k^{k+2}	$2^{\frac{k}{2}n}$	$2^{\frac{3}{2}n}$
G_k^{k+3}	$2^{(\frac{k+1}{2})n}$	$2^{\frac{5}{2}n}$
G_k^{k+i}, $1 \leq i < k$	$2^{(\frac{k+i-2}{2})n}$	$2^{(\frac{2i-1}{2})n}$
G_k^{2k}	$2^{(2k-4)n}$	$2^{(2k-4)n}$
G_k^d, $d \geq 2k$	$2^{(d+(k-2)\lfloor\frac{d}{k}\rfloor-2k)n}$	$2^{(d+(k-2)\lfloor\frac{d}{k}\rfloor-2k)n}$

[a] Here we do not show CPA-2, CPCA-1 and CPCA-2 since for G_k^d, no better attacks are found compared with CPA-1.

7.4 For Unbalanced Feistel Schemes with Expanding Functions

From [22] we have the results of Table 4

Table 4. Best known attacks on F_k^d for $k \geq 3$

	KPA	CPA-1
$F1_k$	1	1
$F2_k$	$2^{\frac{n}{2}}$	2
$F3_k$	2^n	2
F_k^d, $2 \leq d \leq k$	$2^{\frac{d-1}{2}n}$	2
F_k^{k+1}	$2^{\frac{k}{2}n}$	$2^{\frac{n}{2}}$
F_k^{k+2}	$2^{\frac{k+1}{2}n}$	2^n
F_k^{k+3}	$2^{\frac{2k+3}{4}n}$	2^{2n} or $2^{\frac{k+2}{3}n}$
F_k^d, $k+2 \leq d \leq 2k$	$2^{\frac{d+k}{4}n}$	$2^{(d-k-1)n}$ or $2^{\frac{d-1}{3}n}$
F_k^{2k}	$2^{\frac{3k}{4}n}$	$2^{\frac{2k-1}{3}n}$
$\vdots$	$\vdots$	$\vdots$
F_k^{3k-1}	$2^{(k-\frac{1}{8})n}$	$2^{(k-\frac{1}{2})n}$
F_k^{3k}	2^{kn}	2^{kn}
F_k^d, $3k \leq d \leq k2$	$2^{(d-2k)n}$	$2^{(d-2k)n}$
F_k^{k2}	$2^{(k2-2k)n}$	$2^{(k2-2k)n}$
....	....	....
F_k^{k2+1}	$2^{(2k2-3k-2)n}$	$2^{(2k2-3k-2)n}$
F_k^d, $d \geq k2+1$	$2^{(\lfloor 2d(1-\frac{1}{k})\rfloor-k-3)n}$	$2^{(\lfloor 2d(1-\frac{1}{k})\rfloor-k-3)n}$

8 New Designs

8.1 Russian Doll Design

See [23] in this volume.

8.2 Design from Random Unbalanced Feistel Schemes

This design comes directly from Table 3.

8.3 Hash Function Design

From 9.1 and 9.2 we are analyzing a Hash function design (by Xoring two independent pseudorandom permutations, or by Xoring the input and the output of a pseudorandom permutation).

9 Conclusion

With the "coefficient H technique" we were able to prove many security results and to get many generic attacks. Moreover, it was a source of inspiration for the design of new schemes.

References

1. Aiello, W., Venkatesan, R.: Foiling birthday attacks in length-doubling transformations. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 307–320. Springer, Heidelberg (1996)
2. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation. A Concrete Security Treatment of Symmetric Encryption and appeared in the Proceedings of 38th Annual Symposium of Computer Science, IEEE (1997)
3. Hall Jr., M.: A Combinatorial Problem on Abelian Groups. Proceedings of the Americal Mathematical Society 3(4), 584–587 (1952)
4. Katz, J., Yung, M.: Characterization of Security Notions for Probabilistic. In: Private-Key Encription – STOC 2000 (2000)
5. Katz, J., Yung, M.: Unforgeable Encryption and Chosen-Ciphertext-Secure Modes of Operation. In: Fast Software Encryption 2000 (2000)
6. Luby, M., Rackoff, C.: How to Construct Pseudorandom Permutations from Pseudorandom Functions. SIAM J. Comput. 17(2), 373–386 (1988)
7. Maurer, U.M.: A simplified and generalized treatment of luby-rackoff pseudorandom permutation generators. In: Rueppel, R.A. (ed.) EUROCRYPT 1992. LNCS, vol. 658, pp. 239–255. Springer, Heidelberg (1993)
8. Maurer, U.M.: Indistinguishability of random systems. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 100–132. Springer, Heidelberg (2002)
9. Maurer, U., Pietrzak, K.: The Security of Many-Round Luby-Rackoff Pseudo-Random Permutations. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 544–561. Springer, Heidelberg (2003)
10. Naor, M., Reingold, O.: On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited. J. Cryptology 12(1), 29–66 (1999)
11. Patarin, J.: Pseudorandom Permutations based on the DES Scheme. In: Charpin, P., Cohen, G. (eds.) EUROCODE 1990. LNCS, vol. 514, pp. 193–204. Springer, Heidelberg (1991)
12. Patarin, J.: Etude de Générateurs de Permutations Basés sur les Schémas du DES. Ph. Thesis. Inria, Domaine de Voluceau, France (1991)

13. Patarin, J.: New results on pseudorandom permutation generators based on the DES scheme. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 301–312. Springer, Heidelberg (1992)
14. Patarin, J.: How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function. In: Rueppel, R.A. (ed.) EUROCRYPT 1992. LNCS, vol. 658, pp. 256–266. Springer, Heidelberg (1993)
15. Patarin, J.: Generic attacks on feistel schemes. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 222–238. Springer, Heidelberg (2001)
16. Patarin, J.: Luby–rackoff: 7 rounds are enough for formula_image security. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 513–529. Springer, Heidelberg (2003)
17. Patarin, J.: On linear systems of equations with distinct variables and small block size. In: Won, D.H., Kim, S. (eds.) ICISC 2005. LNCS, vol. 3935, pp. 299–321. Springer, Heidelberg (2006)
18. Patarin, J.: A proof of security in O(2^n)for the benes scheme. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 209–220. Springer, Heidelberg (2008)
19. Patarin, J.: A proof of security in O(2^n) for the xor of two random permutations. In: Safavi-Naini, R. (ed.) ICITS 2008. LNCS, vol. 5155, pp. 232–248. Springer, Heidelberg (2008)
20. Patarin, J.: Generic Attacks for the Xor of k Random Permutations (eprint) (2008)
21. Patarin, J., Nachef, V., Berbain, C.: Generic attacks on unbalanced feistel schemes with contracting functions. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 396–411. Springer, Heidelberg (2006)
22. Patarin, J., Nachef, V., Berbain, C.: Generic attacks on unbalanced feistel schemes with expanding functions. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 325–341. Springer, Heidelberg (2007)
23. Patarin, J., Seurin, Y.: Building Secure Block Ciphers on Generic Attacks Assumptions. In: SAC 2008 (2008)
24. Salzborn, F., Szekeres, G.: A Problem in Combinatorial Group Theory. Ars Combinatoria 7, 3–5 (1979)
25. Schneier, B., Kelsey, J.: Unbalanced Feistel Networks and Block Cipher Design. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 121–144. Springer, Heidelberg (1996)
26. Treger, J., Patarin, J.: Generic Attacks On Feistel Schemes with Internal Permutations (paper in preparation)

A Proof of Theorem 1

Let ϕ be an algorithm (with no limitations in the number of computations) that takes the (a_i, b_i), $1 \leq i \leq m$ in input and outputs 0 or 1. let P_1 be the probability that ϕ outputs 1 when $\forall i$, $1 \leq i \leq m$ $b_i = G(f_1, \ldots, f_k)(a_i)$ when $(f_1, \ldots, f_k) \in_R K$. Let P_1^* be the probability that ϕ outputs 1 when $b_i = F(a_i)$ when $F \in_R F_N$. We want to prove that $|E(P_1 - P_1^*)|\alpha + \beta$. Let D be the set of all pairwise distinct a_i, $1 \leq i \leq m$ (so $|D| \simeq 2^{Nm}(1 - \frac{m(m-1)}{2 \cdot 2^N}))$. When the a_i, $1 \leq i \leq m$ are fixed, let $W(a)$ be the set of all $b_1, \ldots, b_m$ such that the algorithm ϕ outputs 1 on the input (a_i, b_i), $1 \leq i \leq m$. When the a_i, $1 \leq i \leq m$ are fixed in D, then we have:

$$P_1^* = \frac{|W(a)|}{2^{Nm}} \quad (1)$$

and

$$P_1 = \frac{1}{|K|} \sum_{b \in W(a)} [Numbers\ of\ (f_1, \ldots, f_k) \in K/$$

$$\forall i,\ 1 \leq i \leq m,\ G(f_1, \ldots, f_k)(a_i) = b_i]$$

so

$$P_1 = \frac{1}{|K|} \sum_{b \in W(a)} H(a,b) \quad (2)$$

Moreover, by hypothesis we have that the number $\mathcal{N}$ of (a,b) such that

$$H(a,b) \geq \frac{|K|}{2^{Nm}}(1-\alpha) \text{ satisfies} : \mathcal{N} \geq |D| \cdot 2^{Nm}(1-\beta) \quad (3)$$

When the (a_i), $1 \leq i \leq m$ are fixed, let $\mathcal{N}(a)$ be the set of all b such that:

$$H(a,b) \geq \frac{|K|}{2^{Nm}}(1-\alpha)$$

From (3) we have:

$$\sum_{a \in D} |\mathcal{N}(a)| \geq |D| \cdot 2^{Nm}(1-\beta) \quad (4)$$

From (2) we have:

$$P_1 \geq \frac{1}{|K|} \sum_{b \in W(a) \cap \mathcal{N}(a)} H(a,b)$$

so

$$P_1 \geq \frac{(1-\alpha)}{2^{Nm}} |W(a) \cap \mathcal{N}(a)|$$

so

$$P_1 \geq \frac{(1-\alpha)}{2^{Nm}} (|W(a)| - |\mathcal{N}'(a)|) \quad (5)$$

where $\mathcal{N}'(a)$ is the set of all b such that $b \notin \mathcal{N}(a)$. $|\mathcal{N}'(a)| = 2^{Nm} - |\mathcal{N}(a)|$, so

$$\sum_{a \in D} |\mathcal{N}'(a)| = |D| 2^{Nm} - \sum_{a \in D} |\mathcal{N}(a)|$$

so from (4) we have:

$$\sum_{a \in D} |\mathcal{N}'(a)| \leq \beta \cdot |D| \cdot 2^{Nm}, \text{ so } E(|\mathcal{N}'(a)|) \leq \beta \cdot 2^{Nm} \quad (6)$$

(where the expectation is computed when the (a_i), $1 \leq i \leq m$ are randomly chosen in D). From (5) and (1) we have:

$$P_1 \geq (1-\alpha)(P_1^* - \frac{|\mathcal{N}'(a)|}{2^{Nm}})$$

$$P_1 \geq (1-\alpha)P_1^* - \frac{|\mathcal{N}'(a)|}{2^{Nm}}$$

so from (6) we get:

$$E(P_1) \geq (1-\alpha)E(P_1^*) - \beta$$

so

$$E(P_1) \geq E(P_1^*) - \alpha - \beta \quad (7)$$

Now if we consider the algorithm ϕ' that outputs 1 if and only if ϕ outputs 0, we have $P_1' = 1 - P_1$ and $P_1^{'*} = 1 - P_1^*$ and from (7) we get: $E(P_1') \geq E(P_1^{'*}) - \alpha - \beta$ (because (7) is true for all algorithm ϕ, so it is true for ϕ'). So

$$E(1 - P_1) \geq E(1 - P_1^*) - \alpha - \beta$$

so

$$E(P_1) - E(P_1^*) \leq \alpha + \beta \quad (8)$$

From (7) and (8) we get $|E(P_1 - P_1^*)| \leq \alpha + \beta$ as claimed.

B Proof of Theorem 3

(I follow here a proof, in French, of this Theorem in my PhD Thesis, 1991, Page 27).

Let ϕ be a (deterministic) algorithm which is used to test a function f of F_n. (ϕ can test any function f from $I_N \to I_N$). ϕ can use f at most m times, that is to say that ϕ can ask for the values of some $f(C_i)$, $C_i \in I_N$, $1 \leq i \leq m$. (The value C_1 is chosen by ϕ, then ϕ receive $f(C_1)$, then ϕ can choose any $C_2 \neq C_1$, then ϕ receive $f(C_2)$ etc). (Here we have adaptive chosen plaintexts). (If $i \neq j$, C_i is always different from C_j). After a finite but unbounded amount of time, ϕ gives an output of "1" or "0". This output (1 or 0) is noted $\phi(f)$.

We will denote by P_1^*, the probability that ϕ gives the output 1 when f is chosen randomly in F_n. Therefore

$$P_1^* = \frac{\text{Number of functions } f \text{ such that } \phi(f) = 1}{|F_N|}$$

where $|F_N| = 2^{N \cdot 2^N}$.

We will denote by P_1, the probability that ϕ gives the output 1 when $(f_1, \ldots, f_k) \in_R K$ and $f = G(f_1, \ldots, f_k)$. Therefore

$$P_1 = \frac{\text{Number of } (f_1, \ldots, f_k) \in K \text{ such that } \phi(G(f_1, \ldots, f_k)) = 1}{|K|}$$

We will prove:

("Main Lemma"): For all such algorithms ϕ,

$$|P_1 - P_1^*| \leq \alpha + \beta$$

Then Theorem 1 will be an immediate corollary of this "Main Lemma" since Adv^{PRF} is the best $|P_1 - P_1^*|$ that we can get with such ϕ algorithms.

Proof of the "Main Lemma"

Evaluation of P_1^*

Let f be a fixed function, and let $C_1, \dots, C_m$ be the successive values that the program ϕ will ask for the values of f (when ϕ tests the function f). We will note $\sigma_1 = f(C_1), \dots, \sigma_m = f(C_m)$. $\phi(f)$ depends **only** of the outputs $\sigma_1, \dots, \sigma_m$. That is to say that if f' is another function of F_n such that $\forall i$, $1 \le i \le m$, $f'(C_i) = \sigma_i$, then $\phi(f) = \phi(f')$. (Since for $i < m$, the choice of C_{i+1} depends only of $\sigma_1, \dots, \sigma_i$. Also the algorithm ϕ cannot distinguish f from f', because ϕ will ask for f and f' exactly the same inputs, and will obtain exactly the same outputs). Conversely, let $\sigma_1, \dots, \sigma_n$ be m elements of I_N. Let C_1 be the first value that ϕ choose to know $f(C_1)$, C_2 the value that ϕ choose when ϕ has obtained the answer σ_1 for $f(C_1)$,..., and C_m the m^{th} value that ϕ presents to f, when ϕ has obtained $\sigma_1, \dots, \sigma_{m-1}$ for $f(C_1), \dots, f(C_{m-1})$. Let $\phi(\sigma_1, \dots, \sigma_m)$ be the output of ϕ (0 or 1). Then

$$P_1^* = \sum_{\substack{\sigma_1, \dots, \sigma_n \\ \phi(\sigma_1, \dots \sigma_m) = 1}} \frac{\text{Number of functions } f \text{ such that } \forall i,\ 1 \le i \le m,\ f(C_i) = \sigma_i}{2^{N \cdot 2^N}}$$

Since the C_i are all distinct the number of functions f such that $\forall i$, $1 \le i \le m$, $f(C_i) = \sigma_i$ is exactly $|F_n|/2^{nm}$. Therefore

$$P_1^* = \frac{\text{Number of outputs } (\sigma_1, \dots, \sigma_m) \text{ such that } \phi(\sigma_1, \dots \sigma_m) = 1}{2^{Nm}}$$

Let $\mathcal{N}$ be the number of outputs $\sigma_1, \dots, \sigma_m$ such that $\phi(\sigma_1, \dots \sigma_m) = 1$. Then $P_1^* = \frac{\mathcal{N}}{2^{Nm}}$.

Evaluation of P_1

With the same notation $\sigma_1, \dots, \sigma_n$, and $C_1, \dots C_m$:

$$P_1 = \frac{1}{|K|} \sum_{\substack{\sigma_1, \dots, \sigma_n \\ \phi(\sigma_1, \dots \sigma_m) = 1}} [\text{Number of } (f_1, \dots, f_k) \in K \text{ such that}$$

$$\forall i,\ 1 \le i \le m,\ G(f_1, \dots, f_k)(C_i) = \sigma_i] \quad (3)$$

Now (by definition of β) we have at most $\beta \cdot 2^{nm}$ sequences $(\sigma_1, \dots, \sigma_m)$ such that $(\sigma_1, \dots, \sigma_m) \notin E$. Therefore, we have at least $\mathcal{N} - \beta \cdot 2^{Nm}$ sequences $(\sigma_1, \dots, \sigma_m)$ such that $\phi(\sigma_1, \dots \sigma_m) = 1$ and $(\sigma_1, \dots, \sigma_m) \in E$ (4). Therefore, from (1), (3) and (4), we have

$$P_1 \ge \frac{(\mathcal{N} - \beta \cdot 2^{Nm}) \cdot \frac{|K|}{2^{Nm}}(1 - \alpha)}{|K|}$$

Therefore

$$P_1 \ge \big(\frac{\mathcal{N}}{2^{Nm}} - \beta\big)(1 - \alpha)$$

$$P_1 \ge (P_1^* - \beta)(1 - \alpha)$$

Thus $P_1 \geq P_1^* - \alpha - \beta$ (5), as claimed.

We now have to prove the inequality in the other side. For this, let P_0^* be the probability that $\phi(f) = 0$ when $f \in_R F_N$. $P_0^{'*} = 1 - P_1^*$. Similarly, let P_0 be the probability that $\phi(f) = 0$ when $(f_1, \ldots, f_k) \in_R K$ and $f = G(f_1, \ldots, f_k)$. $P_0 = 1 - P_1$. We will have $P_0 \geq P_0^* - \alpha - \beta$ (since the outputs 0 and 1 have symmetrical hypothesis. Or, alternatively since we can always consider an algorithm ϕ' such that $\phi'(f) = 0 \Leftrightarrow \phi(f) = 1$ and apply (5) to this algorithm ϕ').

Therefore, $1 - P_1 \geq 1 - P_1^* - \alpha - \beta$, i.e. $P_1^* \geq P_1 - \alpha - \beta$ (6). Finally, from (5) and (6), we have: $|P_1 - P_1^*| \leq \alpha + \beta$, as claimed.