ECOLE NORMALE SUPERIEURE

Provable security for block Ciphers by decorrelation

Serge VAUDENAY

LIENS - 98 - 8

Département de Mathématiques et Informatique

CNRS URA 1327

Provable security for block Ciphers by decorrelation

Serge VAUDENAY

LIENS - 98 - 8

June 1998

Laboratoire d'Informatique de l'Ecole Normale Supérieure
45 rue d'Ulm 75230 PARIS Cedex 05

Tel : (33)(1) 01 44 32 30 00

Adresse électronique : vaudenay@dmi.ens.fr

Provable Security for Block Ciphers by Decorrelation

Serge Vaudenay

Ecole Normale Supérieure — CNRS
Serge.Vaudenay@ens.fr

Abstract. In this paper we investigate a new way for protecting block ciphers against classes of attacks (including differential and linear cryptanalysis) which is based on the notion of decorrelation distance which is fairly connected to Carter-Wegman's universal hash functions paradigm. This defines a simple and friendly combinatorial measurement which enables to quantify the security. We show that we can mix provable protections and heuristic protections. We finally propose two new block cipher families we call COCONUT and PEANUT, which implement these ideas and achieve quite reasonable performances for real-life applications.

Before the second world war, security of encryption used to be based on the secrecy of the algorithm. Mass telecommunication and computer science networking however pushed the development of public algorithms with secret keys. The most important research result on encryption was found for the application to the telegraph by Shannon in the Bell Laboratories in 1949 [30]. It proved the unconditional security of the Vernam's Cipher which had been published in 1926 [38]. Although quite expensive to implement for networking (because the sender and the receiver need to be synchronized, and it needs quite cumbersome huge keys), this cipher was used in the Red Telephone between Moscow and Washington D.C. during the cold war. Shannon's result also proves that unconditional security cannot be achieved in a better (*i.e.* cheaper) way. For this reason, empiric security seemed to be the only efficient possibility, and all secret key block ciphers which have been publicly developed were considered to be secure until some researcher published an attack on it. Therefore research mostly grew like a ball game between the designers team and the analysts team and treatment on the general security of block ciphers has hardly been done.

In adopting the *Data Encryption Standard* (DES) [1] in the late 70's, the U.S. Government classified the development arguments.

Attacking DES was thus quite challenging, and this paradoxically boosted research on block ciphers. Real advances on the security on block ciphers have been made in the early 90's.

One of the most important result has been obtained by Biham and Shamir in performing a *differential cryptanalysis* on DES [3–6]. The best version of this attack can recover a secret key with a simple 2^{47}-chosen plaintext attack[1]. Although this attack is heuristic, experiments confirmed the results.

Biham and Shamir's attack was based on statistical cryptanalysis idea which have also been used by Gilbert and Chassé against another cipher [11, 10]. Those ideas inspired Matsui who developed a *linear cryptanalysis* on DES [22, 23]. This heuristic attack, which has been implemented, can recover the key with a 2^{43}-known plaintext attack. Since then, many researchers tried to generalize and improve these attacks (see for instance [20, 19, 13, 17, 32, 18, 25, 33]), but the general ideas was quite the same.

The basic idea of differential cryptanalysis is to use properties like "if x and x' are two plaintext blocks such that $x' = x + a$, then it is likely that $C(x') = C(x) + b$". Then the attack is an iterated two-chosen plaintexts attack which consists in getting the encrypted values of two random plaintexts which verify $x' = x + a$ until a special event like $C(x') = C(x)+b$ occurs. Similarly, the linear cryptanalysis consists in using the probability $\Pr[C(x) \in H_2 / x \in H_1]$ for two given hyperplanes H_1 and H_2. With the GF(2)-vector space structure, hyperplanes are half-spaces, and this probability shall be close to $1/2$. Linear cryptanalysis uses the distance of this probability to $1/2$ when it is large enough. More precisely, linear cryptanalysis is an incremental one-known plaintext attack where we simply measure the correlation between the events $[x \in H_1]$ and $[C(x) \in H_2]$.

Instead of keeping on breaking and proposing new encryption functions, some researchers tried to focus on the way to protect ciphers against some classes of attacks. Nyberg first formalized the notion of strength against differential cryptanalysis [26], and similarly, Chabaud and Vaudenay formalized the notion of strength against linear cryptanalysis [7]. With this approach we can study how to make

[1] So far, the best known attack was an improvement of exhaustive search which requires on average 2^{54} DES computations.

internal computation boxes resistant against both attacks. This can be used in a heuristic way by usual active s-boxes counting tricks (*e.g.*, see [13, 15]). This has also been used to provide provable security against both attacks by Nyberg and Knudsen [27], but in an unsatisfactory way which introduce some algebraic properties which lead to other attacks as shown by Jakobsen and Knudsen [16].

In this presentation, we introduce a new way to protect block ciphers against various kind of attacks. This approach is based on the notion of universal functions introduced by Carter and Wegman [8, 39] for the purpose of authentication. Protecting block ciphers is so cheap that we call NUT (as for "n-Universal Transformation") the added operations which provide this security. We finally describe two cipher families we call COCONUT (as for "Cipher Organized with Cute Operations and NUT") and PEANUT (as for "Pretty Encryption Algorithm with NUT") and offer two definite examples as a cryptanalysis challenge.

The paper is organized as follows. First we give some definitions on decorrelation distance (Section 1) and basic constructions (Section 2). Then we state Shannon's perfect secrecy notion in term of decorrelation distance (Section 3). We show how to express security results in the Luby-Rackoff's security model (Section 4). Then we compute how much Feistel Ciphers can be decorrelated (Section 5). We prove how pairwise decorrelation can protect a cipher against differential cryptanalysis and linear cryptanalysis (Sections 6 and 7). We generalize those results with the notion of "attacks of order d" (Section 8). Finally, we define the COCONUT and PEANUT families (Sections 9 and 10).

1 Decorrelation Distance

For a treatment on block cipher, we consider ciphers as random permutations C on the message-block space $\mathcal{M}$. (Here the randomness comes from the random choice of the secret key.) In most of practical cases, we have $\mathcal{M} = \{0,1\}^m$.

We first give formal definitions of the notion of decorrelation distance which plays a crucial role in our treatment.

Definition 1. *Given a random function F from a given set $\mathcal{M}_1$ to a given set $\mathcal{M}_2$ and an integer d, we define the* d-wise distribution matrix $[F]^d$ *of F as a $\mathcal{M}_1^d \times \mathcal{M}_2^d$-matrix where the (x, y)-entry of $[F]^d$ corresponding to the multi-points $x = (x_1, \ldots, x_d) \in \mathcal{M}_1^d$ and $y = (y_1, \ldots, y_d) \in \mathcal{M}_2^d$ is defined as the probability that we have $F(x_i) = y_i$ for $i = 1, \ldots, d$.*

Basically, each row of the d-wise distribution matrix corresponds to the distribution of the d-tuple $(F(x_1), \ldots, F(x_d))$ where $(x_1, \ldots, x_d)$ corresponds to the index of the row.

Definition 2. *Given two random functions F and G from a given set $\mathcal{M}_1$ to a given set $\mathcal{M}_2$, an integer d and a distance D over the vector space $\mathbf{R}^{\mathcal{M}_1^d \times \mathcal{M}_2^d}$, we call $D([F]^d, [G]^d)$ the* d-wise decorrelation D-distance *between F and G.*

A decorrelation distance of zero means that for any multi-point $x = (x_1, \ldots, x_d)$ the multi-points $(F(x_1), \ldots, F(x_d))$ and $(G(x_1), \ldots, G(x_d))$ have the same distribution, so that F and G have the same *decorrelation*.

Actually, we do not need a distance over the whole matrix set, but only on some sub-algebra. We distinguish the decorrelation of *functions* from the decorrelation of *permutations* (or *ciphers*). Distribution matrices A of functions (as well as other matrices in the sub-algebra they span) are such that if $x_i = x_j$ for some indices i and j in any multi-point x, then for all multi-point y such that $y_i \neq y_j$ we have $A_{x,y} = 0$ (because if $x_i = x_j$ then $F(x_i) = F(x_j)$). Additional properties hold for permutations. Thus, we indeed need distance over the corresponding sub-algebra.

It is also important to study the decorrelation distance of a given random function F to a reference random function. Random functions F are compared to uniformly distributed random functions (that we call *perfect random functions*) which will be denoted F^*. We say that the decorrelation of the random function F^* is *perfect*. Similarly, random permutations C are compared to a uniformly distributed permutations C^* (which will be called *perfect cipher*), and the *decorrelation of the cipher C^** is *perfect*. Any random function (resp. cipher) with a d-wise decorrelation distance of zero to the perfect random function (resp. perfect cipher) will be said to have a *perfect decorrelation*.

For instance, let say that F is a random function from $\mathcal{M}_1$ to $\mathcal{M}_2$. Saying that F has a perfect 1-wise decorrelation means that for any x_1 the distribution of $F(x_1)$ is uniform. Saying that the *function* F has a perfect 2-wise decorrelation means that for any $x_1 \neq x_2$ the random variables $F(x_1)$ and $F(x_2)$ are uniformly distributed and independent. Saying that a *cipher* C on $\mathcal{M}$ has a perfect 2-wise decorrelation means that for any $x_1 \neq x_2$, the random variable $(C(x_1), C(x_2))$ is uniformly distributed among all the (y_1, y_2) pairs such that $y_1 \neq y_2$.

Definition 3. *Let F (resp. C) be a random function from $\mathcal{M}_1$ to $\mathcal{M}_2$ (resp. a random permutation over $\mathcal{M}$). Let D be a distance over the algebra spanned by the d-wise distribution matrices of random functions (resp. of random permutations). We call* d-wise decorrelation D-bias *and we denote* ${}^{f}\mathrm{Dec}_D^d(F)$ *(resp.* $\mathrm{Dec}_D^d(C)$*) the quantity $D([F]^d, [F^*]^d)$ (resp. $D([C]^d, [C^*]^d)$) where F^* (resp. C^*) is uniformly distributed.*

We note that this notion is fairly similar to the notion of universal functions which was been introduced by Carter and Wegman [8, 39]. More precisely, we recall that a random function F from $\mathcal{M}_2$ to $\mathcal{M}_2$ is ϵ-almost strongly universal$_d$ if for any pairwise different $(x_1, \ldots, x_d)$ and any $(y_1, \ldots, y_d)$ we have

$$\Pr[F(x_i) = y_i; i = 1, \ldots, d] \leq \frac{1}{\#\mathcal{B}^d} + \epsilon.$$

If we define $||A||_\infty = \max_{x,y} |A_{x,y}|$, if the function F has a d-wise decorrelation $||.||_\infty$-bias of ϵ, then it is ϵ-almost strongly universal$_d$. The converse is true when $\epsilon \geq \frac{1}{\#\mathcal{B}^d}$. Although the notion is fairly similar, we will use our formalism which is adapted to our context.

For the purpose of our treatment, we define the L_2 norm, the infinity weighted norm N_∞ and the L_∞-associated matrix norm $|||.|||_\infty$ on $\mathbf{R}^{\mathcal{M}_1^d \times \mathcal{M}_2^d}$ by:

$$||A||_2 = \sqrt{\sum_{x,y} (A_{x,y})^2} \tag{1}$$

$$N_\infty(A) = \max_{x,y} \frac{|A_{x,y}|}{\Pr[x \overset{C^*}{\mapsto} y]} \tag{2}$$

$$|||A|||_\infty = \max_x \sum_y |A_{x,y}| \tag{3}$$

where C^* is the Perfect Cipher. We note that the N_∞ can only be defined on the sub-algebra spanned by distribution matrices of ciphers *i.e.* with the convention that $0/0 = 0$.

We recall that the $||.||_2$ and $|||.|||_\infty$ norms are matrix norms, *i.e.* $||A \times B|| \leq ||A||.||B||$. Moreover, N_∞ has a similar property in its sub-algebra of definition. Multiplicativity of the decorrelation distance to C^* is very useful when we consider product ciphers. Concretely, if C_1 and C_2 are two independent ciphers, then

$$\mathrm{Dec}^d(C_1 \circ C_2) \leq \mathrm{Dec}^d(C_1).\mathrm{Dec}^d(C_2)$$

for any matrix norm. (This comes from $[C_1 \circ C_2]^d = [C_2]^d \times [C_1]^d$ and $[C_i]^d \times [C^*]^d = [C^*]^d$.) This property makes the decorrelation bias a multiplicative combinatorial measurement whenever the norm is a matrix norm.

2 Basic Constructions

Perfect 1-wise decorrelation is easy to achieve when the message-block space $\mathcal{M}$ is given a group structure. For instance we can use $C(x) = x + K$ where K has a uniform distribution on $\mathcal{M}$, which is exactly Vernam's Cipher ([38]).

We can construct perfect pairwise decorrelated ciphers on a field structure $\mathcal{M}$ by $C(x) = a.x + b$ where $K = (a, b)$ is uniform in $\mathcal{M}^* \times \mathcal{M}$. This requires to consider the special case $a = 0$ when generating K. On the standard space $\mathcal{M} = \{0,1\}^m$, it also requires to implement arithmetic on the finite field $\mathrm{GF}(2^m)$, which may lead to poor encryption rate on software. As an example we can mention the COCONUT Ciphers (see Section 9).

A similar way to construct (almost) perfect 3-wise decorrelated ciphers on a field structure $\mathcal{M}$ is by $C(x) = a + b/(x + c)$ where $K = (a, b, c)$ with $b \neq 0$. (By convention we set $1/0 = 0$.)

Perfect decorrelated ciphers of higher orders require dedicated structure. We can for instance use Dickson's Polynomials.

An alternate way consists of using Feistel Ciphers with decorrelated functions [9]. Given a set $\mathcal{M} = \mathcal{M}_0^2$ where $\mathcal{M}_0$ has a group structure and given r random functions $F_1, \ldots, F_r$ on $\mathcal{M}_0$ we denote $C = \Psi(F_1, \ldots, F_r)$ the cipher defined by $C(x^l, x^r) = (y^l, y^r)$ where we iteratively compute a sequence (x_i^l, x_i^r) such that

$$\begin{aligned} x_0^l &= x^l \text{ and } x_0^r = x^r \\ x_i^l &= x_{i-1}^r \text{ and } x_i^r = x_{i-1}^l + F_i(x_{i-1}^r) \\ y^l &= x_r^r \text{ and } y^r = x_r^l. \end{aligned}$$

(Note that the final exchange between the two halves is canceled here.) In most of the constructions, $\mathcal{M}_0$ is the group $\mathbf{Z}_2{}^{\frac{m}{2}}$, so the addition is the bitwise exclusive *or*.

If $\mathcal{M}_0$ has a field structure, we can use perfect d-wise decorrelated F_i functions by $F_i(x) = a_d.x^{d-1} + \ldots + a_2.x + a_1$ where $(a_1, \ldots, a_d)$ is uniformly distributed on $\mathcal{M}_0^d$.

Decorrelation of Feistel Ciphers depends on the decorrelation of all F_i functions. It will be studied in Section 5.

3 Shannon's Unconditional Security

In this section, we consider perfect decorrelation.

Intuitively, if C has a perfect 1-wise decorrelation, the encryption $C(x_1)$ contains no information on the plaintext-block x_1, so the cipher C is secure if we use it only once (as one-time pad [38]). This corresponds to Shannon's perfect secrecy theory [30]. Similarly, if C has a perfect d-wise decorrelation, it is unconditionally secure if we use it only d times (on different plaintexts) as the following theorem shows.

Theorem 4. *Let C be a cipher with a perfect d-wise decorrelation. For any $x_1, \ldots, x_{d-1}$, if X is a random variable such that $X \neq x_i$, then*

$$H(X/C(x_1), \ldots, C(x_{d-1}), C(X)) = H(X)$$

where H denotes Shannon's entropy of random variables.

This means that if an adversary knows $d-1$ pairs $(x_i, C(x_i))$, for any y_d which is different from all $C(x_i)$'s, his knowledge of $C^{-1}(y_d)$ is

exactly that it is different from all x_i's. We recall that by definition we have $H(X/Y) = H(X,Y) - H(Y)$ and

$$H(X) = -\sum_x \Pr[X = x] \log_2 \Pr[X = x]$$

with the convention that $0 \log_2 0 = 0$.

Proof. From definitions, straightforward computations shows that for any random variable X we have

$$H(X/C(x_1), \ldots, C(x_{d-1}), C(X)) = H(X) + p \log_2 p$$

where $p = \Pr[X \neq x_i; i = 1, \ldots, d-1]$. Hence for any random variable such that $\Pr[X = x_i] = 0$ the property holds. □

4 Security in the Luby-Rackoff Model

To illustrate the power of the notion of decorrelation, let us first measure the unconditional security. In the Luby-Rackoff model, an attacker is an infinitely powerful Turing machine $\mathcal{A}^{\mathcal{O}}$ which has access to an oracle $\mathcal{O}$ whose aim is to distinguish a cipher C from the Perfect Cipher C^* by querying the oracle which implements either cipher, and with a limited number d of inputs (see [21]). The oracle $\mathcal{O}$ either implements C or C^*, and that the attacker must finally answer 0 ("reject") or 1 ("accept"). We measure the ability to distinguish C from C^* by the advantage $\mathrm{Adv}_{\mathcal{A}}(C) = |p - p^*|$ where p (resp. p^*) is the probability of answering 1 if $\mathcal{O}$ implements C (resp. C^*). A general distinguisher is illustrated on Fig. 1. We have the

Input: an oracle which implements a permutation c
1. calculate a message X_1 and get $Y_1 = c(X_1)$
2. calculate a message X_2 and get $Y_2 = c(X_2)$
3. ...
4. calculate a message X_d and get $Y_d = c(X_d)$
5. depending on $X = (X_1, \ldots, X_d)$ and $Y = (Y_1, \ldots, Y_d)$, output 0 or 1

Fig. 1. A General d-Limited Distinguisher.

following theorem.

Theorem 5. *Let d be an integer and C be a cipher. For any general d-limited distinguisher (depicted on Fig. 1), we have*

$$\mathrm{Adv}_{\mathrm{Fig.1}}(C) \leq \mathrm{Dec}^{d}_{N_\infty}(C)$$

where the N_∞ norm is defined by Equation (2).

In particular, we have unconditional security when the decorrelation is perfect and we still have a proven quantified security when the decorrelation is small.

Proof. Each execution of the attack with an oracle which implements C is characterized by a random tape ω and the successive answers $y_1, \ldots, y_d$ of the queries which we denote $x_1, \ldots, x_d$ respectively. More precisely, x_1 depends on ω, x_2 depends on ω and y_1 and so on. The answer thus depends on $(\omega, y_1, \ldots, y_d)$. Let A be the set of all $(\omega, y_1, \ldots, y_d)$ such that the output of the distinguisher is 1 and let $\epsilon = \mathrm{Dec}^{d}_{N_\infty}(C)$. We have

$$\begin{aligned} p &= \sum_{(\omega, y_1, \ldots, y_d) \in A} \Pr[\omega] \Pr[C(x_i(\omega, y_1, \ldots, y_{i-1})) = y_i; i = 1, \ldots, d] \\ &\leq (1+\epsilon) \sum_{(\omega, y_1, \ldots, y_d) \in A} \Pr[\omega] \Pr[C^*(x_i(\ldots)) = y_i; i = 1, \ldots, d] \\ &\leq (1+\epsilon) p^* \end{aligned}$$

so we have $p - p^* \leq \epsilon$ for any attacker. We can apply this result to the attacker which produces the opposite output to complete the proof. □

Here is a more intuitive meaning of Theorem 5 which is interesting when we use encryption as a message authentication code.

Corollary 6. *Let d be an integer and C be a cipher on a space of size M. For any chosen plaintext attack which can query up to $d-1$ $C(x_i)$ values and which issues a (x_d, y_d) pair with $x_d \neq x_i$ $(i = 1, \ldots, d-1)$, the probability that $y_d = C(x_d)$ is at most $\frac{1}{M} + \mathrm{Dec}^{d}_{N_\infty}(C)$.*

Proof. Such an attack can be transformed into a d-limited distinguisher: the distinguisher first simulate the attack by obtaining $d-1$ pairs from the oracle and obtain a (x_d, y_d) pair. It then queries the oracle with x_d and output 1 if, and only if $y_d = C(x_d)$. From the fact that the advantage is at most ϵ we obtain the result. □

Here is a more precise theorem in the non adaptive case. We call a distinguisher "non adaptive" if no x_i queried to the oracle depends on some previous answers y_j (see Fig. 2).

Input: an oracle which implements a permutation c
1. calculate some messages $X = (X_1, \ldots, X_d)$
2. get $Y = (c(X_1), \ldots, c(X_d))$
3. depending on X and Y, output 0 or 1

Fig. 2. A d-Limited Non-Adaptive Distinguisher.

Theorem 7. *Let d be an integer and C be a cipher. The best d-limited non-adaptive distinguisher (depicted on Fig. 2) for C is such that*

$$\mathrm{Adv}_{\mathrm{Fig.2}}(C) = \frac{1}{2}\mathrm{Dec}^{d}_{|||.|||_\infty}(C)$$

where the $|||.|||_\infty$ norm is defined by Equation (3).

Proof. For those attacks, with the notations of Theorem 5, we have

$$p = \sum_x \Pr[x] \sum_y 1_{(x,y)\in A} \Pr\left[x \overset{C}{\mapsto} y\right]$$

(where 1_P is defined to be 1 if predicate P is true and 0 otherwise) thus, for the best attack, we have

$$|p - p^*| = \max_{\substack{x \mapsto \Pr[x] \\ A}} \left| \sum_x \Pr[x] \sum_y 1_{(x,y)\in A} \left(\Pr\left[x \overset{C}{\mapsto} y\right] - \Pr\left[x \overset{C^*}{\mapsto} y\right] \right) \right|.$$

We can easily see that this maximum is obtained when $x \mapsto \Pr[x]$ is a Dirac distribution on a multi-point $x = x^0$ and A includes all y's such that $\Pr\left[x_0 \overset{C}{\mapsto} y\right] - \Pr\left[x_0 \overset{C^*}{\mapsto} y\right]$ has the same sign, which gives the result. □

Here is a more intuitive consequence analog to Corollary 6.

Corollary 8. *Let d be an integer and C be a cipher on a space of size M. For any chosen plaintext attack which aims to compute $C(x_d)$ for a given x_d and which only can query for $d-1$ chosen values $C(x_i)$ for $x_i \neq x_d$ ($i = 1, \ldots, d-1$) in a non-adaptive way, the probability of success is at most $\frac{1}{M} + \mathrm{Dec}^{d}_{|||.|||_\infty}(C)$.*

5 Decorrelation of Feistel Ciphers

In this section, we assume that $\mathcal{M} = {\mathcal{M}_0}^2$ where $\mathcal{M}_0$ is a group. Thus we can consider Feistel Ciphers on $\mathcal{M}$.

Theorem 7 can be used in a non-natural way. For instance, let us recall the following theorem.

Theorem 9 (Luby-Rackoff [21]). *Let F_1, F_2, F_3 be three independent uniform random functions on $\mathcal{M}_0$ and d be an integer. For any distinguishing attacker $\mathcal{A}$ against $\Psi(F_1, F_2, F_3)$ on $\mathcal{M} = {\mathcal{M}_0}^2$ which is limited to d queries, we have*

$$\mathrm{Adv}_{\mathcal{A}}(\Psi(F_1, F_2, F_3)) \leq \frac{d^2}{\sqrt{\#\mathcal{M}}}.$$

Thus from Theorem 7 we have

$$\mathrm{Dec}^d_{|||.|||_\infty}(\Psi(F_1, F_2, F_3)) \leq 2\frac{d^2}{\sqrt{\#\mathcal{M}}}.$$

For completeness, we also mention some improvements to the previous theorem due to Patarin [28, 29].

Theorem 10 (Patarin [29]). *Let $F_1, \ldots, F_6$ be six independent uniform random functions on $\mathcal{M}_0$ and d be an integer. For any distinguishing attacker against $\Psi(F_1, \ldots, F_6)$ on $\mathcal{M} = {\mathcal{M}_0}^2$ which is limited to d queries $\mathcal{A}$, we have*

$$\mathrm{Adv}_{\mathcal{A}}(\Psi(F_1, \ldots, F_6)) \leq \frac{37d^4}{(\#\mathcal{M})^{\frac{3}{2}}} + \frac{6d^2}{\#\mathcal{M}}.$$

So, as Theorem 9 guarantees the security of a three-round Feistel Cipher for $d = \Omega\left((\#\mathcal{M})^{\frac{1}{4}}\right)$, this one guarantees the security for $d = \Omega\left((\#\mathcal{M})^{\frac{3}{8}}\right)$.

The decorrelation $|||.|||_\infty$-bias of Feistel Ciphers can be estimated with the following lemma.

Lemma 11. *Let $F_1, \ldots, F_r$ (resp. $R_1, \ldots, R_r$) be r independent random functions on $\mathcal{M}_0$ such that $|||[F_i]^d - [R_i]^d|||_\infty \leq \epsilon_i$ $(i = 1, \ldots, r)$. We have*

$$|||[\Psi(F_1, \ldots, F_r)]^d - [\Psi(R_1, \ldots, R_r)]^d|||_\infty \leq (1 + \epsilon_1) \ldots (1 + \epsilon_r) - 1.$$

Proof. Let u^i denotes the input of F_i (resp. R_i) in $\Psi(F_1,\ldots,F_r)$ (resp. $\Psi(R_1,\ldots,R_r)$). We thus let (u^0,u^1) denotes the input of the ciphers, and (u^{r+1},u^r) denotes the output. Here, all u^is are multi-points, *i.e.* $u^i=(u^i_1,\ldots,u^i_d)$. We have

$$\begin{aligned}
&\Pr_{F_1,\ldots,F_r}[u^0u^1\mapsto u^{r+1}u^r]-\Pr_{R_1,\ldots,R_r}[u^0u^1\mapsto u^{r+1}u^r]\\
&\quad=\sum_{u^2,\ldots,u^{r-1}}\left(\prod_{i=1}^{r}\Pr_{F_i}[u^i\mapsto u^{i+1}-u^{i-1}]-\prod_{i=1}^{r}\Pr_{R_i}[u^i\mapsto u^{i+1}-u^{i-1}]\right)\\
&\quad=\sum_{u^2,\ldots,u^{r-1}}\sum_{\substack{I\subseteq\{1,\ldots,r\}\\ I\neq\emptyset}}\left(\prod_{i\in I}(\Pr_{F_i}-\Pr_{R_i})\prod_{i\notin I}\Pr_{R_i}\right)[u^i\mapsto u^{i+1}-u^{i-1}]
\end{aligned}$$

hence

$$\begin{aligned}
&\sum_{u^{r+1},u^r}\left|\Pr_{F_1,\ldots,F_r}[u^0u^1\mapsto u^{r+1}u^r]-\Pr_{R_1,\ldots,R_r}[u^0u^1\mapsto u^{r+1}u^r]\right|\\
&\quad\le\sum_{u^2,\ldots,u^{r+1}}\sum_{\substack{I\subseteq\{1,\ldots,r\}\\ I\neq\emptyset}}\left(\prod_{i\in I}|\Pr_{F_i}-\Pr_{R_i}|\prod_{i\notin I}\Pr_{R_i}\right)[u^i\mapsto u^{i+1}-u^{i-1}]\\
&\quad\le\sum_{\substack{I\subseteq\{1,\ldots,r\}\\ I\neq\emptyset}}\prod_{i\in I}\epsilon_i\\
&\quad=(1+\epsilon_1)\ldots(1+\epsilon_r)-1.
\end{aligned}$$

□

From this lemma and the previous observation we obtain the following theorem.

Theorem 12. *Let $F_1,\ldots,F_r$ be r independent random functions on $\mathcal{M}_0$ such that ${}^f\mathrm{Dec}^d_{|||.|||_\infty}(F_i)\le\epsilon$ $(i=1,\ldots,r)$. For any $k\ge 3$ we have*

$$\mathrm{Dec}^d_{|||.|||_\infty}(\Psi(F_1,\ldots,F_r))\le\left((1+\epsilon)^k-1+\frac{2d^2}{\sqrt{\#\mathcal{M}}}\right)^{\lfloor\frac{r}{k}\rfloor}.$$

We can remark that the lemma remains valid if we replace the group operation used in the Feistel construction by any other pseudogroup law. This makes the decorrelation $|||.|||_\infty$-bias a friendly tool for constructing Feistel Ciphers.

6 Differential Cryptanalysis

In this section we assume that $\mathcal{M}$ is given a group structure of order M. We study the security of pairwise decorrelated ciphers against basic differential cryptanalysis. We study criteria which prove that the attack cannot be better than exhaustive attack, M.

Let C be a cipher on $\mathcal{M}$ and let C^* be the Perfect Cipher.

Although differential cryptanalysis has been invented in order to recover a whole key by Biham and Shamir (see [5, 6]), we study here the basic underlying notion which makes it work. We call basic differential cryptanalysis the distinguisher which is characterized by a pair $(a, b) \in \mathcal{M}^2$ with $a \neq 0$ and which is depicted on Fig. 3.

Input: a cipher c, a complexity n, a characteristic (a, b)
1. for i from 1 to n do
   (a) pick uniformly a random X and query for $c(X)$ and $c(X + a)$
   (b) if $c(X + a) = c(X) + b$, stop and output 1
2. output 0

Fig. 3. Differential Distinguisher.

It is well known that differential cryptanalysis depends on the following $\mathrm{DP}^C(a, b)$ (see for instance [26]). We define

$$\mathrm{DP}^C(a, b) = \Pr_X[C(X + a) = C(X) + b]$$

where X has a uniform distribution. This quantity thus depends on the choice of the cipher (*i.e.* on the key). Here we focus on average complexities of attacks with no prior information on the key, *i.e.* on the average value $E\left(\mathrm{DP}^C(a, b)\right)$ over the distribution of C. The problem of successful attacks for sets of *weak keys* is not our purpose here. We first mention that $E\left(\mathrm{DP}^C(a, b)\right)$ has an interesting linear expression with respect to the pairwise distribution matrix of C. Namely, straightforward computation shows that

$$E(\mathrm{DP}^C(a, b)) = \frac{1}{M} \sum_{\substack{x_1, x_2 \\ y_1, y_2}} 1_{\substack{x_2 = x_1 + a \\ y_2 = y_1 + b}} \Pr\left[\begin{matrix} x_1 \overset{C}{\mapsto} y_1 \\ x_2 \mapsto y_2 \end{matrix}\right]. \tag{4}$$

Lemma 13. *For the attack of Fig. 3, we have*

$$\mathrm{Adv}_{\mathrm{Fig.3}}(C) \leq n.\max\left(\frac{1}{M-1}, E\left(\mathrm{DP}^{C}(a,b)\right)\right).$$

Proof. It is straightforward to see that the probability, for some fixed key, that the attack accepts C is

$$1 - \left(1 - \mathrm{DP}^{C}(a,b)\right)^{n}$$

which is less than $n.\mathrm{DP}^{C}(a,b)$. Hence we have $p \leq n.E\left(\mathrm{DP}^{C}(a,b)\right)$. Since from Equation (4) we have $E\left(\mathrm{DP}^{C^*}(a,b)\right) = \frac{1}{M-1}$, we obtain the result. □

Theorem 14. *Let C be a cipher on a group $\mathcal{M}$ of order M. For any basic differential distinguisher (depicted on Fig. 3) of complexity n, we have*

$$\mathrm{Adv}_{\mathrm{Fig.3}}(C) \leq \frac{n}{M-1} + \frac{n}{2}\mathrm{Dec}^{2}_{|||\cdot|||_{\infty}}(C).$$

Proof. Actually we notice that $E\left(\mathrm{DP}^{C^*}(a,b)\right) = \frac{1}{M-1}$ and that

$$\left|E\left(\mathrm{DP}^{C}(a,b)\right) - \frac{1}{M-1}\right| \leq \frac{1}{2}\mathrm{Dec}^{2}_{|||\cdot|||_{\infty}}(C)$$

from Equation (4). □

So, if the pairwise decorrelation bias has the order of $1/M$, basic differential cryptanalysis does not work against C, but with a complexity in the scale of M.

7 Linear Cryptanalysis

Linear cryptanalysis has been invented by Matsui [22, 23] based on the notion of statistical attacks which are due to Gilbert *et al.* [11, 31, 10]. We study here the simpler version of the original attack against pairwise decorrelated ciphers.

In this section we assume[2] that $\mathcal{M} = \mathrm{GF}(2^m)$. The inner dot product $a \cdot b$ in $\mathrm{GF}(2^m)$ is the parity of the bitwise *and* of a and b.

[2] Although it is easy to generalize the notion of linear cryptanalysis over other finite fields, we only consider the characteristic 2 case for a better understanding.

Let C be a cipher on $\mathcal{M}$ and let C^* be the Perfect Cipher.

As in Section 6, we similarly call basic linear cryptanalysis the distinguisher characterized by a pair $(a, b) \in \mathcal{M}^2$ with $b \neq 0$ which is depicted on Fig. 4.

Input: a cipher c, a complexity n, a characteristic (a, b), a set A
1. initialize the counter value u to zero
2. for i from 1 to n do
   (a) pick a random X with a uniform distribution and query for $c(X)$
   (b) if $X \cdot a = c(X) \cdot b$, increment the counter u
3. if $u \in A$, output 1, otherwise output 0

Fig. 4. Linear Distinguisher.

We notice here that the attack depends on the way it accepts or rejects depending on the final counter c value.

As pointed out by Chabaud and Vaudenay [7], linear cryptanalysis is based on the quantity

$$\mathrm{LP}^C(a,b) = \left(2 \Pr_X[X \cdot a = C(X) \cdot b] - 1\right)^2 .$$

(Here we use Matsui's notations taken from [24].) As for differential cryptanalysis, we focus on $E\left(\mathrm{LP}^C(a,b)\right)$, and there is a linear expression of this mean value in term of the pairwise distribution matrix $[C]^2$ which comes from straightforward computations :

$$E(\mathrm{LP}^C(a,b)) = 1 - 2^{2-2m} \sum_{\substack{x_1 \neq x_2 \\ y_1 \neq y_2}} 1_{\substack{x_1 \cdot a = y_1 \cdot b \\ x_2 \cdot a \neq y_2 \cdot b}} \Pr \begin{bmatrix} x_1 \overset{C}{\mapsto} y_1 \\ x_2 \mapsto y_2 \end{bmatrix}. \qquad (5)$$

Lemma 15. *For the attack of Fig. 4 we have*

$$\lim_{n \to +\infty} \frac{\mathrm{Adv}_{\mathrm{Fig.4}}(C)}{n^{\frac{1}{3}}} \leq 9.3 \left(\max\left(\frac{1}{2^m - 1}, E\left(\mathrm{LP}^C(a,b)\right)\right)\right)^{\frac{1}{3}} .$$

Proof. Let N_i be the random variable defined as being 1 or 0 depending on whether or not we have $x \cdot a = c(x) \cdot b$ in the ith iteration. All N_i's are independent and with the same 0-or-1 distribution. Let μ be the probability that $N_i = 1$, for a fixed permutation c. From the

Central Limit Theorem, we can approximate the final quantity u/n to a normal distribution law with mean μ and standard deviation $\sigma = \sqrt{\frac{\mu(1-\mu)}{n}}$. Let A be the set of all accepted u/n quantities. For a fixed c, the probability that the attack accepts is

$$p^c \underset{n\to+\infty}{\sim} \int_{t\in A} \frac{e^{-\frac{(t-\mu)^2}{2\sigma^2}}}{\sigma\sqrt{2\pi}} dt.$$

We let p^c_{eq} denotes the right hand term of this equation. We can compare it to the theoretical expected value p_0 of p^c_{eq} defined by $\mu = \frac{1}{2}$ and $\sigma = \frac{1}{2\sqrt{n}}$ *i.e.*

$$p_0 = \int_{t\in A} \frac{e^{-\frac{(t-\frac{1}{2})^2}{n}}}{\sqrt{2\pi}} 2\sqrt{n} dt.$$

The difference $p^c_{\text{eq}} - p_0$ is maximal when $A = [\tau_1, \tau_2]$ for some values τ_1 and τ_2 which are roots of the Equation

$$\frac{(t-\mu)^2}{\sigma^2} + \log\sigma^2 = 4n\left(t - \frac{1}{2}\right)^2 - \log 4n.$$

Hence, the maximum of the difference $p^c_{\text{eq}} - p_0$ is at most the maximum when $A = [\tau_1, \tau_2]$ over the choice of τ_1 and τ_2, which is the maximum minus the minimum of $p^c_{\text{eq}} - p_0$ when $A =]-\infty, \tau]$. Now we have

$$\int_{-\infty}^{\tau} \frac{e^{-\frac{(t-\mu)^2}{2\sigma^2}}}{\sigma\sqrt{2\pi}} dt = \int_{-\infty}^{\frac{\tau-\mu}{\sigma}} \frac{e^{-\frac{t^2}{2}}}{\sqrt{2\pi}} dt$$

so we have

$$p^c_{\text{eq}} - p_0 \leq \left(\max_{\tau} - \min_{\tau}\right) \int_{2\sqrt{n}(\tau-\frac{1}{2})}^{\sqrt{n}\frac{\tau-\mu}{\sqrt{\mu(1-\mu)}}} \frac{e^{-\frac{t^2}{2}}}{\sqrt{2\pi}} dt.$$

We consider the sum as a function $f(\mu)$ on μ. Since we have $f\left(\frac{1}{2}\right) = 0$, we have $|f(\mu)| \leq B.\left|\mu - \frac{1}{2}\right|$ where B is the maximum of $|f'(x)|$ when x varies from μ to $\frac{1}{2}$. We have

$$f'(x)\sqrt{\frac{2\pi}{n}} = \left(-\frac{1}{\sqrt{x(1-x)}} - \frac{\frac{1}{2}-x}{x(1-x)}\frac{\tau-x}{\sqrt{x(1-x)}}\right) e^{-\frac{n(\tau-x)^2}{2x(1-x)}}$$

so

$$|f'(x)| \leq \sqrt{\frac{n}{2\pi\mu(1-\mu)}} + \frac{\left|\mu - \frac{1}{2}\right|}{\mu(1-\mu)} \frac{e^{-\frac{1}{2}}}{\sqrt{2\pi}} \leq \sqrt{\frac{n}{2\pi\mu(1-\mu)}} + \frac{\left|\mu - \frac{1}{2}\right|}{\mu(1-\mu)}.$$

Therefore we have

$$\left|p^c_{\text{eq}} - p_0\right| \leq 2\sqrt{\frac{n}{2\pi}} \frac{\left|\mu - \frac{1}{2}\right|}{\sqrt{\mu(1-\mu)}} + 2\frac{\left(\mu - \frac{1}{2}\right)^2}{\mu(1-\mu)}. \tag{6}$$

Let $\delta = E\left((2\mu - 1)^2\right)$ over the distribution of C. (We recall that μ depends on the permutation c.) Let $\alpha = \frac{1}{8}\left(\delta\sqrt{\frac{2\pi}{n}}\right)^{\frac{1}{3}}$. Since $\delta \leq 1$ and $n \geq 1$, we have $\alpha \leq .17$ so if $\left|\mu - \frac{1}{2}\right| \leq \alpha$ we have

$$\left|p^c_{\text{eq}} - p_0\right| \leq .55(\delta n)^{\frac{1}{3}}.$$

Now we have $\left|\mu - \frac{1}{2}\right| \geq \alpha$ with a probability less than $\frac{\delta}{4\alpha^2}$, which is less than $8.68(\delta n)^{\frac{1}{3}}$, and in this case we have $\left|p^c_{\text{eq}} - p_0\right| \leq 1$. Hence, we have

$$E\left(\left|p^c_{\text{eq}} - p_0\right|\right) \leq 9.3(\delta n)^{\frac{1}{3}}.$$

We note that $\delta = E\left(\text{LP}^C(a,b)\right)$. We finally note that $E\left(\text{LP}^{C^*}(a,b)\right) = \frac{1}{2^m - 1}$ from Equation (5). □

Theorem 16. *Let C be a cipher on $\mathcal{M} = \{0,1\}^m$. For any linear distinguisher (depicted on Fig. 4) we have*

$$\lim_{n \to +\infty} \frac{\text{Adv}_{\text{Fig.4}}(C)}{n^{\frac{1}{3}}} \leq 9.3 \left(\frac{1}{2^m - 1} + 2\text{Dec}^2_{|||\cdot|||_\infty}(C)\right)^{\frac{1}{3}}.$$

This asymptotic result comes from approximation to the normal law by the Large Number Theorem, which is correct whenever n is not too small (*i.e.* $n > 30$). This result is thus actually valid for any practical n.

Proof. Actually we notice that $E\left(\text{LP}^{C^*}(a,b)\right) = \frac{1}{2^m - 1}$ and that

$$\left|E\left(\text{LP}^C(a,b)\right) - \frac{1}{2^m - 1}\right| \leq 2\text{Dec}^2_{|||\cdot|||_\infty}(C)$$

from Equation (5). □

So, if the pairwise decorrelation bias has the order of 2^{-m}, linear distinguishers does not work against C, but with a complexity in the scale of 2^m.

8 Iterated Attacks of Order d

Theorems 14 and 16 suggest that we try to generalize them to attacks in the model depicted on Fig. 5. In this model, we iterate a d-limited non-adaptive attack $\mathcal{T}$. We assume that this attack obtains a sample (X, Y) with $X = (X_1, \ldots, X_d)$ and $Y = (Y_1, \ldots, Y_d)$ such that $y_i = c(X_i)$ for a given distribution of X. Thus, we can think of a known plaintext attack where X has a fixed distribution (*e.g.* a uniform distribution) or of a chosen plaintext attack where X has a given distribution (*e.g.* in differential cryptanalysis, $X = (X_1, X_1 + a)$ where X_1 has a uniform distribution). The result of the attack depends on the result of all iterated ones in a way characterized by a set A. For instance, if $A = \{0,1\}^n \backslash \{(0, \ldots, 0)\}$ we can define the differential cryptanalysis (thus of order $d = 2$). If A is the set of all $(t_1, \ldots, t_n)$ with an acceptable sum we can define the linear cryptanalysis (of order $d = 1$).

Input: a cipher c, a complexity n, a distribution on X, a test $\mathcal{T}$, an acceptance set A

1. for i from 1 to n do
   (a) get a new $X = (X_1, \ldots, X_d)$
   (b) get $Y = (c(X_1), \ldots, c(X_d))$
   (c) set $T_i = 0$ or 1 with an expected value $\mathcal{T}(X, Y)$
2. if $(T_1, \ldots, T_n) \in A$ output 1 otherwise output 0

Fig. 5. Iterated Attack of Order d.

It is tenting to believe that a cipher resists to this model of attacks once it has a small d-wise decorrelation bias. This is wrong as the following example shows. Let C be a cipher with a perfect d-wise decorrelation. We assume that an instance c of C is totally defined by d (x_i, y_i) points so that C is uniformly distributed in a set of $K = M(M-1)\ldots(M-d+1)$ permutations denoted $c_1, \ldots, c_K$.

From $x = (x_1, \ldots, x_d)$ and $y = (y_1, \ldots, y_d)$ we can define $I(x, y)$ as the unique index k such that $c_k(x_i) = y_i$ for $i = 1, \ldots, d$. We let

$$\mathcal{T}(x, y) = \begin{cases} 1 \text{ if } I(x, y) \equiv 0 \bmod \mu \\ 0 \text{ otherwise} \end{cases}$$

for a given modulus $\mu = n/a$ and

$$\mathcal{A} = \{0, 1\}^n \backslash \{(0, \ldots, 0)\}.$$

If we feed this attack with C or C^*, we have

$$p \approx \frac{1}{\mu} = \frac{a}{n} \text{ and } p^* \approx 1 - \left(1 - \frac{1}{\mu}\right)^n \approx 1 - e^{-a}$$

for $a << n$. Thus Adv can be large even with a relatively large n. This problem actually comes from the fact that the tests $\mathcal{T}$ provide a same expected result for C and C^* but a totally different standard deviation.

We can however prove the security when the cipher has a good decorrelation to the order $2d$.

Theorem 17. *Let C be a cipher on a message space of size M such that $\mathrm{Dec}^{2d}_{|||\cdot|||_\infty}(C) \leq \epsilon$ for some given $d \leq M/2$. For any iterated attack (depicted on Fig. 5) of order d such that the obtained plaintexts are independent, we have*

$$\mathrm{Adv}_{\mathrm{Fig.5}}(C) \leq 3 \left(\left(2\delta + \frac{5d^2}{2M} + \frac{3\epsilon}{2} \right) n^2 \right)^{\frac{1}{3}} + \frac{n\epsilon}{2}$$

where δ is the probability that for two independent X and X' there exists i and j such that $X_i = X'_j$.

For instance, if the distribution of X is uniform, we have $\delta \leq \frac{d^2}{2M}$.

Proof. Let Z (resp. Z^*) be the probability that the test accepts $(X, C(X))$ (resp. $(X, C^*(X))$), *i.e.*

$$Z = E_X(\mathcal{T}(X, C(X))).$$

Let p (resp. p^*) be the probability that the attack accepts, *i.e.*

$$p = \Pr_C[(T_1, \ldots, T_n) \in A].$$

Since the T_is are independent and with the same expected value Z which only depends on C, we have

$$p = E_C\left(\sum_{(t_1,\ldots,t_n)\in A} Z^{t_1+\ldots+t_n}(1-Z)^{n-(t_1+\ldots+t_n)}\right).$$

We thus have $p = E(f(Z))$ where $f(z)$ is a polynomial of degree at most n with values in $[0,1]$ for any $z \in [0,1]$ entries and with the form $f(z) = \sum a_i z^{b_i}(1-z)^{n-b_i}$. It is straightforward that $|f'(z)| \leq n$ for any $z \in [0,1]$. Thus we have $|f(z) - f(z^*)| \leq n|z - z^*|$.

The crucial point in the proof is in proving that $|Z - Z^*|$ is small within a high probability. For this, we need $|E(Z) - E(Z^*)|$ and $|V(Z) - V(Z^*)|$ to be both small.

From Theorem 7 we know that $|E(Z) - E(Z^*)| \leq \frac{\epsilon}{2}$. We note that Z^2 corresponds to a another test but with $2d$ entries, hence we have $|E(Z^2) - E((Z^*)^2)| \leq \frac{\epsilon}{2}$. Hence $|V(Z) - V(Z^*)| \leq \frac{3}{2}\epsilon$. Now from the Tchebichev's Inequality we have

$$\Pr[|Z - E(Z)| > \lambda] \leq \frac{V(Z)}{\lambda^2}.$$

Hence we have

$$|p - p^*| \leq \frac{2V(Z^*) + \frac{3}{2}\epsilon}{\lambda^2} + n\left(\frac{\epsilon}{2} + 2\lambda\right)$$

so, with $\lambda = \left(\frac{2V(Z^*)+\frac{3}{2}\epsilon}{n}\right)^{\frac{1}{3}}$ we have

$$|p - p^*| \leq 3\left(\left(2V(Z^*) + \frac{3\epsilon}{2}\right)n^2\right)^{\frac{1}{3}} + \frac{n\epsilon}{2}.$$

Now we have

$$\begin{aligned} V(Z^*) &= \sum_{\substack{(x,y)\in A \\ (x',y')\in A}} \Pr_X[x]\Pr_X[x']\left(\Pr_{C^*}\begin{bmatrix} x \to y \\ x' \to y' \end{bmatrix} - \Pr_{C^*}[x \to y]\Pr_{C^*}[x' \to y']\right) \\ &\leq \frac{1}{2}\sum_{\substack{x,y \\ x',y'}} \Pr_X[x]\Pr_X[x']\left|\Pr_{C^*}\begin{bmatrix} x \to y \\ x' \to y' \end{bmatrix} - \Pr_{C^*}[x \to y]\Pr_{C^*}[x' \to y']\right|. \end{aligned}$$

The sum over all x and x' entries with colliding entries (*i.e.* with some $x_i = x'_j$) is less than δ. The sum over all y and y' entries with colliding entries and no colliding x and x' is less than $d^2/4M$. The sum over all no colliding x and x' and no colliding y and y' is equal to

$$\frac{1-\delta}{2}\left(1 - \frac{M(M-1)\dots(M-2d+1)}{M^2(M-1)^2\dots(M-d+1)^2}\right)$$

which is less than $\frac{d^2}{2(M-d)}$. Thus we have $V(Z^*) \leq \delta + \frac{d^2}{4M} + \frac{d^2}{2(M-d)}$ which is less than $\delta + \frac{5d^2}{4M}$ when $2d \leq M$.. □

This theorem proves that we need $n = \Omega(1/\sqrt{\epsilon})$ or $n = \Omega(\sqrt{M})$ to have a meaningful iterated attack. If we apply it to linear cryptanalysis, this result is thus weaker than Theorem 16. It is however much more general.

9 COCONUT: a Perfect Decorrelation Design

In this section we define the COCONUT Ciphers family which are perfectly decorrelated ciphers to the order two.

The COCONUT Ciphers are characterized by some parameters (m, p). m is the block length, and p is a irreducible polynomial of degree m in GF(2) (which defines a representation of the GF(2^m) Galois Field). A COCONUT Cipher of block length m is simply a product cipher $C_1 \circ C_2 \circ C_3$ where C_1 and C_3 are any (possibly weak) ciphers which can depend from each other, and C_2 is an independent cipher based on a $2m$-bit key which consists of two polynomials A and B of degree at most $m-1$ over GF(2) such that $A \neq 0$. For a given representation of polynomials into m-bit strings, we simply define

$$C_2(x) = A.x + B \bmod p.$$

Since C_2 performs perfect decorrelation to the order two and since it is independent from C_1 and C_3, any COCONUT Cipher is obviously perfectly decorrelated to the order two. Therefore Theorems 14 and 16 shows that COCONUT resists to the basic differential and linear cryptanalysis.

One can wonder why C_1 and C_3 are for. Actually, C_2 makes some precise attacks provably impractical, but in a way which makes the

cipher obviously weak against other attacks. (C_2 is actually a linear function, thus although we can prove it resists to some attacks which are characterized by some parameter $d \leq 2$, it is fairly weak against attacks of $d = 3$.) We believe that all real attacks on any real cipher have an intrinsic *order* d, that is they use the d-wise correlation in the encryption of d messages. Attacks of a large d on real ciphers are impractical, because the d-wise decorrelation can hardly be analyzed since it depends on too many factors. Therefore, the COCONUT approach consists in making the cipher provably resistant against attacks of order at most 2 such as differential or linear cryptanalysis, and heuristically secure against attacks of higher order by real life ciphers as C_1 and C_3.

The COCONUT98 Cipher has been proposed in [35] with parameters $m = 64$ and $p = x^{64} + x^{11} + x^2 + x + 1$.

10 PEANUT: a Partial Decorrelation Design

In this section we define the PEANUT Ciphers family, which achieves an example of partial decorrelation. This family is based on a combinatorial tool which has been previously used by Halevi and Krawczyk for authentication in [14].

The PEANUT Ciphers are characterized by some parameters (m, r, d, p). They are Feistel Ciphers of block length of m bits (m even), r rounds. The parameter d is the order of partial decorrelation that the cipher performs, and p must be a prime number greater than $2^{\frac{m}{2}}$.

The cipher is defined by a key of $\frac{mrd}{2}$ bits which consists of a sequence of r lists of d $\frac{m}{2}$-bit numbers, one for each round. In each round, the F function has the form

$$F(x) = g(k_1.x^{d-1} + k_2.x^{d-2} + \ldots + k_{d-1}.x + k_d \bmod p \bmod 2^{\frac{m}{2}})$$

where g is any permutation on the set of all $\frac{m}{2}$-bit numbers.

Let us now estimate the decorrelation $|||.|||_\infty$-bias of the PEANUT ciphers.

Lemma 18. *Let* $\mathbf{K} = \mathrm{GF}(q)$ *be a finite field, let* $r : \{0,1\}^{\frac{m}{2}} \to \mathbf{K}$ *be an injective mapping, and let* $\pi : \mathbf{K} \to \{0,1\}^{\frac{m}{2}}$ *be a surjective*

mapping. Let F be a random function defined by

$$F(x) = \pi(r(A_{d-1}).r(x)^{d-1} + \ldots + r(A_0))$$

where the A_i's are independent and uniformly distributed in $\{0,1\}^{\frac{md}{2}}$. We have

$$^f\mathrm{Dec}^d_{|||.|||_\infty}(F) \leq 2\left(\left(\frac{q}{2^{\frac{m}{2}}}\right)^d - 1\right).$$

Proof. Let $x = (x_1, \ldots, x_d)$ be a multi-point in $\{0,1\}^{\frac{m}{2}}$. We want to prove that

$$S = \sum_{y=(y_1,\ldots,y_d)} |[F]^d_{x,y} - [F^*]^d_{x,y}| \leq 2\left(\left(\frac{q}{2^{\frac{m}{2}}}\right)^d - 1\right).$$

Let c be the number of pairwise different x_i's. For any y such that there exists (i,j) such that $y_i \neq y_j$ and $x_i = x_j$, the contribution to the sum is zero. So we can assume that y is defined over the $2^{\frac{cm}{2}}$ choices of y_i's on positions corresponding to pairwise different x_i's. If we let $x_{d+1}, \ldots, x_{2d-c}$ be new fixed points such that we have exactly d pairwise different x_i's, since the probability that F (resp. F^*) maps x onto y is equal to the sum over all choices of $y_{d+1}, \ldots, y_{2d-c}$ that it maps the extended x onto the extended y, we can assume w.l.o.g. that $c = d$.

For any multi-point y we thus have that $\Pr[x \mapsto y] = j.2^{-\frac{md}{2}}$ where j is an integer. Let N_j be the number of multi-points y which verify this property. We have $\sum_j N_j = 2^{\frac{md}{2}}$ and $\sum_j jN_j = 2^{\frac{md}{2}}$. We have

$$S \leq \sum_j N_j \left|\frac{j-1}{2^{\frac{md}{2}}}\right| = 2N_0.2^{-\frac{md}{2}}.$$

N_0 is the number of unreachable y's, *i.e.* the y's which correspond to a polynomial whose coefficients are not all r-images. This number is thus less than the number of missing polynomials which is $q^d - 2^{\frac{md}{2}}$. □

From Theorem 12 with $k = 3$ we thus obtain the following theorem.

Theorem 19. *Let C be a cipher in the PEANUT family with parameters (m, r, d, p). We have*

$$\mathrm{Dec}^d_{|||.|||_\infty}(C) \leq \left(\left(1 + 2\left(p^d 2^{-\frac{md}{2}} - 1\right)\right)^3 - 1 + \frac{2d^2}{2^{\frac{m}{2}}}\right)^{\lfloor \frac{r}{3} \rfloor}.$$

When $p \approx 2^{\frac{m}{2}}$ we can approximate

$$\mathrm{Dec}^d_{|||.|||_\infty}(C) \approx \left(\frac{6d\left(p - 2^{\frac{m}{2}}\right) + 2d^2}{2^{\frac{m}{2}}}\right)^{\lfloor \frac{r}{3} \rfloor}.$$

Example 20. We can use the parameters $m = 64$, $r = 9$, $d = 2$ and $p = 2^{32} + 15$. We obtain that $\mathrm{Dec}^2_{|||.|||_\infty}(C) \leq 2^{-76}$. Therefore from Theorems 14 and 16 no differential or linear distinguisher can be efficient. The PEANUT98 Cipher has been proposed with these parameters in [35].

In an earlier version of this work [34], we proposed a similar construction (say PEANUT97) which uses prime numbers smaller than $2^{\frac{m}{2}}$. However the result above does not hold with the $|||.|||_\infty$ norm, but rather with the $||.||_2$ one. The drawback is that this norm has less friendly theorems for constructing Feistel ciphers, and in particular we need more rounds to make the cipher provably secure. (For more information, see [36].)

11 Conclusion and Further Work

Decorrelation modules are cheap and friendly tools which can strengthen the security of block ciphers. Actually, we can quantify their security against a class of cryptanalysis which includes differential and linear cryptanalysis. To illustrate this paradigm, we proposed two definite prototype ciphers in [35].

Research on other general cryptanalysis is still an open problem. In particular, it is not sure that $2d$-decorrelation is necessary for getting provable security against iterated attacks of order d (Theorem 17).

One problem with the COCONUT or PEANUT construction is that it requires a long key (in order to make the internal random

functions independent). In real-life examples, we can generate this long key by using a pseudorandom generator fed with a short key, but the results on the security based on decorrelation are no longer valid. However, provided that the pseudorandom generator produces outputs which are indistinguishable from truly random sequences, we can still prove the security. This approach has been developed in [12] for submitting a candidate (DFC) to the *Advanced Encryption Standard* process which has been initiated by the U.S. Government.

Acknowledgments

I wish to thank Jacques Stern for valuable help. I also thank the CNRS for having honored this work as one of the 100 "important facts" in engineering advances in France (see [2]).

References

1. Data Encryption Standard. *Federal Information Processing Standard Publication 46*, U. S. National Bureau of Standards, 1977.
2. Méthode de chiffrement fondée sur la décorrélation. In *100 Faits Marquants du Département des Sciences Pour l'Ingénieur*, p. 15, CNRS, 1997.
3. E. Biham, A. Shamir. Differential cryptanalysis of DES-like cryptosystems. In *Advances in Cryptology CRYPTO'90*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 537, pp. 2–21, Springer-Verlag, 1991.
4. E. Biham, A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, vol. 4, pp. 3–72, 1991.
5. E. Biham, A. Shamir. Differential cryptanalysis of the full 16-round DES. In *Advances in Cryptology CRYPTO'92*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 740, pp. 487–496, Springer-Verlag, 1993.
6. E. Biham, A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.
7. F. Chabaud, S. Vaudenay. Links between differential and linear cryptanalysis. In *Advances in Cryptology EUROCRYPT'94*, Perugia, Italy, Lectures Notes in Computer Science 950, pp. 356–365, Springer-Verlag, 1995.
8. L. Carter, M. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, vol. 18, pp. 143–154, 1979.
9. H. Feistel. Cryptography and computer privacy. *Scientific American*, vol. 228, pp. 15–23, 1973.
10. H. Gilbert. *Cryptanalyse Statistique des Algorithmes de Chiffrement et Sécurité des Schémas d'Authentification*, Thèse de Doctorat de l'Université de Paris 11, 1997.
11. H. Gilbert, G. Chassé. A statistical attack of the FEAL-8 cryptosystem. In *Advances in Cryptology CRYPTO'90*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 537, pp. 22–33, Springer-Verlag, 1991.

12. H. Gilbert, M. Girault, P. Hoogvorst, F. Noilhan, T. Pornin, G. Poupard, J. Stern, S. Vaudenay. Decorrelated Fast Cipher: an AES candidate. Submitted.
13. H. M. Heys. *The Design of Substitution-Permutation Network Ciphers Resistant to Cryptanalysis*, Ph.D. Thesis of Queen's University, Kingston, Ontatio, Canada, 1994.
14. S. Halevi, H. Krawczyk. MMH: software message authentication in the Gbit/second rates. In *Fast Software Encryption*, Haifa, Israel, Lectures Notes in Computer Science 1267, pp. 172–189, Springer-Verlag, 1997.
15. H. M. Heys, S. E. Tavares. Substitution-Permutation Networks resistant to differential and linear cryptanalysis. *Journal of Cryptology*, vol. 9, pp. 1–19, 1996.
16. T. Jakobsen, L. R. Knudsen. The interpolation attack on block ciphers. In *Fast Software Encryption*, Haifa, Israel, Lectures Notes in Computer Science 1267, pp. 28–40, Springer-Verlag, 1997.
17. L. R. Knudsen. *Block Ciphers — Analysis, Design and Applications*, Aarhus University, 1994.
18. B. R. Kaliski Jr., M. J. B. Robshaw. Linear cryptanalysis using multiple approximations. In *Advances in Cryptology CRYPTO'94*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 839, pp. 26–39, Springer-Verlag, 1994.
19. X. Lai. *On the Design and Security of Block Ciphers*, ETH Series in Information Processing, vol. 1, Hartung-Gorre Verlag Konstanz, 1992.
20. X. Lai, J. L. Massey, S. Murphy. Markov ciphers and differential cryptanalysis. In *Advances in Cryptology EUROCRYPT'91*, Brighton, United Kingdom, Lectures Notes in Computer Science 547, pp. 17–38, Springer-Verlag, 1991.
21. M. Luby, C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, vol. 17, pp. 373–386, 1988.
22. M. Matsui. Linear cryptanalysis methods for DES cipher. In *Advances in Cryptology EUROCRYPT'93*, Lofthus, Norway, Lectures Notes in Computer Science 765, pp. 386–397, Springer-Verlag, 1994.
23. M. Matsui. The first experimental cryptanalysis of the Data Encryption Standard. In *Advances in Cryptology CRYPTO'94*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 839, pp. 1–11, Springer-Verlag, 1994.
24. M. Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. In *Fast Software Encryption*, Cambridge, United Kingdom, Lectures Notes in Computer Science 1039, pp. 205–218, Springer-Verlag, 1996.
25. S. Murphy, F. Piper, M. Walker, P. Wild. Likehood estimation for block cipher keys. Unpublished.
26. K. Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology EUROCRYPT'91*, Brighton, United Kingdom, Lectures Notes in Computer Science 547, pp. 378–385, Springer-Verlag, 1991.
27. K. Nyberg, L. R. Knudsen. Provable security against a differential cryptanalysis. *Journal of Cryptology*, vol. 8, pp. 27–37, 1995.
28. J. Patarin. *Etude des Générateurs de Permutations Basés sur le Schéma du D.E.S.*, Thèse de Doctorat de l'Université de Paris 6, 1991.
29. J. Patarin. About Feistel schemes with six (or more) rounds. In *Fast Software Encryption*, Paris, France, Lectures Notes in Computer Science 1372, pp. 103–121, Springer-Verlag, 1998.
30. C. E. Shannon. Communication theory of secrecy systems. *Bell system technical journal*, vol. 28, pp. 656–715, 1949.

31. A. Tardy-Corfdir, H. Gilbert. A known plaintext attack of FEAL-4 and FEAL-6. In *Advances in Cryptology CRYPTO'91*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 576, pp. 172–181, Springer-Verlag, 1992.
32. S. Vaudenay. *La Sécurité des Primitives Cryptographiques*, Thèse de Doctorat de l'Université de Paris 7, Technical Report LIENS-95-10 of the Laboratoire d'Informatique de l'Ecole Normale Supérieure, 1995.
33. S. Vaudenay. An experiment on DES — Statistical cryptanalysis. In *3rd ACM Conference on Computer and Communications Security*, New Delhi, India, pp. 139–147, ACM Press, 1996.
34. S. Vaudenay. A cheap paradigm for block cipher security strengthening. Technical Report LIENS-97-3, 1997.
35. S. Vaudenay. Provable security for block ciphers by decorrelation. In *STACS 98*, Paris, France, Lectures Notes in Computer Science 1373, pp. 249–275, Springer-Verlag, 1998.
36. S. Vaudenay. Feistel ciphers with L_2-decorrelation. Submitted.
37. S. Vaudenay. The decorrelation technique home-page. URL:`http://www.dmi.ens.fr/~vaudenay/decorrelation.html`
38. G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the American Institute of Electrical Engineers*, vol. 45, pp. 109–115, 1926.
39. M. N. Wegman, J. L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, vol. 22, pp. 265–279, 1981.