Resistance Against General Iterated Attacks

Serge Vaudenay

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

Abstract. In this paper we study the resistance of a block cipher against a class of general attacks which we call "iterated attacks". This class includes some elementary versions of differential and linear cryptanalysis. We prove that we can upper bound the complexity of the attack by using decorrelation techniques. Our main theorem enables to prove the security against these attacks (in our model) of some recently proposed block ciphers COCONUT98 and PEANUT98, as well as the AES candidate DFC. We outline that decorrelation to the order $2d$ is required for proving security against iterated attacks of order d.

1 Introduction

Since public-key cryptography has been discovered in the late 70s, *proving* the security of cryptographic protocols has been a challenging problem. Recently, the random oracle model [2] and the generic algorithm techniques [34] have introduced new tools for validating cryptographic algorithms. Although much older, the area of symmetric cryptography did not get so many tools.

In the early 90s, Biham and Shamir [3] introduced the notion of differential cryptanalysis and Matsui [18, 19] introduced the notion of linear cryptanalysis, which was a quite general model of attacks. Since then many authors tried to formalize these attacks and study their complexity in order to prove the security of block ciphers against it. Earlier work, initiated by Nyberg [23] was based on algebraic techniques.

Recently, Carter-Wegman's combinatoric notion of "universal functions" [5, 42] has been adapted in context with encryption and the notion of "decorrelation bias" has been formalized [36, 37]. Measurement of the decorrelation (*e.g.* by the decorrelation bias) enables to quantify the security of block ciphers against several classes of attacks. In [36, 37], several real-life block cipher prototypes have been proposed, namely COCONUT98 and PEANUT98. Their decorrelation bias have been measured, and the security against basic versions of differential and linear cryptanalysis (as formalized in the present paper) has been formally proved. Similarly, [7] submitted the DFC candidate to the AES process.

In this paper, we generalize these results in a uniform approach. We introduce the notion of "iterated attack of order d" and we prove how the decorrelation bias can measure the security against any of it. Differential and linear cryptanalysis happen to be included in this class of attacks (differential attacks have an order of 2, and linear attacks have an order of 1). In particular we *prove* the security of the above mentioned block ciphers against any iterated known plaintext attack of order 1.[1]

This paper is organized as follows. First we recall the previous results in decorrelation theory which are interesting for our purpose in Section 2. Our contribution starts in Section 3. We define the class of iterated attack of given order. We prove by a counterexample that decorrelation of order d is not sufficient to thwart all iterated attacks of order d. We then show how decorrelation of order $2d$ gives an upper bound on the efficiency of any iterated attacks of order d. We show how to use this result for a practical block cipher (namely, PEANUT98 or DFC). Finally, in Section 4 we investigate how to use the same techniques for combining several cryptanalysis all together and Section 5 investigates extensions of iterated attacks.

2 Previous Work

2.1 Provable Security for Block Ciphers

The notion of "provable security" is often used in public key cryptography. The area of symmetric encryption has seldom results on provable security, and with rare link with each other.

First of all, Shannon's approach [33] (1949) formalizes the notion of "perfect secrecy". It proves the security of Vernam's cipher [40] (also known as the "one-time-pad"). The drawback is that the key must be at least as long as the plaintext, used only once, and perfectly random (*i.e.* chosen with an unbiased uniform distribution).

The Wegman-Carter [42] (1981) approach enables to construct "provably secure" Message Authentication Code (MAC) algorithms by combining the notion of universal function [5] and Vernam's cipher. It has several refinements (see for instance [11, 9]).

The Luby-Rackoff approach [16] (1988) uses the model of distinguishability (which was well known in the area of pseudorandomness, see [8]), also known as Turing's test, for proving that a random Feistel cipher [6] over messages of m bits is provably secure if we use it less than $2^{\frac{m}{4}}$ times. This has many refinements (*e.g.* see [28–30, 17, 22, 31]). It relies the security of the cipher on the pseudorandomness of the round function, which is indeed hard to achieve (because of the key length) for real-life ciphers. We can for instance mention Knudsen's recent DEAL AES candidate [12] which is based on this construction. Here the "provable" security of DEAL relies on the assumption that DES [1] defines a family of random functions. Although this assumption does not make much sense, this provides a piece of security proof.[2]

---

[1] Iterated attacks of order 1 do not include differential attacks, but the security against differential attacks is proven by other approaches as detailed below.

[2] So far, we are not aware about any result which would formally prove that DEAL is significantly more secure than DES.

Biham and Shamir's attacks [3] gave a new breath to the area of symmetric encryption.

First of all, Lai-Massey's notion of Markov cipher [14,15,13] (1990) enables to formalize the complexity of differential cryptanalysis under the hypothesis of stochastic equivalence which assumes that all keys behave as for the average. An alternate approach due to Nyberg [23–25] makes links with some non-linear properties of the internal substitution boxes of the ciphers.

Finally, the Nyberg-Knudsen construction [26,27] (1992) enables to construct block ciphers which are "provably secure" against differential and linear cryptanalysis. They also gave some prototype examples of real-life ciphers which happened to be weak against more general attacks (see [10]). This construction has been successfully used by Matsui in the MISTY construction [20,21] (1996) which has no known attacks so far.

These independent results have been linked with each other through the decorrelation theory [36,37] (1998).

These notions of provable security must however be interpreted with great care, mostly because it refers to some security results against some kinds of attacks and in some sharply formalized model. It does not refer to the intuitive notion of "unbreakability" and must not be blindly trusted. The Jakobsen-Knudsen's attack [10] against the Nyberg-Knudsen ciphers [27] illustrates that security against some attacks does not provide security against other ones. It may also be possible to attack some trusted algorithms (like RSA [32]) in some real-life model (the RSA PKCS#1 standard) without mathematically breaking the algorithm, as was shown by Bleichenbacher's attack [4]. Some constructions which are proposed by the decorrelation theory happen to be vulnerable against some more general attacks as well.[3] We thus need to keep this warning in mind when dealing with "provable security".

2.2 Decorrelation Theory

In our setup, a block cipher is considered as a random permutation C over a message-block space $\mathcal{M}$. (Here the randomness comes from the random choice of the secret key.) The efficiency of a cryptanalysis can be measured by the average complexity of the algorithm over the distribution of the permutation (*i.e.* of the secret key).

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 $i = 1, \ldots, d$.*

[3] Wagner [41] recently broke the COCONUT98 cipher by a "boomerang attack" which is a kind of intermediate attack approach between differential and higher differential attacks.

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.

In this paper, we consider the following matrix norm over $\mathbf{R}^{\mathcal{M}^d \times \mathcal{M}^d}$ defined by

$$||A|| = \max_x \sum_y |A_{x,y}|$$

for any matrix A.[4]

Definition 2. *Let C be a random permutation over $\mathcal{M}$. We call the quantity $||[C]^d - [C^*]^d||$ the "d-wise decorrelation bias of permutation C" and we denote it $\mathrm{DecP}^d(C)$, where C^* is a uniformly distributed random permutation.*

A decorrelation bias of zero means that for any multi-point $x = (x_1, \ldots, x_d)$ the multi-point $(C(x_1), \ldots, C(x_d))$ has the same distribution of the multi-point $(C^*(x_1), \ldots, C^*(x_d))$, so that C and C^* have the same "decorrelation". Throughout the paper, C^* denotes a uniformly distributed permutation which serves as a reference (which will be called "perfect cipher"). We say that its decorrelation is "perfect". For instance, saying that a cipher C on $\mathcal{M}$ has a perfect pairwise 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 $y_1 \neq y_2$. This notion is fairly similar to the notion of universal functions which was been introduced by Carter and Wegman [5, 42].

The matrix norm property (*i.e.* $||A \times B|| \leq ||A||.||B||$) implies

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

Thus we can built ciphers with arbitrarily small decorrelation bias by iterating a simple cipher as long as its own decorrelation bias is smaller than 1. The security results show that when the decorrelation bias is small, then the complexity of the attack is high.

As an example we mention the simple affine cipher defined by $C(x) = Ax+B$ where $(A, B) \in_U \mathrm{GF}(2^m)^* \times \mathrm{GF}(2^m)$ is a random key. This cipher is perfectly decorrelated to the order 2. It is the basic COCONUT cipher [36].

2.3 Security Model

In the Luby-Rackoff model [16], an attacker is an infinitely powerful Turing machine $\mathcal{A}^{\mathcal{O}}$ which has access to an oracle $\mathcal{O}$. Its aim is to distinguish if the oracle implements a cipher C or the Perfect Cipher C^* by querying it and with a limited number d of inputs. The attacker must finally answer 0 ("reject") or 1 ("accept"). We measure the ability to distinguish C from C^* by the advantage $\mathrm{Adv}_{\mathcal{A}}(C, C^*) = |p - p^*|$ where p (resp. p^*) is the probability of answering 1 if $\mathcal{O}$

[4] This norm is the infinity-associated matrix norm and is usually denoted $|||.|||_\infty$. Other norms have been considered, *e.g.* in [38].

implements C (resp. C^*). In this paper we focus on non-adaptive attacks *i.e.* on distinguishers illustrated on Fig. 1: here no X_i queried to the oracle depends on some previous answers $C(X_j)$. The chosen norm is well suited to this notion of

Parameter: a complexity n
Input: an oracle which implements a function c
1. compute some messages $X = (X_1, \ldots, X_d)$
2. get $Y = (c(X_1), \ldots, c(X_d))$ from the oracle
3. depending on X and Y, output 0 or 1

Fig. 1. A Generic d-Limited Non-Adaptive Distinguisher.

non-adaptive attack as shown by the following result (taken from [36, 37]).

Theorem 3. *Let d be an integer. Let C be a cipher. The best d-limited non-adaptive distinguisher $\mathcal{A}$ for C is such that*

$$\mathrm{Adv}_{\mathcal{A}}(C, C^*) = \frac{1}{2}\mathrm{DecP}^d(C).$$

Thus the decorrelation bias for the $||.||$ norm expresses the best possible advantage for a non-adaptive attack.

For instance, if C is the basic COCONUT cipher and $d = 2$, then the advantage of *any* non-adaptive attack which is limited to 2 queries is zero: this cipher is perfectly secure when used only twice (as one-time pad [40] is perfectly secure when used only once).

2.4 Differential and Linear Cryptanalysis

In this section we assume 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.

We formalize the basic notion of differential (resp. linear) cryptanalysis by the distinguisher which is characterized by a pair $(a, b) \in \mathcal{M}^2$ (and which is called a "characteristic") and which is depicted on Fig. 2 (resp. Fig. 3). Linear cryptanalysis also needs an "acceptance set" B.

These formalizations are somewhat different from the original ones. We claim that they are straightforward adaptations of the original attacks in the Luby-Rackoff model. Actually, the Biham-Shamir's original 3R, 2R and 1R attacks [3] can be considered as implicitly starting with the attack which is depicted on Fig. 2 against the same cipher with 3, 2 or 1 less round. One of the technical problems of differential cryptanalysis is that we do not have access to the explicit output of the oracle so we have to filter the outputs and isolate "good pairs" from "wrong pairs". The (theoretical) differential distinguisher against a cipher diminished by i rounds is thus more efficient than Biham-Shamir's iR basic

Parameters: a complexity n, a characteristic (a,b)
Input: an oracle which implements a function c

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. 2. Differential Distinguisher.

Parameters: a complexity n, a characteristic (a,b), an acceptance set B
Input: an oracle which implements a function c

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 $u \in B$, output 1, otherwise output 0

Fig. 3. Linear Distinguisher.

attack, therefore a lower bound on the complexity of differential distinguishers leads to a lower bound on the complexity on these original attacks.[5] Similarly, Fig. 3 is the heart of Matsui's original attack against DES [19] when c is DES reduced to 14 rounds.

It has been shown (see [36, 37]) that for any differential distinguisher we have

$$\mathrm{Adv}_{\mathrm{Fig.2}}(C, C^*) \leq \frac{n}{2^m - 1} + \frac{n}{2}\mathrm{DecP}^2(C). \tag{1}$$

(In particular, the probability of the differential characteristic which usually introduces a dependency on the key in formal expressions is completely replaced by $\mathrm{DecP}^2(C)$: the complexity analysis of the attack on average on the key uses only the decorrelation bias and does not rely on any unproven assumption such as the hypothesis of stochastic equivalence.[6]) Similarly for any linear distinguisher we have

$$\lim_{n \to +\infty} \frac{\mathrm{Adv}_{\mathrm{Fig.3}}(C, C^*)}{n^{\frac{1}{3}}} \leq 9.3 \left(\frac{1}{2^m - 1} + 2\mathrm{DecP}^2(C) \right)^{\frac{1}{3}}. \tag{2}$$

[5] We outline that further versions and extensions of differential cryptanalysis use more tricks and escape from this model. This is why we refer to the "original" differential cryptanalysis.

[6] This does not mean that no "weak keys" exist, which is wrong in general (DFC happens to have weak keys as shown by Coppersmith). This shows that the attack does not work on average, which implies that the fraction of weak keys is negligible against the average case (indeed, weak keys of DFC consist in a fraction of 2^{-128}).

Therefore the decorrelation bias to the order 2 leads to upper bounds on the best advantages of both differential and linear attacks.

2.5 Some Constructions

In [36], two real-life block ciphers (called COCONUT98 and PEANUT98) have been proposed. They come from the general family constructions COCONUT and PEANUT.

A cipher in the COCONUT family is characterized by some parameters (m,p) where m is the message-block length and p is an irreducible polynomial of degree m in GF(2). The COCONUT98 Cipher corresponds to the parameters $m=64$ and $p=x^{64}+x^{11}+x^2+x+1$. From the construction, any of COCONUT ciphers has a perfect pairwise decorrelation. Therefore from Equations (1) and (2) no differential or linear distinguisher (as formalized on Fig. 2 and 3) can be efficient.

A cipher in the PEANUT family has some parameters (m,r,d,p). Here m is the message-block length, r is the number of rounds (actually, a PEANUT cipher is an r-round Feistel cipher [6]), d is the order of constructed decorrelation, and p is a prime number greater than $2^{\frac{m}{2}}$. The PEANUT98 Cipher corresponds to $m=64$, $r=9$, $d=2$ and $p=2^{32}+15$. It has been shown that the d-wise decorrelation bias of this function has an upper bound which is equal to

$$\left(\left(1+2\left(p^d 2^{-\frac{md}{2}}-1\right)\right)^3-1+\frac{2d^2}{2^{\frac{m}{2}}}\right)^{\lfloor\frac{r}{3}\rfloor} \tag{3}$$

This bound is well approximated by

$$\left(6d\delta+d^2 2^{1-\frac{m}{2}}\right)^{\lfloor\frac{r}{3}\rfloor}$$

where $p=2^{\frac{m}{2}}(1+\delta)$. Hence for the PEANUT98 Cipher we have $\mathrm{DecP}^2(C)\leq 2^{-76}$. The AES DFC candidate is also in the PEANUT family with parameters $m=128$, $r=8$, $d=2$ and $p=2^{64}+13$. Therefore $\mathrm{DecP}^2(C)\leq 2^{-113}$ for it (even if we remove two rounds). Equations (1) and (2) show that differential and linear distinguishers must have a high complexity against both ciphers.

2.6 Several Aspect of the Decorrelation Theory

The approach of the decorrelation theory consists of four important steps.

1. Defining the distance between $[C]^d$ and $[C^*]^d$. We have seen that we can use matrix norms. This paper uses the $|||.|||_\infty$ norm. Some other norms can be considered such as the Euclidean L_2 norm as detailed in [38]. The original concept of universal functions deals with the infinity norm (defined as the maximum of all entries). The choice of the distance is very important, because some norms seem to provide better complexity lower bounds than others.

2. Constructing simple toy random function (which we call "decorrelation modules") with low decorrelation bias. For instance, the PEANUT construction of [36,37] shows how the decorrelation of the $Ax + B \bmod p \bmod 2^{\frac{m}{2}}$ random function (when $(A, B) \in_U \{0,1\}^m$) for a prime p greater than $2^{\frac{m}{2}}$ has a decorrelation bias which is less than $2(p^d 2^{-\frac{md}{2}} - 1)$ for $d = 2$ which is approximately 4δ for $p = 2^{\frac{m}{2}}(1 + \delta)$.
3. Constructing decorrelated ciphers: proving how the decorrelation bias of the decorrelation modules can be inherited by a larger structure. For instance, the PEANUT construction shows how the decorrelation of the previous primitive is inherited by a Feistel network [6] which uses it as a round function. (Which leads to the bound of Equation (3).)
4. Considering classes of attacks and proving how the decorrelation bias of the cipher makes a lower bound for the complexity of the attack. For instance, proving how the decorrelation to the order 2 provides security against the class of differential or linear attacks.

The present paper deals with the fourth step only.

3 Iterated Attacks of Order d

In this section we introduce the notion of "iterated attack".

3.1 Definition

Equations (1) and (2) suggest that we try to generalize them to a model of iterated attacks. Intuitively, this is an attack in which we iterate (independently) n times an elementary distinguisher which is limited to d queries. After performing one elementary distinguisher we get only one bit of information (we will extend this model for more bits in Section 5, but the results of Section 3 and 4 are only applicable with this limitation of one bit). We focus here on non-adaptive attacks.

Definition 4. *Let n and d be some integers and $\mathcal{M}$ be a set. A non-adaptive "iterated distinguisher of order d and complexity n" for a permutation on $\mathcal{M}$ is defined by*

- *a distribution $\mathcal{D}$ on $\mathcal{M}^d$ (a "plaintext distribution"),*
- *a function $\mathcal{T}$ from $\mathcal{M}^{2d}$ to $[0,1]$ (a "test function"),*
- *a function A from $\{0,1\}^n$ to $[0,1]$ (an "acceptance function").*

The distinguisher runs as illustrated on Fig. 4.

Obviously differential and linear distinguishers as formalized on Fig. 2 and 3 are particular cases of iterated attacks (of order 2 and 1 respectively). Namely, if $d = 2$, if the distribution $\mathcal{D}$ is the distribution of $(X, X + a)$ where X has a uniform distribution, if $\mathcal{T}((x_1, x_2), (y_1, y_2))$ is defined to be 1 if $y_2 = y_1 + b$ and 0 otherwise, and finally if $A(t_1, \ldots, t_n)$ is defined to be the product of all t_is, then we get a differential distinguisher with characteristic (a, b). Similarly, if $d = 1$, if $\mathcal{D}$ is uniform, if $\mathcal{T}(x, y)$ is defined to be 1 if $a\cdot x = b\cdot y$ and 0 otherwise and finally if $A(t_1, \ldots, t_n)$ is defined to be 1 if the sum of all t_is is in B and 0 otherwise, then we get a linear distinguisher with characteristic (a, b) and acceptance set B. Iterated attacks of order at most 2 are therefore more general than differential and linear attacks.

Parameters: a complexity n, a plaintext distribution $\mathcal{D}$, a test function $\mathcal{T}$, an acceptance function A

Input: an oracle which implements a function c

1. for i from 1 to n do
   (a) pick a random $X = (X_1, \ldots, X_d)$ with distribution $\mathcal{D}$
   (b) get $Y = (c(X_1), \ldots, c(X_d))$ from the oracle c
   (c) pick a random $T_i \in \{0, 1\}$ with an expected value of $\mathcal{T}(X, Y)$
2. randomly output 0 or 1 with an expected value of $A(T_1, \ldots, T_n)$

Fig. 4. Non-Adaptive Iterated Attack of Order d.

When $\mathcal{D}$ is the uniform distribution, we will refer to "known plaintext iterated attacks".

3.2 A Counterexample

It is tempting 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 with $d = 2$. Let C be the simple $Ax + B$ cipher over $\mathrm{GF}(q)$ where $(A, B) \in_U \mathrm{GF}(q)^* \times \mathrm{GF}(q)$. It has a perfect pairwise decorrelation. Obviously, any $((x_1, x_2), (y_1, y_2))$ sample with $x_1 \neq x_2$ and such that $y_1 = C(x_1)$ and $y_2 = C(x_2)$ enables to get (A, B) as a function $f(x_1, x_2, y_1, y_2)$. Let D be a subset of distinguished values of $\mathrm{GF}(q)^* \times \mathrm{GF}(q)$ with a given cardinality denoted $q(q-1)/\mu$. We use the uniform distribution of all (X_1, X_2) pairs such that $X_1 \neq X_2$ as the plaintext distribution. We define

$$\mathcal{T}((x_1, x_2), (y_1, y_2)) = \begin{cases} 1 \text{ if } f(x_1, x_2, y_1, y_2) \in D \\ 0 \text{ otherwise} \end{cases}$$

and

$$A(t_1, \ldots, t_n) = \begin{cases} 1 \text{ if } (t_1, \ldots, t_n) \neq (0, \ldots, 0) \\ 0 \text{ otherwise} \end{cases}$$

The trick is that all iterations will provide the same answer for C but a random one for C^*. For the corresponding iterated attack we thus have $p = 1/\mu$ and

$$p^* = 1 - \left(1 - \frac{1}{\mu}\right)^n.$$

For $n = 2$ (two iterations only) we have an advantage of $\frac{1}{\mu}\left(1 - \frac{1}{\mu}\right)$ thus we can have a quite large $|p - p^*|$ although C is perfectly pairwise decorrelated, and that we have an iterated attack of order 2. The trick comes from the fact that the test $\mathcal{T}$ provides a same expected result for C and C^* but a totally different standard deviation, which is avoided by decorrelation to the order $2d = 4$ as shown in the next section.

This counterexample shows that decorrelation of order d is not sufficient in general to prove the security against iterated attacks of order d. In some special cases (as for differential attacks) it may however be sufficient. In the next section we show that decorrelation of order $2d$ is sufficient.

3.3 Security Result

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

Theorem 5. *Let C be a cipher on a message space $\mathcal{M}$ of size M such that $\mathrm{DecP}^{2d}(C) \leq \epsilon$ for some given d. For any non-adaptive iterated attack of order d and complexity n which uses a distribution $\mathcal{D}$ (see Fig. 4), we have*

$$\mathrm{Adv}_{\mathtt{Fig.4}}(C, C^*) \leq 3\left(\left(2\delta + \frac{2d^2}{M} + \frac{d^3}{M(M-d)} + \frac{3\epsilon}{2}\right)n^2\right)^{\frac{1}{3}} + \frac{n\epsilon}{2}$$

where δ is the probability that for two independent random X and X' with distribution $\mathcal{D}$ there exists i and j such that $X_i = X'_j$.

In the particular case where $\mathcal{D}$ is the uniform distribution (*i.e.* if we have a known plaintext iterated attack), we have $\delta \leq \frac{d^2}{M}$ so

$$\mathrm{Adv}_{\mathtt{Fig.4}}(C, C^*) \leq 3\left(\left(\frac{4d^2}{M} + \frac{d^3}{M(M-d)} + \frac{3\epsilon}{2}\right)n^2\right)^{\frac{1}{3}} + \frac{n\epsilon}{2}.$$

This result shows that with a low decorrelation bias ϵ we need

$$n = \Omega(\min(\epsilon^{-\frac{1}{2}}, \sqrt{M}))$$

in order to get a significant advantage unless the distribution $\mathcal{D}$ has some special property. For known plaintext attacks, the attacker cannot choose this distribution so this results is meaningful. For other attacks we can wonder what happens if the attacker choose a clever distribution. We believe that the present result can be improved in further work. Actually, if the distribution is such that X_1 is always the same query we get the worse case because $\delta = 1$. Having the same query to the oracle is however a strange way for attacking it and we believe that this strategy does not provide any advantage.[7]

[7] We did not state a theorem in term of known plaintext attack only in order to stimulate further research in this way.

If we apply this Theorem to linear cryptanalysis ($d = 1$ and $\delta = \frac{1}{M}$) we obtain

$$\mathrm{Adv}_{\mathrm{Fig.2}}(C, C^*) \leq 3\left(\left(\frac{4}{M} + \frac{1}{M(M-d)} + \frac{3\epsilon}{2}\right)n^2\right)^{\frac{1}{3}} + \frac{n\epsilon}{2}.$$

This result is weaker than Equation (2). Similarly, in order to apply it to differential distinguisher ($d = 2$ and $\delta \leq \frac{4}{M}$), we need decorrelation to the order 4 although Equation (1) needs decorrelation to the order 2 only. This is the cost of more general results!

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

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

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

$$p = E_C(A(T_1, \ldots, T_n)).$$

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

$$p = E_C\left(\sum_{t_1,\ldots,t_n \in \{0,1\}} A(t_1, \ldots, t_n) Z^{t_1+\ldots+t_n}(1-Z)^{n-(t_1+\ldots+t_n)}\right).$$

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 $f(z) = \sum a_i z^i (1-z)^{n-i}$. 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 3 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 Tchebichev's Inequality we have

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

Hence we have

$$\Pr\left[|Z - Z^*| > \frac{\epsilon}{2} + 2\lambda\right] \leq \frac{2V(Z^*) + \frac{3}{2}\epsilon}{\lambda^2}$$

thus

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

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

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

The variance $V(Z^*)$ is expressed by

$$\sum_{\substack{x,y\\x',y'}} \Pr_{\mathcal{D}^2}[x,x']\mathcal{T}(x,y)\mathcal{T}(x',y')\left(\Pr_{C^*}\begin{bmatrix} x \to y \\ x' \to y'\end{bmatrix} - \Pr_{C^*}[x \to y]\Pr_{C^*}[x' \to y']\right)$$

which is maximal when $\mathcal{T}(x,y)$ is 0 or 1 by linear programming results. Thus

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

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 $d^2/2M$. The sum over all no colliding x and x' and no colliding y and y' is less than

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

which is less than $\frac{d^2}{2(M-d)}$. Thus we have $V(Z^*) \leq \delta + \frac{d^2}{2M} + \frac{d^2}{2(M-d)}$ which is equal to $\delta + \frac{d^2}{M} + \frac{d^3}{2M(M-d)}$. □

3.4 Applications

PEANUT98 is a 9-round Feistel Cipher for message-blocks of size 64 which has been proposed in [36] with a constructed pairwise decorrelation such that $\mathrm{DecP}^2(\mathrm{PEANUT98}) \leq 2^{-76}$ as shown in Section 2.5. From Equation (1) we know that no differential distinguisher with a number of chosen plaintext pairs less than 2^{76} will have an advantage greater than 50%. From Equation (2) we know that no linear distinguisher with a number of known plaintext less than 2^{62} will have an advantage greater than 50%. Now from Theorem 5 we know that no known plaintext iterated attack of order 1 (*e.g.* linear attacks) with a number of known plaintext less than 2^{33} will have an advantage greater than 50%. For linear cryptanalysis, this result is weaker than Equation (2), but more general.

Similarly, DFC is immune against any known plaintext iterated attack of order 1 with a number of known plaintext less than 2^{52} in the sense that the advantage of these attacks will always be less than 50%.

All these results are applicable to the COCONUT98 Cipher as well since its pairwise decorrelation bias is even smaller (it is actually zero).

The threshold of 50% is arbitrary here. If we have an attack with low advantage α, we intuitively want to iterate it at least $1/\alpha$ times in order to get a significant success rate. The complexity is therefore increased accordingly. We thus adopted this symbolic threshold of 50%.

4 On Combining Several Attacks

When several (inefficient) attacks hold against a cipher C, it is natural to wonder whether or not we can combine their effort in order to get an efficient attack. This situation is formalized by changing a few things on Fig. 4 and we can rewrite Theorem 5 in this setting. Firstly, the test in each iteration can be changed. Secondly, n must be considered as relatively small, and d as relatively large: we use a few attacks (n) which have no real limitations (d) on the number of queries. This situation is different from the previous one where we used many attacks (many times the same one actually) of limited order d. For this reason and since we want n to express the complexity we rewrite d into n_i for the ith attack and n into r. The resulting model is illustrated on Fig. 5.

Parameters: several attacks $\mathcal{A}_1, \ldots, \mathcal{A}_r$, an acceptance function A
Input: an oracle which implements a function c
1. for i from 1 to r do in parallel
   (a) perform the attack $\mathcal{A}_i$ against c
   (b) set T_i to the result of the attack
2. randomly output 0 or 1 with an expected value of $A(T_1, \ldots, T_n)$

Fig. 5. Combined Attack.

Theorem 6. *Let C be a cipher on a message space $\mathcal{M}$ of size M. Let $\mathcal{A}_1, \ldots, \mathcal{A}_r$ be r attacks on C with advantages $\mathrm{Adv}_{\mathcal{A}_1}, \ldots, \mathrm{Adv}_{\mathcal{A}_r}$ respectively. For each i, we let n_i denote the number of queries from $\mathcal{A}_i$ and we let $\mathcal{A}_i^2$ denotes the following attack.*

Input: *an oracle which implements a cipher c*
1. *perform the attack $\mathcal{A}_i$ and set a to the result*
2. *perform the attack $\mathcal{A}_i$ and set b to the result*
3. *if $a = b = 1$ output 1 otherwise output 0*

We let $\mathrm{Adv}_{\mathcal{A}_i^2}$ denote its advantage, and δ_i denote the probability that the two $\mathcal{A}_i$ attack executions query c with one input in common. For any combined attack (depicted on Fig. 5) with independent attacks, $\mathrm{Adv}_{\mathrm{Fig.5}}(C, C^*)$ is less than

$$\sum_{i=1}^{r} \left(\mathrm{Adv}_{\mathcal{A}_i} + 3 \left(2\delta_i + \frac{2n_i^2}{M} + \frac{n_i^3}{M(M-d)} + 2\mathrm{Adv}_{\mathcal{A}_i} + \mathrm{Adv}_{\mathcal{A}_i^2} \right)^{\frac{1}{3}} \right).$$

For instance, when the attacks are known plaintext attacks with a plaintext source with uniform distribution, we have $\delta_i \leq \frac{n_i^2}{M}$.

This result does not depend on the decorrelation of the cipher but only upper bound what we can best achieve when combining several attacks. The occurrence of $\mathcal{A}_i^2$ is a little frustrating but is necessary. Section 3.2 is actually a counterexample in which some attack $\mathcal{A}$ is totally inefficient (with an advantage of 0) but with a quite high $\mathrm{Adv}_{\mathcal{A}^2}$.

Proof. As for the proof of Theorem 5, the advantage can be written

$$\mathrm{Adv}_{\mathrm{Fig.5}}(C, C^*) = |E(f(Z_1, \dots, Z_r) - f(Z_1^*, \dots, Z_r^*))|$$

for a polynomial $f(x_1, \dots, x_r)$ of partial degrees at most 1 and with values in $[0,1]$ whenever all entries are in $[0,1]$. All partial derivatives $f_i'(x_1, \dots, x_r)$ are in $[-1,1]$, so we have

$$\mathrm{Adv}_{\mathrm{Fig.5}}(C, C^*) \leq \sum_{i=1}^{r} E(|Z_i - Z_i^*|).$$

We have $|E(Z_i - Z_i^*)| = \mathrm{Adv}_{\mathcal{A}_i}$ and $|E(Z_i^2 - (Z_i^*)^2)| = \mathrm{Adv}_{\mathcal{A}_i^2}$. So, as in the proof of Theorem 5, we obtain

$$\mathrm{Adv}_{\mathrm{Fig.5}}(C, C^*) \leq \sum_{i=1}^{r} \left(\mathrm{Adv}_{\mathcal{A}_i} + 3 \left(2V(Z_i^*) + 2\mathrm{Adv}_{\mathcal{A}_i} + \mathrm{Adv}_{\mathcal{A}_i^2} \right)^{\frac{1}{3}} \right).$$

and finally $V(Z_i^*) \leq \delta_i + \frac{n_i^2}{M} + \frac{n_i^3}{2M(M-d)}$. □

5 Generalization

We can even generalize Theorem 5 in the case where the iterations of the attack produce an information T_i which is not necessarily binary. We outline that if the size of T_i is unlimited, then there is no possible result because the attack has unlimited computation power and it would be able to perform exhaustive search with all information from the queries.

Theorem 7. *Let C be a cipher on a message space of size M such that we have $\mathrm{DecP}^{2d}(C) \leq \epsilon$ for some given d. For any non-adaptive iterated attack of order d and complexity n which uses a distribution $\mathcal{D}$ (see Fig. 4) and where we allow the T_i to be in the set $\{1, \dots, s\}$, we have*

$$\mathrm{Adv}_{\mathrm{Fig.4}}(C, C^*) \leq 3s \left(\left(2\delta + \frac{2d^2}{M} + \frac{d^3}{M(M-d)} + \frac{3\epsilon}{2} \right) n^2 \right)^{\frac{1}{3}} + \frac{ns\epsilon}{2}$$

where δ is the probability that for two independent random X and X' with distribution $\mathcal{D}$ there exists i and j such that $X_i = X_j'$.

Proof. In the proof of Theorem 5, $f(Z)$ is replaced by a polynomial $f(Z_1, \dots, Z_s)$ in term of $Z_j = \Pr[T_i = j]$ for $j = 1, \dots, s$. For two distributions $(z_1, \dots, z_s)$ and $(z_1^*, \dots, z_s^*)$, we have

$$|f(z_1, \dots, z_s) - f(z_1^*, \dots, z_s^*)| \leq n \sum_{i=1}^{s} |z_i - z_i^*|.$$

As in the previous proof we have

$$\Pr\left[|Z_i - Z_i^*| > \frac{\epsilon}{2} + 2\lambda\right] \leq \frac{2V(Z_i^*) + \frac{3}{2}\epsilon}{\lambda^2}$$

for any λ and $V(Z_i^*) \leq \delta + \frac{d^2}{M} + \frac{d^3}{2M(M-d)}$. Hence the situation simply consists in multiplying the lower bound by s. □

6 Conclusion

We showed how to unify differential and linear distinguishers in a general notion of iterated attack. We then proved that decorrelation enables to quantify the security against any iterated attack. This result happened to be applicable to a real life block cipher. Our result are however not so tight because of the use of Tchebichev's Inequality, and it is still an open problem to improve the complexity upper bounds (with Chernov's bounds?). We encourage researches in this direction.

References

1. Data Encryption Standard. *Federal Information Processing Standard Publication 46*, U. S. National Bureau of Standards, 1977.
2. M. Bellare, P. Rogaway. Random Oracles are Practical: a Paradigm for Designing Efficient Protocols. In *1st ACM Conference on Computer and Communications Security*, Fairfax, Virginia, U.S.A., pp. 62–73, ACM Press, 1993.
3. E. Biham, A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.
4. D. Bleichenbacher. Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1. In *Advances in Cryptology CRYPTO'98*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 1462, pp. 1–12, Springer-Verlag, 1998.
5. L. Carter, M. Wegman. Universal Classes of Hash Functions. *Journal of Computer and System Sciences*, vol. 18, pp. 143–154, 1979.
6. H. Feistel. Cryptography and Computer Privacy. *Scientific American*, vol. 228, pp. 15–23, 1973.
7. H. Gilbert, M. Girault, P. Hoogvorst, F. Noilhan, T. Pornin, G. Poupard, J. Stern, S. Vaudenay. Decorrelated Fast Cipher: an AES Candidate. Submitted to the Advanced Encryption Standard process. In *CD-ROM "AES CD-1: Documentation"*, National Institute of Standards and Technology (NIST), August 1998.
8. O. Goldreich, S. Goldwasser, S. Micali. How to Construct Random Functions. In *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science*, Singer Island, U.S.A., pp. 464–479, IEEE, 1984.
9. 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.
10. 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.

11. H. Krawczyk. LFSR-based Hashing and Authentication. In *Advances in Cryptology CRYPTO'94*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 839, pp. 129–139, Springer-Verlag, 1994.
12. L. R. Knudsen. DEAL - A 128-Bit Block Cipher. Presented at the SAC'97 Workshop (Invited Lecture). Submitted to the Advanced Encryption Standard process. In *CD-ROM "AES CD-1: Documentation"*, National Institute of Standards and Technology (NIST), August 1998.
13. X. Lai. *On the Design and Security of Block Ciphers*, ETH Series in Information Processing, vol. 1, Hartung-Gorre Verlag Konstanz, 1992.
14. X. Lai, J. L. Massey. A Proposal for a New Block Encryption Standard. In *Advances in Cryptology EUROCRYPT'90*, Aarhus, Denemark, Lectures Notes in Computer Science 473, pp. 389–404, Springer-Verlag, 1991.
15. 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.
16. M. Luby, C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM Journal on Computing*, vol. 17, pp. 373–386, 1988.
17. S. Lucks. Faster Luby-Rackoff Ciphers. In *Fast Software Encryption*, Cambridge, United Kingdom, Lectures Notes in Computer Science 1039, pp. 189–203, Springer-Verlag, 1996.
18. 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.
19. 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.
20. 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.
21. M. Matsui. New Block Encryption Algorithm MISTY. In *Fast Software Encryption*, Haifa, Israel, Lectures Notes in Computer Science 1267, pp. 54–68, Springer-Verlag, 1997.
22. M. Naor, O. Reingold. On the construction of pseudo-random permutations: Luby-Rackoff revisited. Presented at the Security in Communication Networks Workshop, Amalfi, Italy, 1996. Submitted for publication. `http://www.unisa.it/SCN96/papers/Reingold.ps`
23. 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.
24. K. Nyberg. Differentially Uniform Mapping for Cryptography. In *Advances in Cryptology EUROCRYPT'93*, Lofthus, Norway, Lectures Notes in Computer Science 765, pp. 55–64, Springer-Verlag, 1994.
25. K. Nyberg. Linear Approximation of Block Ciphers. In *Advances in Cryptology EUROCRYPT'94*, Perugia, Italy, Lectures Notes in Computer Science 950, pp. 439–444, Springer-Verlag, 1995.
26. K. Nyberg, L. R. Knudsen. Provable Security against a Differential Cryptanalysis. In *Advances in Cryptology CRYPTO'92*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 740, pp. 566–574, Springer-Verlag, 1993.
27. K. Nyberg, L. R. Knudsen. Provable Security against a Differential Attack. *Journal of Cryptology*, vol. 8, pp. 27–37, 1995.

28. J. Pieprzyk. How to Construct Pseudorandom Permutations from a Single Pseudorandom Functions. In *Advances in Cryptology EUROCRYPT'90*, Aarhus, Denemark, Lectures Notes in Computer Science 473, pp. 140–150, Springer-Verlag, 1991.
29. 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.
30. J. Patarin. How to Construct Pseudorandom and Super Pseudorandom Permutations from One Single Pseudorandom Function. In *Advances in Cryptology EUROCRYPT'92*, Balatonfüred, Hungary, Lectures Notes in Computer Science 658, pp. 256–266, Springer-Verlag, 1993.
31. 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.
32. R. L. Rivest, A. Shamir and L. M. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystem. In *Communications of the ACM*, vol. 21, pp. 120–126, 1978.
33. C. E. Shannon. Communication Theory of Secrecy Systems. *Bell system technical journal*, vol. 28, pp. 656–715, 1949.
34. V. Shoup. Lower Bounds for Discrete Logarithms and Related Problems. In *Advances in Cryptology EUROCRYPT'97*, Konstanz, Germany, Lectures Notes in Computer Science 1233, pp. 256–266, Springer-Verlag, 1997.
35. 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.
36. 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.
37. S. Vaudenay. Provable Security for Block Ciphers by Decorrelation. (Full Paper.) Submitted. Preliminary version available on URL:`ftp://ftp.ens.fr/pub/reports/liens/liens-98-8.A4.ps.Z`
38. S. Vaudenay. Feistel Ciphers with L_2-Decorrelation. To appear in SAC'98, LNCS.
39. S. Vaudenay. The Decorrelation Technique Home-Page. URL:`http://www.dmi.ens.fr/~vaudenay/decorrelation.html`
40. 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.
41. D. Wagner. The Boomerang Attack. Personal communication.
42. 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.