On Provable Security for Conventional Cryptography

Serge Vaudenay

Ecole Polytechnique Fédérale de Lausanne
Serge.Vaudenay@epfl.ch

Abstract Many previous results on the provable security of conventional cryptography have been published so far. We provide here handy tools based on Decorrelation Theory for dealing with them and we show how to make their proof easier. As an illustration we survey a few of these results and we (im)prove some by our technique.
This paper covers results on pseudorandomness of some block cipher constructions and on message authentication code constructions.

Decorrelation theory was introduced in [18–25]. Its first aim was to address provable security in the area of block ciphers in order to prove their security against differential and linear cryptanalysis. As a matter of fact, these techniques can also be used for other areas of conventional cryptography as shown in this paper.

In [25] was noticed that decorrelation distances of some integral order d was linked to the advantage of the best attacks which is limited to d samples in several classes of attacks. Namely, non-adaptive attacks was characterized by decorrelation distance with the $|||.|||_\infty$ norm, chosen input attacks was characterized by decorrelation distance with the $||.||_a$ norm, and chosen input and output attacks was characterized by decorrelation distance with the $||.||_s$ norm. This can be used to address provable security of, say, MAC construction schemes. Due to nice properties of decorrelation distances, some previous results turn out to get simpler and more systematic.

A similar systematic approach was recently addressed by Maurer [11] and it would be interesting to compare both approaches.

1 Definitions and Properties

This section recalls basic facts in decorrelation theory.

1.1 Definitions and Notations

First of all, for any random function F from a set $\mathcal{M}_1$ to a set $\mathcal{M}_2$ and any integer d we associate the "d-wise distribution matrix" which is denoted $[F]^d$, defined in the matrix set $\mathbf{R}^{\mathcal{M}_1^d \times \mathcal{M}_2^d}$ by

$$[F]^d_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)} = \Pr[F(x_1) = y_1, \ldots, F(x_d) = y_d].$$

Given a metric structure D in $\mathbf{R}^{\mathcal{M}_1^d\times\mathcal{M}_2^d}$ we can define the distance between the matrices associated to two random functions F and G. This is the "d-wise decorrelation distance". If G is a random function uniformly distributed in the set of all functions from $\mathcal{M}_1$ to $\mathcal{M}_2$ (we let F^* denote such a function), this distance is called the "d-wise decorrelation bias of function F" and denoted $\mathrm{DecF}^d_D(F)$. When F is a permutation (which will usually be denoted C as for "Cipher") and G is a uniformly distributed permutation (denoted C^*) it is called the "d-wise decorrelation bias of permutation F" and denoted $\mathrm{DecP}^d_D(F)$. In previous results we used the metric structures defined by the norms denoted $||.||_2$ (see [20]), $|||.|||_\infty$, $||.||_a$, $||.||_s$ (see [25]). These four norms are matrix norms, which means that they are norms on $\mathbf{R}^{\mathcal{M}_1^d\times\mathcal{M}_2^d}$ with the property that

$$||A\times B|| \leq ||A||.||B||.$$

This property leads to non-trivial inequalities which can shorten many treatments on the security of conventional cryptography.

Given two random functions F and G from $\mathcal{M}_1$ to $\mathcal{M}_2$ we call "distinguisher between F and G" any oracle Turing machine $\mathcal{A}^O$ which can send $\mathcal{M}_1$-element queries to the oracle O and receive $\mathcal{M}_2$-element responses, and which finally output 0 or 1. In particular the Turing machine can be probabilistic. In the following, the number of queries to the oracle will be limited to d. The distributions on F and G induces a distribution on $\mathcal{A}^F$ and $\mathcal{A}^G$, thus we can compute the probability that these probabilistic Turing machines output 1. The advantage for distinguishing F from G is

$$\mathrm{Adv}_{\mathcal{A}}(F,G) = \Pr\left[\mathcal{A}^F = 1\right] - \Pr\left[\mathcal{A}^G = 1\right].$$

We consider the class Cl^d_{na} of non-adaptive distinguishers limited to d queries, which are distinguishers who must commit to d queries before receiving the responses. Similarly, we consider its extension Cl^d_a of all distinguishers limited to d queries. For instance, these distinguishers can choose the second query with the hint of the first response. Finally, when F and G are permutations, we also consider the extension Cl^d_s of distinguishers limited to d queries but who can query either the function F/G or its inverse F^{-1}/G^{-1}. For any class of distinguishers Cl we will denote

$$\mathrm{Adv}_{\mathrm{Cl}}(F,G) = \max_{\mathcal{A}\in\mathrm{Cl}} \mathrm{Adv}_{\mathcal{A}}(F,G).$$

We notice that if $\mathcal{A}$ is a distinguisher, we can always define a complementary distinguisher $\bar{\mathcal{A}} = 1-\mathcal{A}$ which gives the opposite output. There is no need for investigating the minimum advantage when the class is closed under the complement (which is the case of the above classes) since

$$\mathrm{Adv}_{\bar{\mathcal{A}}}(F,G) = -\mathrm{Adv}_{\mathcal{A}}(F,G).$$

1.2 Properties

The d-wise distribution matrices have the property that if F and G are independent random functions, F from $\mathcal{M}_2$ to $\mathcal{M}_3$ and G from $\mathcal{M}_1$ to $\mathcal{M}_2$, then

$$[F \circ G]^d = [G]^d \times [F]^d.$$

As an illustrative consequence, if F^* is a uniformly distributed random function, we obtain that

$$[F]^d \times [F^*]^d = [F^*]^d \times [F]^d = [F^*]^d.$$

Thus, if we are using a matrix norm $||.||$, we obtain

$$\mathrm{DecF}^d_{||.||}(F \circ G) \leq \mathrm{DecF}^d_{||.||}(F).\mathrm{DecF}^d_{||.||}(G).$$

and the same for permutations. In the sequel we will refer to the multiplicative property of decorrelation biases.

The $|||.|||_\infty$, $||.||_a$, $||.||_s$ have the quite interesting property that they characterize the best advantage of a distinguisher in Cl^d_{na}, Cl^d_a or Cl^d_s.

Lemma 1 ([18, 25]). *For any random functions F and G we have*

$$|||[F]^d - [G]^d|||_\infty = 2.\mathrm{Adv}_{\mathrm{Cl}^d_{na}}(F, G)$$
$$||[F]^d - [G]^d||_a = 2.\mathrm{Adv}_{\mathrm{Cl}^d_a}(F, G)$$

and when F and G are permutations we also have

$$||[F]^d - [G]^d||_s = 2.\mathrm{Adv}_{\mathrm{Cl}^d_s}(F, G).$$

This is quite a useful property which may lead to some non-trivial inequalities. For example, if F_1, ..., F_r are r independent identically distributed random functions from $\mathcal{M}$ to itself, and if F^* denotes a uniformly distributed random function, we have

$$\mathrm{Adv}_{\mathrm{Cl}^d_a}(F_1 \circ \ldots \circ F_r, F^*) \leq 2^{r-1}.\left(\mathrm{Adv}_{\mathrm{Cl}^d_a}(F_1, F^*)\right)^r.$$

There is a simple link between $||.||_s$ and $||.||_a$. Actually, if for any random permutation C on $\mathcal{M}$ we let $\bar{C}$ be defined from $\{0,1\} \times \mathcal{M}$ to $\mathcal{M}$ by

$$\bar{C}(0, x) = C(x) \quad \text{and} \quad \bar{C}(1, x) = C^{-1}(x).$$

Obviously we have

$$||[C_1]^d - [C_2]^d||_s = ||[\bar{C_1}]^d - [\bar{C_2}]^d||_a. \tag{1}$$

Finally we recall the following lemma.

Lemma 2 ([25]). *Let d be an integer, $F_1, \ldots, F_r$ be r independent random function oracles, and $C_1, \ldots, C_s$ be s independent random permutation oracles. We let Ω be a deterministic oracle Turing machine which can access to the previous oracles and an input tape x. It defines a random function $G(x) = \Omega(F_1, \ldots, F_r, C_1, \ldots, C_s)(x)$. We assume that Ω is such that the number of queries to F_i is limited to some integer a_i, and the number of queries to C_j or C_j^{-1} is limited to b_j in total for any $i = 1, \ldots, r$ and any $j = 1, \ldots, s$. We let the F_i^* (resp. C_j^*) be independent uniformly distributed random functions (resp. permutations) on the same range than F_i (resp. C_j) and we let $G^* = \Omega(F_1^*, \ldots, F_r^*, C_1^*, \ldots, C_s^*)$. We have*

$$\mathrm{DecF}^{d}_{||.||_a}(G) \leq \sum_{i=1}^{r} \mathrm{DecF}^{a_i d}_{||.||_a}(F_i) + \sum_{j=1}^{s} \mathrm{DecP}^{b_j d}_{||.||_s}(C_j) + \mathrm{DecF}^{d}_{||.||_a}(G^*).$$

In addition, if the Ω construction defines a permutation G, assuming that computing G^{-1} leads to the same a_i and b_j limits, we have

$$\mathrm{DecF}^{d}_{||.||_s}(G) \leq \sum_{i=1}^{r} \mathrm{DecF}^{a_i d}_{||.||_a}(F_i) + \sum_{j=1}^{s} \mathrm{DecP}^{b_j d}_{||.||_s}(C_j) + \mathrm{DecF}^{f}_{||.||_s}(G^*).$$

This lemma actually separates the problem of studying the decorrelation bias of a construction scheme into the problem of studying the decorrelation biases of its internal primitives F_i and C_j and studying the decorrelation bias of an ideal version G^* with truly random functions inside.

2 Randomness of Cryptographic Primitives Designs

2.1 The Luby-Rackoff Result

Many previous papers on cryptography investigated how much randomness provides such or such design scheme. The Luby-Rackoff result [8] addressed the Feistel construction [5] with truly random rounds. By translating it into our formalism, it turns into the following lemma.

Lemma 3 (Luby-Rackoff 1986 [8]). *Let $F_1^*, F_2^*, F_3^*, F_4^*$ be four independent random function on $\{0,1\}^{\frac{m}{2}}$ with uniform distribution. We have*

$$\mathrm{DecF}^{d}_{||.||_a}(\Psi(F_1^*, F_2^*, F_3^*)) \leq 2d^2.2^{-\frac{m}{2}}$$
$$\mathrm{DecP}^{d}_{||.||_a}(\Psi(F_1^*, F_2^*, F_3^*)) \leq 2d^2.2^{-\frac{m}{2}}$$
$$\mathrm{DecP}^{d}_{||.||_s}(\Psi(F_1^*, F_2^*, F_3^*, F_4^*)) \leq 2d^2.2^{-\frac{m}{2}}.$$

The results hold for Feistel schemes defined from any (quasi)group operation.

(Here $\Psi(F_1, \ldots, F_r)$ is the standard notation introduced by Luby and Rackoff in order to denote a Feistel scheme in which the ith round function is F_i.) This result can be used together with Lemma 2 in order to study the decorrelation bias of a Feistel scheme with independent rounds. This is the basis of the Peanut construction over which the AES candidate DFC [2, 6, 7] is based.

2.2 General Approach

Many other similar results (and extensions) followed the Luby-Rackoff paper. For instance Zheng-Matsumoto-Imai [27] and Patarin's Thesis [13]. We show here how we can make this kind of result easier by using a technique inspired by both Patarin's "H coefficient method" [13, 14] and Maurer [10].

We aim to upper bound the decorrelation bias of a given random function. Our paradigm consists in first proving a combinatorial lemma by using the structure of the random function then using a standard proof given by the following lemma.

Lemma 4. *Let d be an integer. Let F be a random function from a set $\mathcal{M}_1$ to a set $\mathcal{M}_2$. We let $\mathcal{X}$ be the subset of $\mathcal{M}_1^d$ of all $(x_1, \ldots, x_d)$ with pairwise different entries. We let F^* be a uniformly distributed random function from $\mathcal{M}_1$ to $\mathcal{M}_2$. We know that for all $x \in \mathcal{X}$ and $y \in \mathcal{M}_2^d$ the value $[F^*]^d_{x,y}$ is a constant $p_0 = (\#\mathcal{M}_2)^{-d}$. We assume there exists a subset $\mathcal{Y} \subseteq \mathcal{M}_2^d$ and two positive real values ϵ_1 and ϵ_2 such that*

- $|\mathcal{Y}|p_0 \geq 1 - \epsilon_1$
- $\forall x \in \mathcal{X} \quad \forall y \in \mathcal{Y} \quad [F]^d_{x,y} \geq [F^*]^d_{x,y}(1 - \epsilon_2)$.

Then we have $\mathrm{DecF}^d_{||.||_a}(F) \leq 2\epsilon_1 + 2\epsilon_2$.

This lemma intuitively means that if $[F]^d_{x,y}$ is close to $[F^*]^d_{x,y}$ for all x and almost all y, then the decorrelation bias of F is small.

We have a twin lemma for the $||.||_s$ norm. Here, since we can query y as well, the approximation must hold for all x and y.

Lemma 5. *Let d be an integer. Let C be a random permutation on a set $\mathcal{M}$. We let $\mathcal{X}$ be the subset of $\mathcal{M}^d$ of all $(x_1, \ldots, x_d)$ with pairwise different entries. We let F^* be a uniformly distributed random function on $\mathcal{M}$. We let C^* be a uniformly distributed random permutation on $\mathcal{M}$. We have*

- *if $[C]^d_{x,y} \geq [C^*]^d_{x,y}(1 - \epsilon)$ for all x and y in $\mathcal{X}$ then $\mathrm{DecP}^d_{||.||_s}(F) \leq 2\epsilon$*
- *if $[C]^d_{x,y} \geq [F^*]^d_{x,y}(1 - \epsilon)$ for all x and y in $\mathcal{X}$ then $\mathrm{DecP}^d_{||.||_s}(F) \leq 2\epsilon + 2d^2(\#\mathcal{M})^{-1}$.*

Proof. We use the characterization of $\mathrm{DecF}^d_{||.||_a}$ in term of best adaptive distinguisher. We let $\mathcal{A}$ be one d-limited distinguisher between F and F^* with maximum advantage. We can assume w.l.o.g. that all queries to the oracle are pairwise different (we can simulate the distinguisher by replacing repeated queries by dummy queries). The behavior of $\mathcal{A}$ is deterministically defined by the initial random tape ω and the oracle responses $y = (y_1, \ldots, y_d)$. We let x_i denotes the ith query defined by (ω, y). It actually depends on ω and $y_1, \ldots, y_{i-1}$ only. We let $x = (x_1, \ldots, x_d)$ which is assumed to be in $\mathcal{X}$. We let A be the set of all (ω, y) for which $\mathcal{A}$ outputs 0. It is straightforward that

$$\mathrm{Adv}_{\mathcal{A}}(F, F^*) = -\sum_{(\omega,y)\in A} \Pr[\omega] \left([F]^d_{x,y} - [F^*]^d_{x,y}\right).$$

Next we have

$$\mathrm{Adv}_{\mathcal{A}}(F,F^*) \leq \sum_{\substack{(\omega,y)\in A\\ y\in\mathcal{Y}}} \Pr[\omega]\epsilon_2[F^*]^d_{x,y} + \sum_{\substack{(\omega,y)\in A\\ y\notin\mathcal{Y}}} \Pr[\omega][F^*]^d_{x,y}.$$

By relaxing the (ω, y) in the first sum, we observe that it is upper bounded by ϵ_2. (We just have to sum the y_js backward, starting by summing all y_ds, then y_{d-1}, ...) For the second sum, we recall that all x_is are pairwise different, so $[F^*]^d_{x,y}$ is always equal to p_0. This sum is thus less than ϵ_1.

For the $||.||_s$ norm, we simply use the $\bar{F}$ function as in Equation (1). In the case where we approximate $[C]^d_{x,y}$ by $[F^*]^d_{x,y}$, we just notice that

$$[C^*]^d_{x,y} - [F^*]^d_{x,y} \leq [F^*]^d_{x,y} d^2(\#\mathcal{M})^{-1}.$$

□

We can now prove Lemma 3 by using Lemma 4 and 5 but with a quite compact proof.

Proof (Lemma 3). Following the Feistel scheme $F = \Psi(F_1^*, F_2^*, F_3^*)$, we let

$$\begin{aligned} x_i &= (z_i^0, z_i^1) \\ z_i^2 &= z_i^0 + F_1^*(z_i^1) \\ y_i &= (z_i^4, z_i^3) \end{aligned}$$

We let E be the event $z_i^3 = z_i^1 + F_2^*(z_i^2)$ and $z_i^4 = z_i^2 + F_3^*(z_i^3)$ for $i = 1, \ldots, d$. We thus have $[F]^d_{x,y} = \Pr[E]$. We now define

$$\mathcal{Y} = \left\{(y_1, \ldots, y_d); \forall i < j \quad z_i^3 \neq z_j^3\right\}.$$

(This is a set of non-pathologic outputs when computing $[F]^d_{x,y}$.) We can easily check that $\mathcal{Y}$ fulfill the requirements of Lemma 4. Firstly we have

$$|\mathcal{Y}| \geq \left(1 - \frac{d(d-1)}{2} 2^{-\frac{m}{2}}\right) 2^{md}$$

thus we let $\epsilon_1 = \frac{d(d-1)}{2} 2^{-\frac{m}{2}}$. Second, for $y \in \mathcal{Y}$ and any x (with pairwise different entries), we need to consider $[F]^d_{x,y}$. Let E^2 be the event that all z_i^2s are pairwise different over the distribution of F_1^*. We have

$$[F]^d_{x,y} \geq \Pr[E/E^2] \Pr[E^2].$$

For computing $\Pr[E/E^2]$ we know that z_i^3s are pairwise different, as for the z_i^2s. Hence $\Pr[E/E^2] = 2^{-md}$. It is then straightforward that $\Pr[E^2] \geq 1 - \frac{d(d-1)}{2} 2^{-\frac{m}{2}}$ which is $1 - \epsilon_2$. We thus obtain from Lemma 4 that $\mathrm{DecF}^d_{||.||_a}(F) \leq 2d(d-1)2^{-\frac{m}{2}}$. From Lemma 4 it is straightforward that $\mathrm{DecF}^d_{||.||_a}(C^*) \leq d(d-1)2^{-m}$. We thus obtain $\mathrm{DecP}^d_{||.||_a}(F) \leq 2d^2 2^{-\frac{m}{2}}$ for $d \leq 2^{1+\frac{m}{2}}$. Since DecF is always less than 2, it also holds for larger d.

The $||.||_s$-norm case with $C = \Psi(F_1^*, F_2^*, F_3^*, F_4^*)$ is fairly similar with Lemma 5. We let

$$\begin{aligned} x_i &= (z_i^0, z_i^1) \\ z_i^2 &= z_i^0 + F_1^*(z_i^1) \\ y_i &= (z_i^5, z_i^4) \\ z_i^3 &= z_i^5 - F_4^*(z_i^4) \end{aligned}$$

for $i = 1, \ldots, d$. We have

$$[F]_{x,y}^d = \Pr\left[\begin{matrix} z_i^3 = z_i^1 + F_2^*(z_i^2) \\ z_i^4 = z_i^2 + F_3^*(z_i^3) \end{matrix}; i = 1, \ldots, d\right].$$

Let E be this event. If we let E^2 (resp. E^3) be the event that all z_i^2 (resp. z_i^3) are pairwise different, then

$$[F]_{x,y}^d \geq \Pr[E/E^2, E^3] \Pr[E^2, E^3].$$

The E^2 and E^3 events are independent, with probability greater than $1 - \frac{d(d-1)}{2} 2^{-\frac{m}{2}}$ which is $1 - \epsilon$. The probability of E when E^2 and E^3 hold is obviously $2^{-md} = [F^*]_{x,y}^d$. So, $\mathrm{DecP}^d_{||.||_s}(F) \leq 2d^2.2^{-\frac{m}{2}}$. □

2.3 Random Permutations Collection

We collect here a few results taken from the literature, which can be proven by our techniques.

First of all, Zheng-Matsumoto-Imai investigate the pseudorandomness of generalized Feistel transformations. Originally with two branches, they consider having k branches. The first generalization ("type-1 transformation") $\psi_1(f_1, \ldots, f_r)$ is defined by

$$\begin{aligned} &\psi_1(f_1, \ldots, f_r)(x_1, \ldots, x_k) = \\ &\psi_1(f_2, \ldots, f_r)(f_1(x_1) + x_2, x_3, x_4, \ldots, x_k, x_1). \end{aligned}$$

The second generalization ("type-2 transformation") $\psi_2(f_1, \ldots, f_r)$ is similarly defined for k even and r multiple of $\frac{k}{2}$ by

$$\begin{aligned} &\psi_2(f_1, \ldots, f_r)(x_1, \ldots, x_k) = \\ &\psi_2(f_{\frac{k}{2}+1}, \ldots, f_r)(f_1(x_1) + x_2, x_3, f_2(x_3) + x_4, x_5, \ldots, f_{\frac{k}{2}}(x_{k-1}) + x_k, x_1). \end{aligned}$$

And finally the "type-3 transformation" $\psi_3(f_1, \ldots, f_r)$ for r multiple of k:

$$\begin{aligned} &\psi_3(f_1, \ldots, f_r)(x_1, \ldots, x_k) = \\ &\psi_3(f_k, \ldots, f_r)(f_1(x_1) + x_2, f_2(x_2) + x_3, \ldots, f_{k-1}(x_{k-1}) + x_k, x_1). \end{aligned}$$

(We also define $\Psi_\ell()(x) = y$ for $\ell = 1, 2, 3$.)

Lemma 6 (Zheng-Matsumoto-Imai 1989 [27]). *We consider the previous generalizations of Feistel schemes with k branches on $\{0,1\}^m$. For independent uniformly distributed random functions F_1^*, ..., F_{2k-1}^* and an integer d, we have*

$$\mathrm{DecP}^d_{||.||_a}(\Psi_1(F_1^*,\ldots,F_{2k-1}^*)) \le 2(k-1)d^2.2^{-\frac{m}{k}}$$
$$\mathrm{DecP}^d_{||.||_a}(\Psi_2(F_1^*,\ldots,F_{k^2-1}^*)) \le \frac{k^2}{2}d^2.2^{-\frac{m}{k}}$$
$$\mathrm{DecP}^d_{||.||_a}(\Psi_3(F_1^*,\ldots,F_{k^2-1}^*)) \le (k^2-2k+2)d^2.2^{-\frac{m}{k}}.$$

The results hold for generalized Feistel schemes defined from any (quasi)group operation.[1]

(Note that they all generalize Lemma 3 for which $k=2$.)

Proof (sketch). We use Lemma 4 for evaluating DecF. Then we use the triangular inequality

$$\mathrm{DecF}^d(F) \le \mathrm{DecP}^d(F) + \mathrm{DecP}^d(F^*) \le \mathrm{DecP}^d(F) + d^2 2^{-m}.$$

For Ψ_1 we let $\mathcal{Y}$ be the set of all $y=(y_1,\ldots,y_d)$ where $y_i=(y_i^1,\ldots,y_i^k)$ such that we have $y_i^j = y_{i'}^j$ for no $j>1$ and $i<i'$. We get $\epsilon_1=(k-1)\frac{d(d-1)}{2}2^{-\frac{m}{k}}$. We then consider the event in which the first entry after the $k-1$th round takes pairwise different values for $x_1,\ldots,x_d$. Upper bounding the probability when this event occurs we get $\epsilon_2=(k-1)\frac{d(d-1)}{2}2^{-\frac{m}{k}}$. Thus $\mathrm{DecF}^d(F)\le 2(k-1)d(d-1)2^{-\frac{m}{k}}$.

Similarly, for Ψ_2 we let $\mathcal{Y}$ be the set of all y such that we have $y_i^j=y_{i'}^j$ for no even j and $i<i'$. We get $\epsilon_1=\frac{k}{2}\times\frac{d(d-1)}{2}2^{-\frac{m}{k}}$. We consider the event in which all odd entries after the $k-1$th round takes pairwise different values for $x_1,\ldots,x_d$. We get $\epsilon_2=\frac{k}{2}(k-1)\times\frac{d(d-1)}{2}2^{-\frac{m}{k}}$. Thus $\mathrm{DecF}^d(F)\le\frac{k^2}{2}d(d-1)2^{-\frac{m}{k}}$.

For Ψ_3 we let $\mathcal{Y}$ be the set of all y such that we have $y_i^k=y_{i'}^k$ for no $i<i'$. We get $\epsilon_1=\frac{d(d-1)}{2}2^{-\frac{m}{k}}$. We consider the event in which all first $k-1$ entries after the $k-1$th round take pairwise different values for $x_1,\ldots,x_d$. We get $\epsilon_2=(k-1)^2\frac{d(d-1)}{2}2^{-\frac{m}{k}}$. Thus $\mathrm{DecF}^d(F)\le(k^2-2k+2)d(d-1)2^{-\frac{m}{k}}$.

In the three cases, ϵ_2 is evaluated as the number of unexpected equalities between two outputs from a single circuit of depth $k-1$ with k inputs and internal F_j^* and additions times the probability it occurs, which is at most the depth $k-1$ times $2^{-\frac{m}{k}}$.

Now to get DecP from DecF we notice that the obtained upper bound is always $\mathrm{DecF}^d(F)\le Ad(d-1)2^{-\frac{m}{k}}$ for some $A\ge 2$. For $d\le A2^{m-\frac{m}{k}}$ we thus obtain $\mathrm{DecP}^d(F)\le Ad^2 2^{-\frac{m}{k}}$. For larger d, this bound is greater than $A^3 2^{m\left(2-\frac{3}{k}\right)}$ which is greater than 8 since $m\ge k\ge 2$. Since $\mathrm{DecP}^d(F)$ is always less than 2, the bound is thus still valid. □

[1] Here we slightly improved the original result for Ψ_3 from [27] which is

$$\mathrm{DecP}^d_{||.||_a}(\Psi_3(F_1^*,\ldots,F_{k^2-1}^*)) \le k(k-1)d^2.2^{-\frac{m}{k}}.$$

One problem proposed by Schnorr in the late 80's was to extend the Luby-Rackoff result with a single random function. This has been first solved by Pieprzyk when he show that $\Psi(F^*, F^*, F^*, F^* \circ F^*)$ is pseudorandom [16]. In [14], Patarin improved this result by using less rounds by showing that $\Psi(F^*, F^*, F^* \circ \zeta \circ F^*)$ is pseudorandom when ζ is a special fixed function (like for instance the bitwise circular rotation).

Lucks [9] adopted a different approach for reducing the number of random function in Lemma 3: instead of making all functions depend on each other, he tried to "derandomize" the first and last function and to use imbalance Feistel schemes (with branches with different size). This work was followed by Naor and Reingold's [12] who proved the following result.

Lemma 7 (Naor-Reingold 1999 [12]). *Let C_1 and C_2 be two random permutations such that $\mathrm{DecP}^1(C_1) = 0$ and $\mathrm{DecP}^2_{|||.|||_\infty}(C_i) \leq \delta_i$ for $i = 1, 2$. Let F^* be a uniformly distributed random function. We assume that C_1, C_2 and F^* are independent. For any integer d, we have*

$$\mathrm{DecP}^d_{||.||_s}(C_2^{-1} \circ \Psi(F^*, F^*) \circ C_1) \leq d(d-1)\frac{\delta_1 + \delta_2}{2} + 4d^2.2^{-\frac{m}{2}}.$$

The result holds for Feistel schemes defined from any (quasi)group operation.[2]

The $\mathrm{DecP}^1(C_1) = 0$ requirement is quite easy to achieve since for any random C_0 we can construct $C_1(x) = C_0(x) + K$ with an independent uniformly distributed K and we get the requirement. (For any quasigroup addition.)

Proof (sketch). For $C_2^{-1} \circ \Psi(F^*, F^*) \circ C_1(x_i) = y_i$ we let u_i and v_i denote the inputs of the two F^* functions, which are the right half of $C_1(x_i)$ and the left half of $C_2(y_i)$ respectively. Applying Lemma 5 we consider the event that all u_i and v_j are pairwise different. We get

$$\epsilon = \sum_{i<j} \Pr[u_i = u_j] + \sum_{i<j} \Pr[v_i = v_j] + \sum_{i,j} \Pr[u_i = v_j] + d^2.2^{-m}.$$

Let us first consider $\Pr[u_i = u_j]$. We have

$$\Pr[u_i = u_j] = \sum_{\xi_i \neq \xi_j} \Pr[x_i = \xi_i, x_j = \xi_j] \Pr[u(\xi_i) = u(\xi_j)]$$

[2] The original result from [12] was not stated with the same hypothesis. The first result corresponds with $\delta_1 = \delta_2 = 0$ and states

$$\mathrm{DecP}^d_{||.||_s}(C_2^{-1} \circ \Psi(F^*, F^*) \circ C_1) \leq 4d^2.2^{-\frac{m}{2}} + 2d^2.2^{-m}.$$

The second result needs two independent random functions F_1^* and F_2^* and the hypothesis that for any fixed $x \neq y$ the right (resp. left) halves of $C_1(x)$ and $C_1(y)$ (resp. $C_2(x)$ and $C_2(y)$) are equal with probability less than δ. It states

$$\mathrm{DecP}^d_{||.||_s}(C_2^{-1} \circ \Psi(F_1^*, F_2^*) \circ C_1) \leq 2d^2\delta + 2d^2.2^{-m}.$$

where $u(\xi)$ denotes the right half of $C_1(\xi)$ and the probabilities $\Pr[x_i = \xi_i, x_j = \xi_j]$ are taken over the distribution of the distinguisher and the oracle. Hence we have

$$\Pr[u_i = u_j] \leq \max_{\xi_i \neq \xi_j} \Pr[u(\xi_i) = u(\xi_j)].$$

Now we can see that $u(\xi_i) = u(\xi_j)$ defines a distinguisher for C_1 with two non adaptive deterministic queries ξ_i and ξ_j. Hence From $\mathrm{DecP}^2(C_1)_{|||.|||_\infty} \leq \delta_1$ we can get $\Pr[u_i = u_j] \leq \frac{1}{2}\delta_1 + 2^{-\frac{m}{2}}$. The same holds for $\Pr[v_i = v_j]$. Similarly, since $\mathrm{DecP}^1(C_1) = 0$ and u_i and v_j are independent we have $\Pr[u_i = v_j] = 2^{-\frac{m}{2}}$. Hence

$$\epsilon \leq \frac{d(d-1)}{2} \times \frac{\delta_1 + \delta_2}{2} + d(2d-1).2^{-\frac{m}{2}} + d^2.2^{-m}.$$

Thus the result holds when $2d \leq 2^{\frac{m}{2}}$. Since the bound is greater than $2^{\frac{m}{2}}$ in the other case, it also holds for $m > 1$. The trivial $m = 1$ case is later solved by inspection. □

In addition Naor and Reingold presented an alternate scheme with parallel branches which achieves better decorrelation bias.

Other alternate permutation constructions were investigated, for instance by Sugita [17] based on MISTY-like permutations and in [24] based on IDEA-like permutations.

3 Mode of Operation and Similar Constructions

3.1 CBC-MAC

Another family of results was originated by Bellare-Kilian-Rogaway [4]. This paper consider the regular CBC-MAC construction which transforms a block cipher function C into a message authentication code MAC by

$$\mathrm{MAC}(m_1, \ldots, m_\ell) = C(C(\ldots C(m_1) + m_2 \ldots) + m_\ell).$$

We do not really need invertibility for C, so we can use a random function F instead of C. This construction is provably secure when ℓ is fixed, provided that F is already secure. This informal result can be quantified as follows.

Lemma 8 (Bellare-Kilian-Rogaway 1994 [4]). *For any fixed integer ℓ, we consider the function* MAC *defined on ℓ m-bit blocks from a uniformly distributed random function F^* as above. For any d we have* $\mathrm{DecF}^d_{||.||_a}(\mathrm{MAC}) \leq d\ell(d\ell - 1)2^{-m}$.[3]

When F is pseudorandom it becomes trivial from this and Lemma 2 that

$$\mathrm{DecF}^d_{||.||_a}(\mathrm{MAC}) \leq \mathrm{DecF}^{d\ell}_{||.||_a}(F) + d\ell(d\ell - 1)2^{-m}.$$

[3] The original result from [4] is $\mathrm{DecF}^d_{||.||_a}(\mathrm{MAC}) \leq 6d^2\ell^2 2^{-m}$.

Proof (sketch). By using Lemma 4 again, we take $\mathcal{Y}$ equal to full set of $y = (y_1, \ldots, y_d)$. Thus we have $\epsilon_1 = 0$. Let us define the random variable $U_{i,j}$ as the input of the jth F^* computation on the message $x_i = (m_{i,1}, \ldots, m_{i,\ell})$ respectively. We consider the event E that all $U_{i,j}$ for any i and $j < \ell$ are different from the $U_{k,\ell}$ for any k, and all $U_{k,\ell}$ are pairwise different. As usual we obtain

$$\Pr[\mathrm{MAC}(x_i) = y_i; i = 1, \ldots, d] \geq 2^{-md} \Pr[E]$$

since $\Pr[\mathrm{MAC}(x_i) = y_i; i = 1, \ldots, d/E] = 2^{-md}$. Thus we can take $\epsilon_2 = \Pr[\bar{E}]$.

Let Coll be the event that we have an F^*-collision $F^*(U_{i,j}) = F^*(U_{r,s})$ with $U_{i,j} \neq U_{r,s}$ for some values of i, j, r, s with $j < \ell$ and $r < \ell$. Since the number of queries to F^* for this is $d(\ell - 1)$, we have

$$\Pr[\mathrm{Coll}] \leq \frac{d(\ell-1)(d(\ell-1)-1)}{2} 2^{-m}.$$

Now we have

$$\Pr[\bar{E}] \leq \Pr[\mathrm{Coll}] + \Pr[\bar{E} \text{ and } \overline{\mathrm{Coll}}].$$

Let us study the $U_{i,j} = U_{k,\ell}$ event with $j \leq \ell$ and $i \neq k$ if $j = \ell$ when $\overline{\mathrm{Coll}}$ holds. We let r be the smallest positive integer such that $m_{j-r} \neq m_{\ell-r}$ (with the convention that $m_0 \neq m_{\ell-j}$; we notice that if $j = \ell$, since the ith and the kth messages are different we must have $r < \ell$). Since we have no collision on F^* we must have

- either $F^*(U_{i,j-r-1}) + m_{i,j-r} = F^*(U_{k,\ell-r-1}) + m_{k,\ell-r}$ if $r < j - 1$
- or $m_{i,1} = F^*(U_{k,\ell-r-1}) + m_{k,\ell-r}$ if $r = j - 1 < \ell - 1$
- or $F^*(U_{k,\ell-r}) = 0$ if $r = j$.

Since we have no collision all these events hold with probability at most 2^{-m}. Therefore

$$\Pr[\bar{E}] \leq \frac{d(\ell-1)(d(\ell-1)-1)}{2} 2^{-m} + \left((\ell-1)d^2 + \frac{d(d-1)}{2}\right) 2^{-m}.$$

Thus we can take $\epsilon_2 = \frac{d\ell(d\ell-1)}{2} 2^{-m}$. □

3.2 Similar Results

Lemma 8 means that we can make one Fixed-Input-Length (FIL) MAC from one Single-Block-Input (SBI) MAC. There are other related results. Namely we can consider making Variable-Input-Length (VIL) MAC from FIL-MAC (see [1]), or directly from SBI-MAC. We can consider making VIL-encryption from SBI-encryption[4] (see [3]), SBI-MAC from SBI-encryption, and so on. The technique is basically the same and straightforward from our presentation of Lemma 8.

In order to define decorrelation biases for VIL-MAC, we need to face to the problem of having infinite sets. Let for instance F be a random function

[4] This is usually referred to as "mode of operation" in the literature.

defined from $\mathcal{M}_1^*$ to $\mathcal{M}_2$ ($\mathcal{M}_1^*$ is the set of all finite sequences with entries in $\mathcal{M}_1$). We define the $[F]^{q_1,\ldots,q_d}$ matrix with rows defined on $\mathcal{M}_1^{q_1} \times \ldots \times \mathcal{M}_1^{q_d}$ and columns defined on $\mathcal{M}_2^d$. Next we define $\mathrm{DecF}_D^{q_1,\ldots,q_d}(F)$ as the D-distance between $[F]^{q_1,\ldots,q_d}$ and $[F^*]^{q_1,\ldots,q_d}$. We can easily check that all previous theorems remain valid for these definitions. Additionally, we can define

$$\mathrm{DecF}_D^{d,q}(F) = \max_{q_1+\ldots+q_d=q} \mathrm{DecF}_D^{q_1,\ldots,q_d}(F)$$

and still check that $\mathrm{Adv}_{\mathrm{Cl}_a^{d,q}}(F, F^*) = \frac{1}{2}\mathrm{DecF}_{||\cdot||_a}^{d,q}(F)$ where $\mathrm{Cl}_a^{d,q}$ is the class of adaptive attacks limited to d queries with a total length of q blocks.

Here is for instance a VIL-MAC from FIL-MAC construction which improves the An-Bellare result [1].

Lemma 9. *Let F_1 and F_2 be two independent random functions from $\{0,1\}^{m+b}$ to $\{0,1\}^b$. For any ℓ and any $(m_1, \ldots, m_\ell) \in (\{0,1\}^m)^\ell$ we define*

$$\mathrm{MAC}(m_1, \ldots, m_\ell) = F_2(F_1(\ldots F_1(F_1(0, m_1), m_2) \ldots, m_\ell), \ell)$$

where 0 means a b-bit zero string, and ℓ means an m-bit string which represents the ℓ value. Considering distinguishers limited to d queries and a total length of qm bits we have

$$\mathrm{DecF}_{||\cdot||_a}^{d,q} \leq \mathrm{DecF}_{||\cdot||_a}^{q}(F_1) + \mathrm{DecF}_{||\cdot||_a}^{d}(F_2) + q(q-1)2^{-m}.$$

Proof (sketch). As in the proof of Lemma 8 we consider the event E where all F_2 inputs are pairwise different. In Lemma 4 we have $\epsilon_1 = 0$ and $\epsilon_2 = \Pr[\bar{E}]$. If we have two equal F_2 inputs, we must have a collision on F_1, thus $\Pr[\bar{E}] \leq \frac{q(q-1)}{2} 2^{-m}$. □

Note that we can still use

$$\mathrm{MAC}(m_1, \ldots, m_\ell) = F_2(F_1(\ldots F_1(F_1(0, m_1), m_2) \ldots, m_\ell))$$

with F_2 define on $\{0,1\}^m$ (the same construction, but without the message length) and obtain

$$\mathrm{DecF}_{||\cdot||_a}^{d,q} \leq \mathrm{DecF}_{||\cdot||_a}^{q}(F_1) + \mathrm{DecF}_{||\cdot||_a}^{d}(F_2) + q(q+1)2^{-m}.$$

(In the proof, any equal F_2 inputs lead to a collision on F_1 or a preimage of 0.)

We state an ultimate similar result with the CBC-MAC construction.

Lemma 10 ([26]). *Let C_1 and C_2 be two independent uniformly distributed random permutations on $\{0,1\}^m$. For any ℓ and any $(m_1, \ldots, m_\ell) \in (\{0,1\}^m)^\ell$ we define*

$$\mathrm{MAC}(m_1, \ldots, m_\ell) = C_2(C_1(\ldots C_1(C_1(m_1) + m_2) \ldots + m_{\ell-1}) + m_\ell).$$

Considering distinguishers limited to d queries and a total length of qm bits we have

$$\mathrm{DecF}^{d,q}(\mathrm{MAC}) \leq d(d-1)2^{-m} + q(q+1)(1 + q2^{-m})2^{-m}.$$

The result holds for any (quasi)group addition.

Proof (sketch). Using Lemma 4, let $\mathcal{Y}$ be the set of all $y = (y_1, \ldots, y_d)$ with different y_is. We thus have $\epsilon_1 = \frac{d(d-1)}{2} 2^{-m}$. Now for any collection of $x_i = (m_{i,1}, \ldots, m_{i,\ell_i})$ we let

$$U_{i,j} = C_1(\ldots C_1(C_1(m_{i,1}) + m_{i,2}) \ldots + m_{i,j-1}) + m_j.$$

We consider the event E that all U_{i,ℓ_i} are pairwise different. We have

$$[\mathrm{MAC}]_{x,y}^{\ell_1,\ldots,\ell_d} \geq 2^{-md}(1 - \Pr[\bar{E}])$$

therefore we can take $\epsilon_2 = \Pr[\bar{E}] = \Pr[\exists i < r; U_{i,\ell_i} = U_{r,\ell_r}]$.

The $U_{i,\ell_i} = U_{r,\ell_r}$ event reduces to a collision $U_{i,\ell_i - t_{i,r}} = U_{r,\ell_r - t_{i,r}}$ or to a preimage of 0 for C_1. Let Inv be the event that $C_1(U_{i,j}) = 0$ for some i,j, and let Coll be the event that we have $U_{i,j} = U_{r,s}$ for some i,j,r,s such that $(m_{i,1}, \ldots, m_{i,j}) \neq (m_{r,1}, \ldots, m_{r,s})$. We have $\epsilon_2 \leq \Pr[\mathrm{Inv}] + \Pr[\mathrm{Coll}]$.

The probability that any adaptive attack against C_1 finds a preimage of 0 after q queries is obviously less than $\frac{q}{2^m - q}$. Thus $\Pr[\mathrm{Inv}] \leq \frac{q}{2^m - q}$.

We let $\mathcal{I}$ be the set of all $((i,j),(r,s))$ pairs such that $1 \leq j \leq \ell_i$ and $1 \leq s \leq \ell_r$ and $(m_{i,1}, \ldots, m_{i,j}) \neq (m_{r,1}, \ldots, m_{r,s})$. This is the set of all potential $U_{i,j} = U_{r,s}$ collision indices. We define $c(i,j,r,s)$ equal to the set of all (i,j') and (r,s') such that $j' \leq j$ and $s' \leq s$. We define an ordering on $\mathcal{I}$ by

$$((i,j),(r,s)) \leq ((i',j'),(r',s')) \Longleftrightarrow c(i,j,r,s) \subseteq c(i',j',r',s').$$

For $((i,j),(r,s)) \in \mathcal{I}$ we let $\mathrm{Coll}_{i,j,r,s}$ be the event that $((i,j),(r,s))$ is the minimal pair in $\mathcal{I}$ such that $U_{i,j} = U_{r,s}$. We have

$$\Pr[\mathrm{Coll}] \leq \frac{q(q-1)}{2} \max_{((i,j),(r,s)) \in \mathcal{I}} \Pr[\mathrm{Coll}_{i,j,r,s}].$$

For $((i,j),(r,s)) \in \mathcal{I}$, let us consider the $\mathrm{Coll}_{i,j,r,s}$ event. We assume without loss of generality that $s \leq j$. Since we have no previous collision we must have $m_{i,j} \neq m_{r,s}$. Furthermore we must have $U_{i,j-1} \neq U_{r,s-1}$ and $j > 1$, and we need to consider the event

$$C_1(U_{i,j-1}) + m_{i,j} = U_{r,s}.$$

If $U_{i,j-1}$ is equal to some $U_{i',j'}$ with $(i,j-1) \neq (i',j')$ and $(i',j') \in c(i,j,r,s)$, we must have $((i,j-1),(i',j')) \notin \mathcal{I}$ (otherwise we have a previous collision) which means $j' = j-1$ and $i' = r \neq i$ and $(m_{i,1}, \ldots, m_{i,j-1}) = (m_{r,1}, \ldots, m_{r,j-1})$. If $s < j$ we have $U_{i,j} = U_{r,s} = U_{i,s}$ with $((i,j),(i,s)) \in \mathcal{I}$ which contradicts the minimality of the collision. Thus $s = j$, but this contradicts $U_{i,j-1} \neq U_{r,s-1}$. Hence $U_{i,j-1}$ is not equal to some $U_{i',j'}$ with any previously used (i',j'). The distribution of $C_1(U_{i,j-1})$ is thus uniform among a set of at least $2^m - q$ elements and independent of $U_{r,s}$. Hence $\Pr[\mathrm{Coll}_{i,j,r,s}] \leq \frac{1}{2^m - q}$.

Finally we obtain

$$\epsilon_2 \leq \frac{q}{2^m - q} + \frac{q(q-1)}{2} \times \frac{1}{2^m - q} \leq \frac{q(q+1)}{2}(1 + q2^{-m})2^{-m}.$$

□

4 Conclusion

We have shown how to make several results on conventional cryptography more systematic by using decorrelation theory. The new presentation of the results helps to understand and improve them. Namely, we improved a few of the pseudorandomness results. We also improved results related to MAC constructions, and we proved that the encrypted CBC-MAC construction is secure.

References

1. J. H. An, M. Bellare. Constructing VIL-MACs from FIL-MACs: Message Authentication under Weakened Assumptions. In *Advances in Cryptology CRYPTO'99*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 1666, pp. 252–269, Springer-Verlag, 1999.
2. O. Baudron, H. Gilbert, L. Granboulan, H. Handschuh, R. Harley, A. Joux, P. Nguyen, F. Noilhan, D. Pointcheval, T. Pornin, G. Poupard, J. Stern, S. Vaudenay. DFC Update. In Proceedings from the Second Advanced Encryption Standard Candidate Conference, National Institute of Standards and Technology (NIST), March 1999.
3. M. Bellare, P. Rogaway. On the Construction of Variable-Input-Length Ciphers. In *Fast Software Encryption*, Roma, Italy, Lectures Notes in Computer Science 1636, pp. 231–244, Springer-Verlag, 1999.
4. M. Bellare, J. Kilian, P. Rogaway. The Security of Cipher Block Chaining. In *Advances in Cryptology CRYPTO'94*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 839, pp. 341–358, Springer-Verlag, 1994.
5. H. Feistel. Cryptography and Computer Privacy. *Scientific American*, vol. 228, pp. 15–23, 1973.
6. H. Gilbert, M. Girault, P. Hoogvorst, F. Noilhan, T. Pornin, G. Poupard, J. Stern, S. Vaudenay. Decorrelated Fast Cipher: an AES Candidate. (Extended Abstract.) In *Proceedings from the First Advanced Encryption Standard Candidate Conference*, National Institute of Standards and Technology (NIST), August 1998.
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. M. Luby, C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM Journal on Computing*, vol. 17, pp. 373–386, 1988.
9. 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.
10. U. M. Maurer. A Simplified and Generalized Treatment of Luby-Rackoff Pseudorandom permutation generators. In *Advances in Cryptology EUROCRYPT'92*, Balatonfüred, Hungary, Lectures Notes in Computer Science 658, pp. 239–255, Springer-Verlag, 1993.
11. U. M. Maurer. Information-Theoretic Cryptography. Invited lecture. In *Advances in Cryptology CRYPTO'99*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 1666, pp. 47–64, Springer-Verlag, 1999.
12. M. Naor, O. Reingold. On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited. *Journal of Cryptology*, vol. 12, pp. 29–66, 1999.

13. 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.
14. 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.
15. 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.
16. 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.
17. M. Sugita. Pseudorandomness of Block Ciphers with Recursive Structures. Technical Report of IEICE. ISEC97–9.
18. 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.
19. S. Vaudenay. Provable Security for Block Ciphers by Decorrelation. (Full Paper.) Technical report LIENS-98-8, Ecole Normale Supérieure, 1998. URL:`ftp://ftp.ens.fr/pub/reports/liens/liens-98-8.A4.ps.Z`
20. S. Vaudenay. Feistel Ciphers with L_2-Decorrelation. In *Selected Areas in Cryptography*, Kingston, Ontario, Canada, Lectures Notes in Computer Science 1556, pp. 1–14, Springer-Verlag, 1999.
21. S. Vaudenay. The Decorrelation Technique Home-Page. URL:`http://www.dmi.ens.fr/~vaudenay/decorrelation.html`
22. S. Vaudenay. *Vers une Théorie du Chiffrement Symétrique*, Dissertation for the diploma of "habilitation to supervise research" from the University of Paris 7, Technical Report LIENS-98-15 of the Laboratoire d'Informatique de l'Ecole Normale Supérieure, 1998.
23. S. Vaudenay. Resistance Against General Iterated Attacks. In *Advances in Cryptology EUROCRYPT'99*, Prague, Czech Republic, Lectures Notes in Computer Science 1592, pp. 255–271, Springer-Verlag, 1999.
24. S. Vaudenay. On the Lai-Massey Scheme. Technical report LIENS-99-3, Ecole Normale Supérieure, 1999. To appear in Asiacrypt' 99, LNCS, Springer-Verlag.
25. S. Vaudenay. Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness. Technical report LIENS-99-2, Ecole Normale Supérieure, 1999. (To appear in SAC' 99, LNCS, Springer-Verlag.) URL:`ftp://ftp.ens.fr/pub/reports/liens/liens-99-2.A4.ps.Z`
26. S. Vaudenay. Security of CBC-MAC. Submitted.
27. Y. Zheng, T. Matsumoto, and H. Imai. "On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses. In *Advances in Cryptology CRYPTO'89*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 435, pp. 461–480, Springer-Verlag, 1990.