Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness

Serge Vaudenay*

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

Abstract In previous work, security results of decorrelation theory was based on the infinity-associated matrix norm. This enables to prove that decorrelation provides security against non-adaptive iterated attacks. In this paper we define a new matrix norm dedicated to adaptive chosen plaintext attacks. Similarly, we construct another matrix norm dedicated to chosen plaintext and ciphertext attacks.
The formalism from decorrelation enables to manipulate the notion of best advantage for distinguishers so easily that we prove as a trivial consequence a somewhat intuitive theorem which says that the best advantage for distinguishing a random product cipher from a truly random permutation decreases exponentially with the number of terms.
We show that several of the previous results on decorrelation extend with these new norms. In particular, we show that the Peanut construction (for instance the DFC algorithm) provides security against adaptive iterated chosen plaintext attacks with unchanged bounds, and security against adapted iterated chosen plaintext and ciphertext attacks with other bounds, which shows that it is actually super-pseudorandom.
We also generalize the Peanut construction to any scheme instead of the Feistel one. We show that one only requires an equivalent to Luby-Rackoff's Lemma in order to get decorrelation upper bounds.

Since the beginning of conventional cryptography, theory on the formal security of encryption algorithms hardly got foundations. Decorrelation theory enables to deal with randomness and d-wise independence in connexion with security. This provides a way for proving the security against restricted attacks. Other approaches treats unconditional security for encryption in a group structure (see Pliam [11]).

Decorrelation theory provides new directions to design block ciphers with provable security against some classes of standard attacks. Decorrelating to an order of d a block cipher C_K which depends on a random key K roughly consists in making sure that for all d plaintexts $(x_1, \ldots, x_d)$, the corresponding ciphertexts $(C_K(x_1), \ldots, C_K(x_d))$ are uncorrelated. This way, decorrelated functions are generalizations of Maurer's locally random functions [9]. Although the notion of decorrelation is quite intuitive, there is no formal definition of it, but instead several ways to measure it. Decorrelation theory has usually four tasks.

* Part of this work was done while the author was visiting the NTT Laboratories.

1. Defining a measurement for the decorrelation. This usually relies on a matrix norm.
2. Constructing a simple primitive (also called "decorrelation module") with a quite good decorrelation.
3. Constructing cryptographic algorithms with decorrelation modules in such a way that the decorrelation of the primitive can be inherited by the algorithm.
4. Proving that the decorrelation provides security against classes of attacks.

In [13, 14, 17, 18], these issues have been treated with the infinity-associated matrix norm (denoted $|||.|||_\infty$). In particular, it was shown that this norm corresponds to the best advantage of a non-adaptive chosen plaintext attack. The present paper proves the results, but with a quite non-intuitive norm which corresponds to the best advantage of adaptive chosen plaintext attacks, and of adaptive chosen plaintext and ciphertext attacks. In particular we show that previous results on Peanut constructions extend to this setting. In particular, DFC has the same provable security against adaptive iterated chosen plaintext and ciphertext attacks.

This paper address the first three tasks, but hardly deals with the fourth one which may deserve further research.

1 Previous Results

The goal of decorrelation theory is to provide some kinds of formal proof of security on block ciphers. Earlier results was due to Shannon [12] (who show the limits of unconditional security) and Luby and Rackoff [8] (who show how the randomness theory is applicable to provide provable security). Decorrelation theory is mainly based on Carter-Wegman's universal hashing paradigm [2]. As was shown by Wegman and Carter [20], this enables to provide provably secure Message Authentication Codes.

Results on decorrelation have first been published in STACS' 98 [13].[1] In this paper, decorrelation bias was formally defined.

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

Definition 2. *Given a random function F from a given set $\mathcal{M}_1$ to a given set $\mathcal{M}_2$, an integer d, and a distance D over the matrix space $\mathbf{R}^{\mathcal{M}_1^d \times \mathcal{M}_2^d}$, we define the "$d$-wise decorrelation bias of function F" as being the distance*

$$\mathrm{DecF}^d_D(F) = D([F]^d, [F^*]^d)$$

[1] A more complete version (with some error fixed in it) is available in [14].

where F^* is a uniformly distributed random function from $\mathcal{M}_1$ to $\mathcal{M}_2$. Similarly, for $\mathcal{M}_1 = \mathcal{M}_2$, if C is a random permutation over $\mathcal{M}_1$ we define the "d-wise decorrelation bias of permutation C" as being the distance

$$\mathrm{DecP}^d_D(C) = D([C]^d, [C^*]^d)$$

where C^* is a uniformly distributed random permutation over $\mathcal{M}_1$.

In [13, 14], the infinity-associated matrix norm denoted $|||.|||_\infty$ and defined by

$$|||A|||_\infty = \max_{\text{row } i} \sum_{\text{col } j} |A_{i,j}|$$

was considered. For an injection r from $\{0,1\}^m$ to $\mathrm{GF}(q)$ and a surjection π from $\mathrm{GF}(q)$ to $\{0,1\}^m$, it was shown that the random function F defined on $\{0,1\}^m$ by

$$F(x) = \pi\left(r(K_0) + r(K_1)x + \ldots + r(K_{d-1})x^{d-1}\right)$$

for $(K_0, \ldots, K_{d-1})$ uniformly distributed in $\{0,1\}^{dm}$ provides a quite good decorrelation. Namely,

$$\mathrm{DecF}^d_{|||.|||_\infty}(F) \leq 2(q^d.2^{-md} - 1).$$

This construction is called the "NUT-IV decorrelation module" on [16] since there are three other ones.

It was shown that this decorrelation could be inherited by a Feistel network [3] in a construction called "Peanut". Namely, when the round functions of an r-round Feistel network ($r \geq 3$) has a d-wise decorrelation bias less than ϵ, the d-wise decorrelation bias of the whole permutation is less than

$$\left(3\epsilon + 3\epsilon^2 + \epsilon^3 + d^2.2^{1-\frac{m}{2}}\right)^{\left\lfloor \frac{r}{3} \right\rfloor}. \tag{1}$$

It was also shown that decorrelation to the order 2 provides security against differential and linear attacks.

In SAC' 98 [15], the Euclidean norm (denoted $||.||_2$) was proposed, and it was shown that the same results hold for the $d = 2$ case with other upper bounds. These bounds unfortunately provide worse bounds than for the $|||.|||_\infty$ ones, but are applicable to the following decorrelation module for which the $|||.|||_\infty$ is not:

$$F(x) = (K_0 + K_1 x) \bmod p$$

with $(K_0, K_1) \in_U \{0, \ldots, 2^m - 1\}^2$ and a prime $p < 2^m$.

Based on the Peanut construction, an algorithm called "DFC" [4, 5, 1] was submitted to the Advanced Encryption Standard process.

In Eurocrypt' 99 [18], the family of iterated attacks of order d was considered. It was shown that decorrelation to the order $2d$ provides security against iterated attacks of order d.

2 A New Decorrelation Measurement Dedicated to Adaptive Attacks

Let us consider a distinguisher $\mathcal{A}$ which is limited to d queries to an oracle $\mathcal{O}$. Its computation power is unlimited, and its output (0 or 1) can be probabilistic. Its aim is to distinguish if $\mathcal{O}$ implements a random function F_1 or a random function F_2. For this we consider the advantage

$$\mathrm{Adv}^{\mathcal{A}}(F_1, F_2) = \left|\Pr\left[\mathcal{A}^{\mathcal{O}=F_1} = 1\right] - \Pr\left[\mathcal{A}^{\mathcal{O}=F_2} = 1\right]\right|.$$

We say that $\mathcal{A}$ is non-adaptive if all queries can be sent simultaneously to the oracle (in particular, no query depend on the answer to a previous query). A well known result shows that the largest advantage of a non-adaptive chosen plaintext attack corresponds to the $|||.|||_\infty$ norm of $[F_1]^d - [F_2]^d$. Namely, we have

$$\max_{\substack{\mathcal{A} \text{ non-adaptive} \\ \text{chosen plaintext} \\ d\text{-limited}}} \mathrm{Adv}^{\mathcal{A}}(F_1, F_2) = \frac{1}{2}|||[F_1]^d - [F_2]^d|||_\infty.$$

We adapt this result in order to define a new norm which will be denoted $||.||_a$.

Definition 3. *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be two sets, and d be an integer. For a matrix $A \in \mathbf{R}^{\mathcal{M}_1^d \times \mathcal{M}_2^d}$ we define*

$$||A||_a = \max_{x_1} \sum_{y_1} \max_{x_2} \sum_{y_2} \ldots \max_{x_d} \sum_{y_d} |A_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)}|.$$

Theorem 4. *For any random functions F_1 and F_2 from a set $\mathcal{M}_1$ to a set $\mathcal{M}_2$ and any integer d, we have*

$$\max_{\substack{\mathcal{A} \text{ distinguisher} \\ d\text{-limited}}} \mathrm{Adv}^{\mathcal{A}}(F_1, F_2) = \frac{1}{2}||[F_1]^d - [F_2]^d||_a.$$

Proof. Let $\mathcal{A}$ be a distinguisher. It first queries with a random X_1 (where the randomness comes from $\mathcal{A}$ only), then get a random Y_1 (whose randomness also comes from $\mathcal{O}$). Then it queries a random X_2 which depends on X_1 and Y_2, and get a Y_2, ... At the end, $\mathcal{A}$ answers a random value $A = 0$ or 1. We have

$$\Pr\left[\mathcal{A}^{\mathcal{O}} = 1\right] = \sum_{x_1, y_1, \ldots, x_d, y_d} \Pr[x_1] \Pr[y_1/x_1] \ldots \Pr[A = 1/x_1 \ldots y_d].$$

Let $p_i = \Pr\left[\mathcal{A}^{\mathcal{O}=F_i} = 1\right]$. Since the randomness of $\mathcal{A}$ and F_i are independent, we have

$$p_i = \sum_{x_1, y_1, \ldots, x_d, y_d} \Pr[x_1] \Pr[x_2/x_1, y_1] \ldots \Pr[A = 1/x_1 \ldots y_d][F_i]^d_{x,y}$$

where $x = (x_1, \ldots, x_d)$ and $y = (y_1, \ldots, y_d)$. This is a sum of terms of the form $\Pr[x_1]f(x_1)$. Obviously, the advantage is maximal when $\Pr[x_1] = 1$ for the maximal $f(x_1)$. Actually, we show that this sum is maximal for some deterministic distinguisher in which x_j is a function of $y_1, \ldots, y_{j-1}$ only. We have

$$p_1 - p_2 = \sum_y a_y \left([F_1]^d_{x,y} - [F_2]^d_{x,y}\right)$$

where a_y is 0 or 1. Obviously, this difference is maximal if a_y is 1 for the positive terms, and 0 for the negative terms. We notice that the sum of all terms is 0. Hence we have

$$|p_1 - p_2| = \frac{1}{2}\sum_y \left|[F_1]^d_{x,y} - [F_2]^d_{x,y}\right|$$

when it is maximal. The choice of x which maximizes this sum completes the proof. □

In order to deal with decorrelation biases, it is pleasant to have matrix norms, *i.e.* norms such that $||A \times B|| \leq ||A||.||B||$. If we have such a norm, we actually have the following property

$$\mathrm{DecP}^d_{||.||}(C_1 \circ C_2) \leq \mathrm{DecP}^d_{||.||}(C_1).\mathrm{DecP}^d_{||.||}(C_2) \tag{2}$$

and the same for $\mathrm{DecF}_{||.||}$. The following result says it is applicable for the $||.||_a$ norm.

Theorem 5. *$||.||_a$ is a matrix norm.*

Proof. We make an induction on d. Let A be a matrix in $\mathbf{R}^{\mathcal{M}_1^d \times \mathcal{M}_2^d}$. To each $x_1 \in \mathcal{M}_1$ and each $x_2 \in \mathcal{M}_2$ we associate a submatrix $\pi_{x_1,y_1}(A)$ in $\mathbf{R}^{\mathcal{M}_1^{d-1} \times \mathcal{M}_2^{d-1}}$ defined by

$$(\pi_{x_1,y_1}(A))_{(x_2,\ldots,x_d),(y_2,\ldots,y_d)} = A_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)}.$$

These submatrices actually define a matrix $\pi(A)$ which is basically a different way of viewing A. We have the following property which links the corresponding norms for the parameters d and $d-1$

$$||A||_a = \max_{x_1} \sum_{y_1} ||\pi_{x_1,y_1}(A)||_a.$$

Let A and B be two matrices. We have

$$||A \times B||_a = \max_{x_1} \sum_{y_1} ||\pi_{x_1,y_1}(A \times B)||_a.$$

Straightforward computations show that

$$\pi_{x_1,y_1}(A \times B) = \sum_{t_1} \pi_{x_1,t_1}(A) \times \pi_{t_1,y_1}(B).$$

Thus by induction we have

$$\begin{aligned}||A \times B||_a &= \max_{x_1} \sum_{y_1} \sum_{t_1} ||\pi_{x_1,t_1}(A) \times \pi_{t_1,y_1}(B)||_a \\ &\leq \max_{x_1} \sum_{y_1} \sum_{t_1} ||\pi_{x_1,t_1}(A)||_a.||\pi_{t_1,y_1}(B)||_a.\end{aligned}$$

This last expression is actually a $|||.|||_\infty$ norm of the product of two matrices A' and B' defined by

$$(A')_{x_1,t_1} = ||\pi_{x_1,t_1}(A)||_a$$

and

$$(B')_{t_1,y_1} = ||\pi_{t_1,y_1}(B)||_a.$$

We already know that $|||.|||_\infty$ is a matrix norm. Therefore we have

$$\begin{aligned}||A \times B||_a &\leq |||A' \times B'|||_\infty \\ &\leq |||A'|||_\infty.|||B'|||_\infty\end{aligned}$$

which is $||A||_a.||B||_a$. □

As in [13, 14], this theorem implies the following properties.

Corollary 6. *For any random function $F_1, \ldots, F_4$, if F^* denotes a random function with uniform distribution, the following properties hold.*

$$\mathrm{DecF}^d_{||.||_a}(F_1 \circ F_2) \leq \mathrm{DecF}^d_{||.||_a}(F_1).\mathrm{DecF}^d_{||.||_a}(F_2) \tag{3}$$

$$||[F_1 \circ F_2]^d - [F_1 \circ F_3]^d||_a \leq \mathrm{DecF}^d_{||.||_a}(F_1).||[F_2]^d - [F_3]^d||_a \tag{4}$$

$$\begin{aligned}||[F_1 \circ F_2]^d - [F_3 \circ F_4]^d||_a \leq{}& \mathrm{DecF}^d_{||.||_a}(F_1).||[F_2]^d - [F_4]^d||_a \\ &+\mathrm{DecF}^d_{||.||_a}(F_4).||[F_1]^d - [F_3]^d||_a\end{aligned} \tag{5}$$

Similar properties hold for permutations.

We outline that Equation (3) means that if F_1 and F_2 are two independent random functions with the same distribution and if α is the best advantage of a d-limited distinguisher between F_1 and a uniformly distributed random function F^*, then the best advantage of a d-limited distinguisher between $F_1 \circ F_2$ and F^* is less than $2\alpha^2$. Similarly, for r rounds, the best advantage is less than $\frac{1}{2}(2\alpha)^r$: the advantage decreases exponentially with the number of rounds.

3 On the NUT-IV Decorrelation Module

The DFC algorithm is a Peanut construction which uses the following decorrelation module.

$$F(x) = (Ax + B) \bmod (2^{64} + 13) \bmod 2^{64}$$

where $(A, B) \in_U \{0, \ldots, 2^{64} - 1\}^2$. This is a particular case of the NUT-IV decorrelation module for which we prove the same bound for its decorrelation bias, but with the $||.||_a$ norm.

Theorem 7. *For an integer m, let $q = 2^m(1+\delta)$ be a prime power with $\delta > 0$. We consider an injection r from $\{0,1\}^m$ to $\mathrm{GF}(q)$, and a surjection π from $\mathrm{GF}(q)$ to $\{0,1\}^m$. We define the following random function on $\{0,1\}^m$.*

$$F(x) = \pi\left(r(A_0) + r(A_1).r(x) + \ldots + r(A_{d-1}).r(x)^{d-1}\right)$$

where $(A_0, \ldots, A_{d-1}) \in \{0,1\}^{md}$. We have

$$\mathrm{DecF}^d_{||\cdot||_a}(F) \leq 2\left((1+\delta)^d - 1\right).$$

Proof. We adapt the proof of [14]. We let F^* be a uniformly distributed random function. In the computation of $||[F]^d - [F^*]^d||_a$, let x_1, $x_2 = f_2(y_1)$, $\ldots$ $x_d = f_d(y_1, \ldots, y_{d-1})$ such that

$$\sum_{y=(y_1,\ldots,y_d)} |[F]^d_{x,y} - [F^*]^d_{x,y}|$$

is maximal, where $x = (x_1, \ldots, x_d)$.

For some terms in the sum, some x_i may be equal to each other. For this we need to make a transformation in order to assume that all x_is are pairwise different. For any (x, y) term, let c be the total number of different x_is. Let σ be a monotone injection from $\{1, \ldots, c\}$ to $\{1, \ldots, d\}$ such that all $x_{\sigma(i)}$ are different. We notice that if $x_i = x_j$, we can restrict the sum to $y_i = y_j$ (because the other terms will be all zero). We thus still have $x'_i = x_{\sigma(i)} = f'_i(y'_1, \ldots, y'_{i-1})$ where $y'_i = y_{\sigma(i)}$, and all x'_i are pairwise different for $i = 1, \ldots, c$. We can now define $x'_{c+1}, \ldots, x'_d$ with some new arbitrary functions $f'_{c+1}, \ldots, f'_d$ in such a way that all x'_i are pairwise different. We have

$$\begin{aligned}
\mathrm{DecF}^d_{||\cdot||_a}(F) &= \sum_{y'_1,\ldots,y'_c} \left| \sum_{y'_{c+1},\ldots,y'_d} \left([F]^d_{x',y'} - [F^*]^d_{x',y'}\right) \right| \\
&\leq \sum_{y'_1,\ldots,y'_d} |[F]^d_{x',y'} - [F^*]^d_{x',y'}|
\end{aligned}$$

where $x' = (x'_1, \ldots, x'_d)$ and $y' = (y'_1, \ldots, y'_d)$. Hence we can assume without loss of generality that all x_is are pairwise different.

Obviously, $[F]^d_{x,y}$ can be written $j.2^{-md}$ where j is an integer. Let N_j be the number of y such that $[F]^d_{x,y} = j.2^{-md}$. We have

$$\begin{aligned}
\mathrm{DecF}^d_{||\cdot||_a}(F) &\leq \sum_{j=0}^{+\infty} N_j |j-1| 2^{-md} \\
&= 2N_0.2^{-md} + \sum_{j=0}^{+\infty} N_j j.2^{-md} - \sum_{j=0}^{+\infty} N_j.2^{-md}.
\end{aligned}$$

The first sum is equal to

$$\sum_y [F]^d_{x,y}$$

which is equal to 1. The second sum is 2^{-md} times the total number of y, which is also 1. Thus we have $\mathrm{DecF}^d_{||.||_a}(F) \leq 2N_0.2^{-md}$.

Let A be the set of all (x, y) such that $[F]^d_{x,y} = 0$. Let B be the set of all $(a_0, \ldots, a_{d-1})$ in $\mathrm{GF}(q)^d$ such that for at least one j we have $a_j \notin r(\{0,1\}^m)$. From usual interpolation tricks, we know that for any (x, y) in A there exists at least one $(a_0, \ldots, a_{d-1})$ in $\mathrm{GF}(q)^d$ such that

$$\pi(a_0 + a_1.r(x_j) + \ldots + a_{d-1}.r(x_j)^{d-1}) = y_j$$

for $j = 1, \ldots, d$. Since $[F]^d_{x,y} = 0$ this must be in B. Furthermore this mapping from A to B must be an injection. Hence N_0, which is the cardinality of A is less than the cardinality of B which is $q^d - 2^{md}$. □

4 Decorrelation of Peanut-like Constructions

We show here that the decorrelation of internal decorrelation modules in a cipher can be inherited by the whole scheme.

Lemma 8. *Let d be an integer, and $F_1, \ldots, F_r$ be r random functions which are use in order to define a random function $\Omega(F_1, \ldots, F_r)$. We assume that the Ω structure is such that for any x, computing $\Omega(F_1, \ldots, F_r)(x)$ requires a_i computations of F_i for $i = 1, \ldots, r$. We have*

$$||[\Omega(F_1, \ldots, F_r)]^d - [\Omega(F_1^*, \ldots, F_r^*)]^d||_a \leq \sum_{i=1}^{r} \mathrm{DecF}^{a_i d}_{||.||_a}(F_i)$$

where $F_1^*, \ldots, F_r^*$ are uniformly distributed random functions.

Proof. By triangular inequalities, we have

$$||[\Omega(F_1, \ldots, F_r)]^d - [\Omega(F_1^*, \ldots, F_r^*)]^d||_a \leq$$
$$\sum_{i=1}^{r} ||[\Omega(F_1, \ldots, F_{i-1}, F_i^*, \ldots, F_d^*)]^d - [\Omega(F_1, \ldots, F_i, F_{i+1}^*, \ldots, F_d^*)]^d||_a.$$

From Theorem 4, each term corresponds to the best distinguisher between $\Omega(F_1, \ldots, F_{i-1}, F_i^*, \ldots, F_d^*)$ and $\Omega(F_1, \ldots, F_i, F_{i+1}^*, \ldots, F_d^*)$. This attack can be transformed into a distinguisher between F_i and F_i^* by simulating the other functions. Hence this attack cannot have an advantage greater than the best attack for distinguishing F_i from F_i^* with the same number of queries. The number of queries for this attack is at most $a_i d$. By applying back Theorem 4, we obtain the result. □

This lemma can be considered as a "meta-theorem" which is applicable to any product cipher construction. For instance, for the Feistel construction $\Psi(F_1, \ldots, F_r)$, we have $a_i = 1$ for all i. The Peanut construction consists of picking decorrelated modules as round functions. In order to finish to estimate the decorrelation of Feistel structures, we need a lemma in order to estimate the decorrelation of Feistel ciphers with truly random functions. This is precisely the Luby-Rackoff [8] Lemma.

Lemma 9 (Luby-Rackoff 1988). *Let F_1^*, F_2^*, F_3^* be three random function on $\{0,1\}^{\frac{m}{2}}$ with uniform distribution. We have*

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

(This is a straightforward translation of the original result by using Theorem 4.) We can thus upper bound the decorrelation bias in a Peanut construction.

Corollary 10. *If $F_1, \ldots, F_r$ are r random function ($r \geq 3$) on $\{0,1\}^{\frac{m}{2}}$ such that $\mathrm{DecF}^d_{||.||_a}(F_i) \leq \epsilon$, we have*

$$\mathrm{DecP}^d_{||.||_a}(\Psi(F_1, \ldots, F_r)) \leq (3\epsilon + 2d^2.2^{-\frac{m}{2}})^{\lfloor \frac{r}{3} \rfloor}.$$

We note that this slightly improves Equation (1) taken from [13, 14].

Proof. Since the best advantage cannot increase when we make a product of independent ciphers, Lemma 9 holds for any Feistel cipher with at least three rounds. We write $\Psi(F_1, \ldots, F_r)$ as a product of $\lfloor \frac{r}{3} \rfloor$ Feistel ciphers with at least 3 rounds. We apply Lemma 8 and Lemma 9 to each of it, and we finally apply Equation (2). □

As another example, we mention this lemma taken from [10].

Lemma 11 (Patarin 1992). *Let ζ be a permutation on $\{0,1\}^{\frac{m}{2}}$ such that for any y there exists at least λ values x such that $x \oplus \zeta(x) = y$. Given a uniformly distributed random function F^* on $\{0,1\}^{\frac{m}{2}}$ and an integer d, we have*

$$\mathrm{DecP}^d_{||.||_a}(\Psi(F^*, F^*, F^* \circ \zeta \circ F^*)) \leq 13d^2 2^{-\frac{m}{2}} + 2\lambda d 2^{-\frac{m}{2}}$$

Corollary 12. *Let ζ be a permutation on $\{0,1\}^{\frac{m}{2}}$ such that for any y there exists at least λ values x such that $x \oplus \zeta(x) = y$. Given independent random functions $F_1, \ldots, F_r$ on $\{0,1\}^{\frac{m}{2}}$ and an integer d, we have*

$$\begin{aligned}&\mathrm{DecP}^d_{||.||_a}(\Psi(F_1, F_1, F_1 \circ \zeta \circ F_1, \ldots, F_r, F_r, F_r \circ \zeta \circ F_r)) \\ &\leq \left(13d^2 2^{-\frac{m}{2}} + 2\lambda d 2^{-\frac{m}{2}} + \epsilon\right)^r\end{aligned}$$

where $\epsilon = \max_i \mathrm{DecF}^{4d}_{||.||_a}(F_i)$.

Other product constructions require an equivalent to Lemma 9. For instance, the Lai-Massey scheme which is used in IDEA [7, 6] has an equivalent result. (See [19].)

5 Super-Pseudorandomness

We now address the problem of d-limited adaptive chosen plaintext and ciphertext distinguishers. Since the proofs are essentially the same, we do not give all details here. We first define the corresponding norm.

Definition 13. *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be two sets, and d be an integer. For a matrix $A \in \mathbf{R}^{\mathcal{M}_1^d \times \mathcal{M}_2^d}$ we let $\pi_{x_1,y_2}(A)$ denote the matrix in $\mathbf{R}^{\mathcal{M}_1^{d-1} \times \mathcal{M}_2^{d-1}}$ defined by*

$$(\pi_{x_1,y_1}(A))_{(x_2,\ldots,x_d),(y_2,\ldots,y_d)} = A_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)}.$$

By induction on d we define

$$||A||_s = \max\left(\max_{x_1}\sum_{y_1}||\pi_{x_1,y_2}(A)||_s, \max_{y_1}\sum_{x_1}||\pi_{x_1,y_2}(A)||_s\right)$$

with the convention that $||A||_s = |A_{(),()}|$ for $d = 0$.

Since chosen ciphertext makes sense for permutation only, all the following results hold for permutations.

Theorem 14. *For any random permutation C_1 and C_2 over a set $\mathcal{M}$ and any integer d, we have*

$$\max_{\substack{\mathcal{A}\text{ distinguisher}\\ \text{chosen plaintex and ciphertext}\\ d-\text{limited}}} \mathrm{Adv}^{\mathcal{A}}(C_1, C_2) = \frac{1}{2}||[C_1]^d - [C_2]^d||_s.$$

The proof is a straightforward adaptation of the proof of Theorem 4.

Theorem 15. *$||.||_s$ is a matrix norm.*

For this proof, we adapt the proof of Theorem 5 and notice that

$$\max_{y_1}\sum_{x_1}|M_{x_1,y_1}| = |||M|||_1$$

where $|||.|||_1$ is the matrix norm associated to the L_1 vector norm. Therefore Corollary 6 holds for the $||.||_s$ norm with permutations.

We can also extend Lemma 8.

Lemma 16. *Let d be an integer, $F_1, \ldots, F_r$ be r random functions and let $C_1, \ldots, C_s$ be s random permutations which are used in order to define a random permutation $C = \Omega(F_1, \ldots, F_r, C_1, \ldots, C_s)$. We assume that the Ω structure is such that for any x and y, computing $C(x)$ or $C^{-1}(y)$ requires a_i computations of F_i for $i = 1, \ldots, r$ and b_i computations of C_i or C_i^{-1} for $i = 1, \ldots, s$. We have*

$$\begin{aligned}&||[\Omega(F_1, \ldots, F_r, C_1, \ldots, C_s)]^d - [\Omega(F_1^*, \ldots, F_r^*, C_1^*, \ldots, C_s^*)]^d||_s\\ &\leq \sum_{i=1}^{r}\mathrm{DecF}^{a_i d}_{||.||_a}(F_i) + \sum_{i=1}^{s}\mathrm{DecP}^{b_i d}_{||.||_s}(C_i)\end{aligned}$$

where $F_1^*, \ldots, F_r^*$ are uniformly distributed random functions and $C_1^*, \ldots, C_s^*$ are uniformly distributed random permutations.

For instance, in the Peanut construction, we have $s = 0$ and $a_i = 1$ for all i. However Lemma 9 is not applicable with the $||.||_s$ norm. We thus use a similar lemma for 4-round Feistel ciphers.

Lemma 17 (Luby-Rackoff 1988). *Let $F_1^*, F_2^*, F_3^*, F_4^*$ be four random function on $\{0,1\}^{\frac{m}{2}}$ with uniform distribution. We have*

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

We can therefore measure the decorrelation in the sense of $||.||_s$ of Peanut constructions.

Corollary 18. *If $F_1, \ldots, F_r$ are r random function ($r \geq 4$) on $\{0,1\}^{\frac{m}{2}}$ such that $\mathrm{DecF}^d_{||.||_a}(F_i) \leq \epsilon$, we have*

$$\mathrm{DecP}^d_{||.||_s}(\Psi(F_1, \ldots, F_r)) \leq (4\epsilon + 2d^2.2^{-\frac{m}{2}})^{\lfloor \frac{r}{4} \rfloor}.$$

This shows how much super-pseudorandom a Peanut construction is.

6 Security by Decorrelation with the New Norms

We already know that the decorrelation with the $|||.|||_\infty$ norm enables to prove the security against differential, linear distinguishers and non-adaptive chosen plaintext iterated attacks. Since we have $||.||_s \geq ||.||_a \geq |||.|||_\infty$, all these results are applicable to the decorrelation with the $||.||_a$ and $||.||_s$ norms.

From the proofs in [18] it is quite clear that all results on iterated attack extends to $||.||_a$-decorrelation when each iteration is adaptive, and to $||.||_s$-decorrelation when they can use chosen ciphertexts in addition.

One open question remains from the iterated attacks results. In [18] it was shown that the security proof requires some assumption on the distribution of the queries to the oracle. This was meaningful when we addresses the known plaintext non-adaptive attacks. But now adaptive attacks are chosen plaintext in essence. It thus remains to improve the results from [18] in order to get provable security against these attacks.

7 Conclusion

We have shown which matrix norm adaptive attacks and chosen plaintext and ciphertext attacks was related to. These norms define a much stronger notion of decorrelation. We have shown that previous upper bounds on the decorrelation extends to these new norms, in particular for the Peanut construction and the NUT-IV decorrelation module. We also generalized the Peanut construction to any scheme which is not necessarily a Feistel one. We have shown that if it is a product scheme, then we can upper bound the decorrelation of the whole scheme from the decorrelation of its internal functions, provided that we can extend the Luby-Rackoff Lemma to this scheme.

Our formalism happens to be practical enough in order to make trivial the exponential decreasing of the best advantage of a distinguisher between a product cipher and a truly random cipher.

Acknowledgment

I wish to thank NTT and Tatsuaki Okamoto for providing a good environment for research activities, and his team for enjoyable meetings and fruitful discussions.

References

1. 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.
2. L. Carter, M. Wegman. Universal Classes of Hash Functions. *Journal of Computer and System Sciences*, vol. 18, pp. 143–154, 1979.
3. H. Feistel. Cryptography and Computer Privacy. *Scientific American*, vol. 228, pp. 15–23, 1973.
4. 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.
5. 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.
6. X. Lai. *On the Design and Security of Block Ciphers*, ETH Series in Information Processing, vol. 1, Hartung-Gorre Verlag Konstanz, 1992.
7. 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.
8. M. Luby, C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM Journal on Computing*, vol. 17, pp. 373–386, 1988.
9. 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.
10. 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.
11. J. O. Pliam. Bounding Guesswork and Variation Distance: A New Technique for Provable Cipher Security. In these proceedings.
12. C. E. Shannon. Communication Theory of Secrecy Systems. *Bell system technical journal*, vol. 28, pp. 656–715, 1949.
13. 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.
14. 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`

15. 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.
16. S. Vaudenay. The Decorrelation Technique Home-Page.
URL:`http://www.dmi.ens.fr/~vaudenay/decorrelation.html`
17. 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.
18. 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.
19. S. Vaudenay. On the Lai-Massey Scheme. Technical report LIENS-99-3, Ecole Normale Supérieure, 1999. To appear in Asiacrypt' 99, LNCS, Springer-Verlag.
URL:`ftp://ftp.ens.fr/pub/reports/liens/liens-99-3.A4.ps.Z`
20. 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.