On the Lai-Massey Scheme

Serge Vaudenay*

Ecole Normale Supérieure — CNRS
e-mail: `Serge.Vaudenay@ens.fr`

Abstract Constructing a block cipher requires to define a random permutation, which is usually performed by the Feistel scheme and its variants. In this paper we investigate the Lai-Massey scheme which was used in IDEA. We show that we cannot use it "as is" in order to obtain results like Luby-Rackoff Theorem. This can however be done by introducing a simple function which has an orthomorphism property. We also show that this design offers nice decorrelation properties, and we propose a block cipher family called Walnut.

Designing a block cipher requires to build a random permutation from a random key. In most of block cipher constructions, we distinguish two approaches. First we use a fixed network with parallel permutations which are modified at their inputs or outputs by subkey values. This was used for instance in Safer [11] and Square [3]. Second we use the Feistel scheme [4] (or one of its variants) which starts from a random function (see Fig. 1). This was used for instance in DES [1] and Blowfish [14]. The literature gives an extra construction which is not in these categories and which was used in the IDEA cipher [9, 8]. It uses a simple scheme which we illustrated on Fig. 2 and which we call the "Lai-Massey scheme" throughout the paper. As for the Feistel scheme, this structure relies on a group structure.

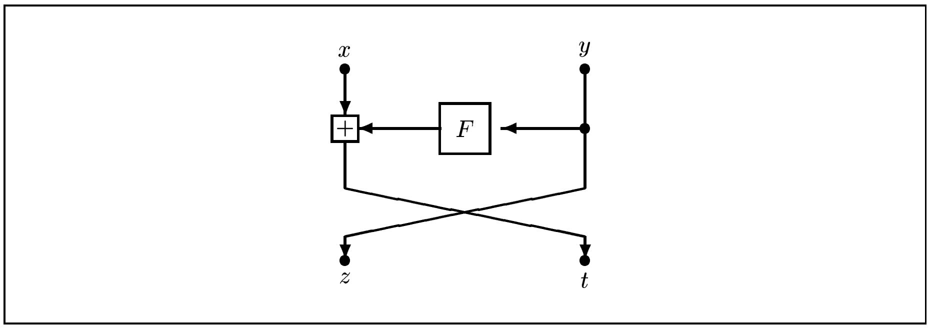

Figure1. The Feistel Scheme.

---

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

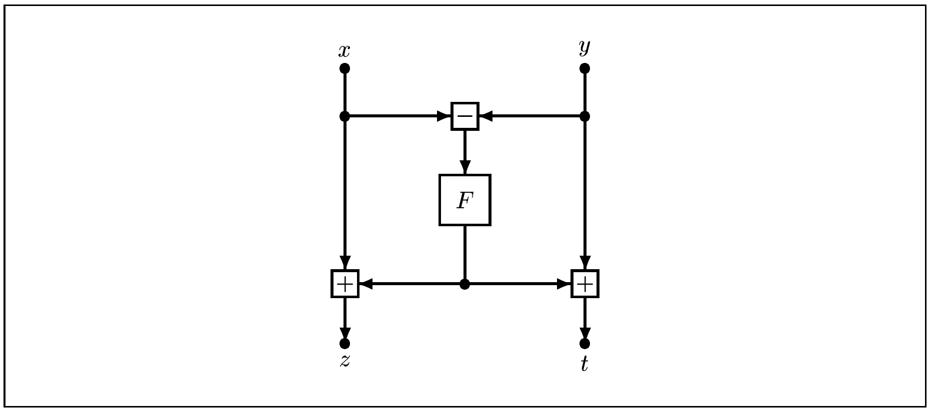

Figure2. The Lai-Massey Scheme.

For the Feistel scheme, Luby and Rackoff [10] proved that if the round functions are random, then a 3-round Feistel cipher will look random to any chosen plaintext attack when the number of chosen plaintexts d is negligible towards $2^{\frac{m}{4}}$ (where m is the block length). In this paper, we show a similar result for the Lai-Massey scheme if we add a simple function σ which has the orthomorphism property: it must be such that σ and $x \mapsto \sigma(x) - x$ are both permutations.

The Luby-Rackoff result however holds when the round functions are random. This has been extended by the decorrelation theory [18–22] when the round function have some decorrelation property. This was used to define the Peanut construction family in which the DFC cipher [2, 5, 6] is an example. We show that we can have similar results with the Lai-Massey scheme and propose a similar construction.

1 Notations

1.1 Feistel and Lai-Massey Schemes

Let $(G, +)$ be a group. Given r functions $F_1, \ldots, F_r$ on G we can define an r-round Feistel scheme which is a permutation on G^2 denoted $\Psi(F_1, \ldots, F_r)$. It is define by iterating the scheme on Fig. 1. If $r > 1$, we let

$$\Psi(F_1, \ldots, F_r)(x, y) = \Psi(F_2, \ldots, F_r)(y, x + F_1(y))$$

and

$$\Psi(F_1)(x, y) = (x + F_1(y), y).$$

(The last swap is omitted.)

Similarly, given a permutation σ on G, we define an r-round Lai-Massey scheme as a permutation $\Lambda^\sigma(F_1, \ldots, F_r)$ by

$$\Lambda^\sigma(F_1, \ldots, F_r)(x, y) = \Lambda^\sigma(F_2, \ldots, F_r)(\sigma(x + F(x - y)), y + F(x - y))$$

and

$$\Lambda^\sigma(F_1)(x,y) = (x + F(x-y), y + F(x-y))$$

in which the last σ is omitted.

For more convenience, if $x \in G^2$, we let x^l and x^r denote its two halves: $x = (x^l, x^r)$.

1.2 Advantage of Distinguishers and Best Advantage

A distinguisher $\mathcal{A}$ is a probabilistic Turing machine with unlimited computation power. It has access to an oracle $\mathcal{O}$ and can send it a limited number of queries. At the end, the distinguisher must output 0 or 1. We consider the advantage for distinguishing a random function F from a random function G defined by

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

Given an integer d and a random function F from a given set $\mathcal{M}_1$ to a given set $\mathcal{M}_2$, we define the d-wise distribution matrix $[F]^d$ as a matrix in $\mathbf{R}^{\mathcal{M}_1^d \times \mathcal{M}_2^d}$ by

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

For a matrix A in $\mathbf{R}^{\mathcal{M}_1^d \times \mathcal{M}_2^d}$, we define

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

It has been shown that $||.||_a$ is a matrix norm which can compute the best advantage. Namely we have

$$\max_{\substack{\mathcal{A} \text{ limited to } d \text{ queries} \\ \text{chosen plaintext attack}}} \mathrm{Adv}^{\mathcal{A}}(F,G) = \frac{1}{2}||[F]^d - [G]^d||_a. \tag{1}$$

(See [24].)

Similarly, we recursively define the $||.||_s$ norm by

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

(the norm of a matrix reduced to one entry being its absolute value) where $\pi_{x_1,y_1}(A)$ denotes the matrix in $\mathbf{R}^{\mathcal{M}_1^{d-1} \times \mathcal{M}_2^{d-1}}$ such that

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

Then we have

$$\max_{\substack{\mathcal{A} \text{ limited to } d \text{ queries} \\ \text{chosen plaintext and ciphertext attack}}} \mathrm{Adv}^{\mathcal{A}}(F,G) = \frac{1}{2}||[F]^d - [G]^d||_s. \tag{2}$$

(See [24].)

1.3 Decorrelation Biases

We also use the decorrelation bias of order d of a function in the sense of a given norm $||.||$ defined by

$$\mathrm{DecF}^d_{||.||}(F) = ||[F]^d - [F^*]^d||$$

where F^* is a random function uniformly distributed, and the decorrelation bias of order d of a permutation defined by

$$\mathrm{DecP}^d_{||.||}(C) = ||[C]^d - [C^*]^d||$$

where C^* is a random permutation uniformly distributed. (See [18, 20, 23, 24].)

2 On the Need for Orthomorphisms

Let us first consider the Λ^σ construction when σ is the identity function. Obviously if $(z,t) = \Lambda^\sigma(F_1,\ldots,F_r)(x,y)$ we have $z - t = x - y$. Thus, for any random round functions, $\Lambda^\sigma(F_1,\ldots,F_r)$ is fairly easily distinguishable with only one known plaintext. This is why we have to introduce the σ permutation.

Let us consider a one-round Lai-Massey scheme with σ:

$$(z,t) = (\sigma(x + F(x-y)), y + F(x-y)).$$

We have

$$\begin{aligned} z - t &= (\sigma(x + F(x-y)) - (x + F(x-y))) + (x - y) \\ &= \sigma'(x + F(x-y)) + x - y \end{aligned}$$

where $\sigma'(u) = \sigma(u) - u$. Thus, if F is uniformly distributed and σ' is a permutation, then $z - t$ is uniformly distributed. Ideally we thus require that σ and σ' are permutations, which means that σ is an orthomorphism of the group.

Unfortunately, the existence of orthomorphisms is not guaranteed for arbitrary groups. Actually, Hall-Paige Theorem [7] states that an Abelian finite group has an orthomorphism if and only if its order is odd or $\mathbf{Z}_2^2$ is isomorphic to one of its subgroups. In particular, $\mathbf{Z}_{2^m}$ has no orthomorphism. In odd-ordered groups G, with multiplicative notations, the square $\sigma(x) = x^2$ is an orthomorphism since σ' is the identity permutation and σ is a permutation (its inverse is the $\frac{1+\#G}{2}$-power function). In $\mathbf{Z}_2^m$ with $m > 1$, Schnorr and Vaudenay [15, 16] exhibited

$$\sigma(x) = (x \text{ AND } c) \text{ XOR } \mathrm{ROTL}^i(x)$$

which is an orthomorphism when the AND of all $\mathrm{ROTL}^{ij}(c)$ values is zero and the OR is `11...1`.[1] For instance, $i = 1$ and $c =$ `00...01` leads to an orthomorphism. Stern and Vaudenay used a similar construction in CS-Cipher [17].

We thus relax the orthomorphism properties by adopting the following notion of α-almost orthomorphism.

[1] Throughout this paper OR, AND and XOR denote the usual bit-wise boolean operators on bitstrings of equal length, and ROTL^i denotes the left circular rotation by i positions.

Definition 1. *In a given group G of order g, a permutation σ is called an α-almost orthomorphism if the function $\sigma'(x) = \sigma(x) - x$ is such that there are at most α elements in G with no preimage by σ'.*

This definition fits to Patarin's notion of "spreading" [12, 13]. We prefer here to emphasis on the approximation of orthomorphism properties.

We notice that since $(\sigma^{-1})'(x) = -\sigma'(\sigma^{-1}(x))$, then σ^{-1} is also an α-almost orthomorphism when σ is an α-almost orthomorphism.

Here is an useful lemma.

Lemma 2. *If σ is an α-almost orthomorphism over the group G, then*

$$\forall\delta \in G\backslash\{0\} \quad \Pr_{(X,Y)\in_U G^2}[\sigma'(X) - \sigma'(Y) = \delta] \leq \max(\alpha, 1)g^{-1} \tag{3}$$

$$\forall\delta \in G\backslash\{0\} \quad \Pr_{X\in_U G}[\sigma'(X) = \sigma'(X + \delta)] \leq \alpha g^{-1} \tag{4}$$

$$\forall\delta \in G \quad \Pr_{X\in_U G}[\delta - \sigma'(X) \notin \sigma'(G)] \leq 2\alpha g^{-1}. \tag{5}$$

Proof. It is straightforward that for any set A, the number of preimages x such that $\sigma'(x) \in A$ is at most $\alpha + \#A$. Let n_y denote the number of preimages of y. We have

$$\Pr_{(X,Y)\in_U G^2}[\sigma'(X) - \sigma'(Y) = \delta] = g^{-2}\sum_u n_u n_{u+\delta}.$$

First, if $\alpha = 1$, for $\delta \neq 0$, the number of (x, y) pairs such that $\sigma'(x) - \sigma'(y) = \delta$ is at most g which is equal to αg.

Let us now consider $\alpha \geq 2$. If there exists one y such that $n_y = \alpha + 1$, then for all other ys we have $n_y \leq 1$. Hence

$$\begin{aligned}\Pr_{(X,Y)\in_U G^2}[\sigma'(X) - \sigma'(Y) = \delta] &\leq \frac{\alpha + 1}{g^2} - g^{-2} + g^{-2}\sum_u n_{u+\delta} \\ &= \alpha g^{-2} + g^{-1} \\ &\leq \alpha g^{-1}.\end{aligned}$$

In the other cases, we have $n_y \leq \alpha$ hence

$$\Pr_{(X,Y)\in_U G^2}[\sigma'(X) - \sigma'(Y) = \delta] \leq g^{-2}\alpha\sum_u n_{u+\delta} = \alpha g^{-1}.$$

Therefore, in all cases this inequality holds.

We have

$$\Pr_{X\in_U G}[\sigma'(X) = \sigma'(X + \delta)] \leq \sum_{y; n_y \geq 2} n_y g^{-1} = 1 - g^{-1}\#\{y; n_y = 1\}.$$

The number of ys such that $n_y = 1$ is greater than $g - 2\alpha$, thus the probability is less than $2\alpha g^{-1}$.

The number of xs such that $\delta - \sigma'(x) \notin \sigma'(G)$ is at most $\alpha + g - \#\sigma'(G)$ which is at most 2α. $\square$

As an example of almost orthomorphism in $\mathbf{Z}_{2^m}$ (which has no orthomorphism), we claim that the simple rotation ROTL is a 1-almost orthomorphism. Actually, it is a permutation, and $\mathrm{ROTL}'(x)$ is equal to $x + \mathrm{MSB}(x)$ where $\mathrm{MSB}(x)$ denotes the most significant bit of x. The 0 value is taken twice by this function (by $x = 0$ and $x = \texttt{11}\ldots\texttt{1}$), the value $\texttt{100}\ldots\texttt{0}$ is never taken, and all the other values are taken once.

3 Extending the Luby-Rackoff Theorem

In order to extend Luby-Rackoff Theorem to the Lai-Massey scheme, we need the following lemma, which corresponds to Patarin's "coefficient H technique" [12, 13].

Lemma 3. *Let F_1^*, F_2^*, F_3^* be three independent random functions on a group G with uniform distribution, and let d be a positive integer. Let σ be an α-almost orthomorphism on G. For any family of G^2 elements $(x_1, \ldots, x_d, y_1, \ldots, y_d)$ such that the x_i values are pairwise different as well as the $y_i^l - y_i^r$ values, we have*

$$\frac{\Pr[\Lambda^\sigma(F_1^*, F_2^*, F_3^*)(x_i) = y_i; i]}{\Pr[C^*(x_i) = y_i; i]} \geq 1 - \frac{d(d-1)}{2}(g^{-1} + g^{-2}) - f(\alpha)$$

where g denotes the cardinality of G and C^* is a random permutation of G^2 uniformly distributed, provided that $d < g^2$, and $f(\alpha)$ is a function such that $f(0) = 0$ and

$$f(\alpha) = d\frac{d(\alpha - 1) + 3\alpha - 1}{2g} \quad \text{for} \quad \alpha > 0.$$

Proof. We let U_i, V_i, W_i denote the values after the first, second and final round of $\Lambda^\sigma(F_1^*, F_2^*, F_3^*)(x_i)$ respectively. For any value t in G^2, we let Δt denote $t^l - t^r$. The probabilistic event $[W_i = y_i]$ is equivalent to $[\Delta V_i = \Delta y_i \text{ and } W_i^l = y_i^l]$. Now we have

$$\begin{aligned} \Delta V_i &= \sigma'(U_i^l + F_2^*(\Delta U_i)) + \Delta U_i \\ W_i^l &= V_i^l + F_3^*(\Delta V_i). \end{aligned}$$

The $[W_i = y_i]$ event is thus equivalent to

$$e_i = [F_2^*(\Delta U_i) \in {\sigma'}^{-1}(\Delta y_i - \Delta U_i) - V_i^l \text{ and } F_3^*(\Delta y_i) = y_i^l - U_i^l].$$

When the ΔU_i are pairwise different, as well as the ΔV_i, it is thus easy to compute the probability that we have $W_i = y_i$ for all i because it relies on independent $F_2(\Delta U_i)$ and $F_3(\Delta V_i)$ uniformly distributed random variables. In addition we need all $\Delta y_i - \Delta U_i$ to have preimages by σ'.

We have

$$\begin{aligned} &\Pr[W_i = y_i; i = 1, \ldots, d] \\ &= \Pr[e_i; i = 1, \ldots, d] \end{aligned}$$

$$\begin{aligned}
&\geq \Pr[e_i, \Delta U_i \neq \Delta U_j, \Delta y_i - \Delta U_i \in \sigma'(G); i \neq j] \\
&= \Pr[e_i / \Delta U_i \neq \Delta U_j, \Delta y_i - \Delta U_i \in \sigma'(G); i \neq j] \times \\
&\quad \Pr[\Delta U_i \neq \Delta U_j, \Delta y_i - \Delta U_i \in \sigma'(G); i \neq j] \\
&= g^{-2d}(1 - \Pr[\exists i < j \quad \Delta U_i = \Delta U_j \quad \text{or} \quad \exists i \quad \Delta y_i - \Delta U_i \notin \sigma'(G))])
\end{aligned}$$

which is greater than g^{-2d} times

$$1 - \frac{d(d-1)}{2} . \max_{i<j} \Pr[\Delta U_i = \Delta U_j] - d . \max_i \Pr[\Delta y_i - \Delta U_i \notin \sigma'(G)].$$

We notice that

$$\Delta U_i = \sigma'(x_i^l + F(\Delta x_i)) + \Delta x_i.$$

The probability of having collisions with σ' with two different uniformly distributed inputs is less than $\max(\alpha, 1)g^{-1}$ for $\Delta x_i \neq \Delta x_j$ from Equation (3). If we have $\Delta x_i = \Delta x_j$, then we will have $\Delta U_i = \Delta U_j$ with probability at most αg^{-1} from Equation (4) since $x_i \neq x_j$ and thus $x_i^l \neq x_j^l$. In addition, $\Pr[\Delta y_i - \Delta U_i \notin \sigma'(G)]$ is less than $2\alpha g^{-1}$ from Equation (5). Therefore $\Pr[W_i = y_i; i = 1, \ldots, d]$ is greater than

$$g^{-2d}\left(1 - \frac{d(d-1)}{2}\max(\alpha, 1)g^{-1} - 2d\alpha g^{-1}\right).$$

We have

$$\Pr[C^*(x_i) = y_i; i = 1, \ldots, d] = \frac{1}{g^2(g^2-1)\ldots(g^2-d+1)}.$$

Since

$$\frac{g^2(g^2-1)\ldots(g^2-d+1)}{g^{2d}} \geq 1 - \frac{d(d-1)}{2g^2}$$

when $g^2 > d$, we obtain the result. □

We can now state our result.

Theorem 4. *Let F_1^*, F_2^*, F_3^* be three independent random functions on a group G with a uniform distribution. Let σ be an α-almost orthomorphism on G. For any distinguisher limited to d chosen plaintexts ($d < g^2$) between $\Lambda^\sigma(F_1^*, F_2^*, F_3^*)$ and a random permutation C^* with a uniform distribution, we have*

$$\mathrm{Adv}(\Lambda^\sigma(F_1^*, F_2^*, F_3^*), C^*) \leq d(d-1)\left(g^{-1} + g^{-2}\right) + f(\alpha)$$

where g is the cardinality of G and $f(\alpha)$ is defined as in Lemma 3.

Proof. We can assume without loss of generality that the distinguisher never request the same query twice. Let ω denote the random tape of the distinguisher $\mathcal{A}$, and A be the set of all (ω, y) entries which leads to the output 1. We have

$$p^{\mathcal{O}} = \Pr\left[\mathcal{A}^{\mathcal{O}} = 1\right] = \sum_{(\omega,y)\in A} \Pr[\omega] \Pr[C(x_i) = y_i; i = 1, \ldots, d]$$

where $x = (x_1, \ldots, x_d)$ in which x_i depends on ω and $(y_1, \ldots, y_{i-1})$. We let $C = \Lambda^\sigma(F_1^*, F_2^*, F_3^*)$. Thus we have

$$p^C - p^{C^*} = \sum_{(\omega,y)\in A} \Pr[\omega](\Pr[C(x_i) = y_i; i] - \Pr[C^*(x_i) = y_i; i]).$$

We split the sum between the y entries for which the Δy_i are pairwise different, and the others. From the previous lemma we have

$$p^C - p^{C^*} \geq - \sum_{\substack{(\omega,y)\in A \\ \Delta y_i \neq \Delta y_j}} \Pr[\omega] p^* \epsilon - \Pr[\exists i < j \quad \Delta C^*(y_i) = \Delta C^*(y_j)]$$

where $\epsilon = \frac{d(d-1)}{2}(g^{-1} + g^{-2}) + f(\alpha)$ and p^* is the probability that $C^*(x_i) = y_i$ for $i = 1, \ldots, d$. The first sum is less than ϵ, and the last probability is less than $\frac{d(d-1)}{2} g^{-1}$, thus

$$p^C - p^{C^*} \geq -\epsilon - \frac{d(d-1)}{2} g^{-1}.$$

We can then apply the same result to the symmetric distinguisher, and obtain the result. □

4 Inheritance of Decorrelation in the Lai-Massey Scheme

We can use the same proof as in [24] for proving that the decorrelation bias of the round functions of a Lai-Massey scheme is inherited by the whole structure. The following lemma is a straightforward application of a more general lemma from [24].

Lemma 5. *Let m be an integer, and $F_1, \ldots, F_r$ be r independent random functions on a group G. Let σ be a permutation on G. We have*

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

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

Following [24], this lemma and Lemma 3 enables to prove the following corollary.

Corollary 6. *If $F_1, \ldots, F_r$ are r (with $r \geq 3$) independent random functions on a group G of order g such that $\mathrm{DecF}^d_{||.||_a}(F_i) \leq \epsilon$ and if σ is an α-almost orthomorphism on G, we have*

$$\mathrm{DecP}^d_{||.||_a}(\Lambda^\sigma(F_1, \ldots, F_r)) \leq \left(3\epsilon + d(d-1)\left(2g^{-1} + g^{-2}\right) + 2f(\alpha)\right)^{\left\lfloor \frac{r}{3} \right\rfloor}$$

where $f(\alpha)$ is defined in Lemma 3.

5 On Super-Pseudorandomness

Super-pseudorandomness corresponds to cases where attacks can query chosen ciphertexts as well. We extend Lemma 3 in order to get results on the super-pseudorandomness.

Lemma 7. *Let $F_1^*, F_2^*, F_3^*, F_4^*$ be four independent random functions on a group G with uniform distribution, and let d be an integer. Let σ be an α-almost orthomorphism on G. For any set of $x_1, \ldots, x_d, y_1, \ldots, y_d$ values in G^2 such that the x_i values are pairwise different, we have*

$$\frac{\Pr[\Lambda^\sigma(F_1^*, F_2^*, F_3^*, F_4^*)(x_i) = y_i; i]}{\Pr[C^*(x_i) = y_i; i]} \geq 1 - d(d-1)\left(g^{-1} + g^{-2}\right) - f'(\alpha)$$

where g denotes the cardinality of G and C^* is a random permutation of G^2 uniformly distributed, provided that $d < g^2$, and $f'(\alpha)$ is a function such that $f'(0) = 0$ and

$$f'(\alpha) = dg^{-1}(d(\alpha - 1) + \alpha - 1) \quad \text{for} \quad \alpha > 0.$$

Proof. $\Lambda^\sigma(F_1^*, F_2^*, F_3^*, F_4^*)(x_i) = y_i)$ is equivalent to

$$\Lambda^\sigma(F_1^*, F_2^*, F_3^*)(x_i) = \Lambda^{\sigma^{-1}}(F_4^*)(y_i).$$

We can focus on the probability that all $\Delta\Lambda^{\sigma^{-1}}(F_4^*)(y_i)$ are pairwise different. Similarly as in the proof of Lemma 3, this holds but for a probability less than $\frac{d(d-1)}{2}\max(\alpha, 1)g^{-1}$. We can then apply Lemma 3 to complete the proof. □

This extends Theorem 4.

Theorem 8. *Let $F_1^*, F_2^*, F_3^*, F_4^*$ be four independent random functions on a group G with a uniform distribution. Let σ be an α-almost orthomorphism on G. For any distinguisher limited to d chosen plaintexts or ciphertexts ($d < g^2$) between $\Lambda^\sigma(F_1^*, F_2^*, F_3^*, F_4^*)$ and a random permutation C^* with a uniform distribution, we have*

$$\mathrm{Adv}(\Lambda^\sigma(F_1^*, F_2^*, F_3^*, F_4^*), C^*) \leq d(d-1)\left(g^{-1} + g^{-2}\right) + f'(\alpha)$$

where g denotes the cardinality of G and $f'(\alpha)$ is defined in Lemma 7.

The proof is the same as in Theorem 4, but with no consideration on the $\Delta y_i \neq \Delta y_j$ cases.

This shows that a 4-round random Lai-Massey scheme with an α-almost orthomorphism is a super-pseudorandom permutation when it is used less than $\sqrt{g/\max(\alpha, 1)}$ times. This also extends to the following decorrelation bias upper bound.

Corollary 9. *If $F_1, \ldots, F_r$ are r (with $r \geq 4$) independent random functions on a group G of order g such that $\mathrm{DecF}^d_{||.||_a}(F_i) \leq \epsilon$ and if σ is an α-almost orthomorphism on G, we have*

$$\mathrm{DecP}^d_{||.||_s}(\Lambda^\sigma(F_1, \ldots, F_r)) \leq \left(4\epsilon + d(d-1)\left(2g^{-1} + g^{-2}\right) + 2f'(\alpha)\right)^{\lfloor \frac{r}{4} \rfloor}$$

where $f'(\alpha)$ is defined in Lemma 7.

6 A New Family of Block Ciphers

In this section we construct a new family of block ciphers called Walnut (as for "Wonderful Algorithm with Light N-Universal Transformation") Walnut is a Lai-Massey scheme which depends on four parameters (m, r, d, q) where m is the message-block length (must be even), r is the number of rounds, d is the order of decorrelation and q is an integral prime power at least $2^{\frac{m}{2}}$. It is characterized by having round function F_i with the form

$$F_i(x) = \pi_i(r_i(K_{i,1}) + r_i(K_{i,2})r_i(x) + \ldots + r_i(K_{i,d})r_i(x)^{d-1})$$

where the $K_{i,j}$ are independent uniformly distributed bitstrings of length $m/2$, r_i is an injective mapping from $\{0,1\}^{\frac{m}{2}}$ to $\mathrm{GF}(q)$, and π_i is a surjective mapping from $\mathrm{GF}(q)$ to $\{0,1\}^{\frac{m}{2}}$. This is a straightforward extension of the Peanut construction. It has been shown in [24] that $\mathrm{DecF}^d(F_i)$ is less than

$$\epsilon = 2\left((1+\delta)^d - 1\right)$$

where $q = (1+\delta)2^{\frac{m}{2}}$. We use $\sigma = \mathrm{ROTL}$ as a 1-almost orthomorphism. Therefore by approximating the upper bounds of Corollaries 6 and 9 we have

$$\mathrm{DecP}^d_{||.||_a}(\mathrm{Walnut}(m,r,d,q)) \leq\sim \left(6d\delta + 2d^2 2^{-\frac{m}{2}}\right)^{\left\lfloor \frac{r}{3} \right\rfloor}$$
$$\mathrm{DecP}^d_{||.||_s}(\mathrm{Walnut}(m,r,d,q)) \leq\sim \left(8d\delta + 2d^2 2^{-\frac{m}{2}}\right)^{\left\lfloor \frac{r}{4} \right\rfloor}.$$

With $m = 64$, $d = 2$ and $p = 2^{32} + 15$, we obtain

$$\mathrm{DecP}^d_{||.||_a}(\mathrm{Walnut}(64, r, 2, 2^{32}+15)) \leq 2^{-24\left\lfloor \frac{r}{3} \right\rfloor}$$
$$\mathrm{DecP}^d_{||.||_s}(\mathrm{Walnut}(64, r, 2, 2^{32}+15)) \leq 2^{-24\left\lfloor \frac{r}{4} \right\rfloor}.$$

This provides sufficient security against differential and linear attacks for $r \geq 12$.

7 Conclusion

We have shown that adding a simple orthomorphism (or almost orthomorphism) enables the Lai-Massey scheme to provide randomness on three rounds, and super-pseudorandomness on four rounds, like for the Feistel scheme. We have shown that we can get similar decorrelation upper bounds as well and propose a new block cipher family.

Acknowledgement

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. *FIPS 46*, Data Encryption Standard. U.S. Department of Commerce — National Bureau of Standards, National Technical Information Service, Springfield, Virginia. *Federal Information Processing Standard Publication 46*, 1977.
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. J. Daemen, L. Knudsen, V. Rijmen. The Block Cipher Square. In *Fast Software Encryption*, Haifa, Israel, Lectures Notes in Computer Science 1267, pp. 149–171, Springer-Verlag, 1997.
4. H. Feistel. Cryptography and Computer Privacy. *Scientific American*, vol. 228, pp. 15–23, 1973.
5. 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.
6. 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.
7. M. Hall, L. J. Paige. Complete Mappings of Finite Groups. In *Pacific Journal of Mathematics*, vol. 5, pp. 541–549, 1955.
8. X. Lai. *On the Design and Security of Block Ciphers*, ETH Series in Information Processing, vol. 1, Hartung-Gorre Verlag Konstanz, 1992.
9. 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.
10. M. Luby, C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM Journal on Computing*, vol. 17, pp. 373–386, 1988.
11. J. L. Massey. SAFER K-64: a Byte-Oriented Block-Ciphering Algorithm. In *Fast Software Encryption*, Cambridge, United Kingdom, Lectures Notes in Computer Science 809, pp. 1–17, Springer-Verlag, 1994.
12. 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.
13. 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.
14. B. Schneier. Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). In *Fast Software Encryption*, Cambridge, United Kingdom, Lectures Notes in Computer Science 809, pp. 191–204, Springer-Verlag, 1994.
15. C. P. Schnorr, S. Vaudenay. Parallel FFT-Hashing. In *Fast Software Encryption*, Cambridge, United Kingdom, Lectures Notes in Computer Science 809, pp. 149–156, Springer-Verlag, 1994.
16. C. P. Schnorr, S. Vaudenay. Black Box Cryptanalysis of Hash Networks based on Multipermutations. In *Advances in Cryptology EUROCRYPT'94*, Perugia, Italy, Lectures Notes in Computer Science 950, pp. 47–57, Springer-Verlag, 1995.

17. J. Stern, S. Vaudenay. CS-Cipher. In *Fast Software Encryption*, Paris, France, Lectures Notes in Computer Science 1372, pp. 189–205, Springer-Verlag, 1998.
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. 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`