Comparison of Randomness Provided by Several Schemes for Block Ciphers

Shiho Moriai[1] and Serge Vaudenay[2⋆]

[1] NTT Laboratories
[2] Swiss Federal Institute of Technologies (EPFL)

Abstract. Block ciphers are usually made from one general scheme in which we plug round functions. For analyzing the security, it is important to study the intrinsic security provided by the general scheme from a randomness viewpoint: we study the minimal number of known plaintexts required to break it when the round functions are replaced by ideal random functions.
This approach provides comparisons between several generalized Feistel schemes, and other ones. In particular, we compare the randomness provided by the schemes which are used by the AES candidates.

1 Introduction

From the attacker viewpoint, a block cipher which is used by a given user can be considered as an instance of a random permutation over a message block space: since he only knows how the secret key has been chosen he only has a probabilistic information (in a Shannon sense) on the key and the permutation. In this setting security can be formalized by pseudorandomness: if there is no way to distinguish the block cipher from an ideal random permutation, then we cannot attack it. Pseudorandomness more precisely means that no oracle circuit with polynomially many oracle gates can distinguish between the encryption function and a truly random permutation.

A block cipher is usually made from an outer oracle circuit that we call "scheme" (for instance the circuit of the Feistel scheme [4]) in which we plug inner oracles that we call "primitives" like round functions, S-boxes, and so on. Sometimes an attack succeeds in "bypassing" some of the primitives by using intrinsic weaknesses of the scheme. For instance, differential cryptanalysis [1] can investigate

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

differentials in which some S-boxes play no role at all. This motivates the analysis of this paper: we consider ideal models of the block ciphers by replacing the primitives by truly random functions and study the pseudorandomness provided by the scheme.

In this paper we investigate the randomness of several schemes used in many block ciphers. The target schemes are the Feistel scheme, variants of the Feistel scheme (the CAST256-like Feistel scheme, the MARS-like Feistel scheme, and the RC6-like Feistel scheme), and the SQUARE-like scheme used in SQUARE, Rijndael and Crypton.

The pseudorandomness of some general schemes were discussed in previous papers e.g. [6, 16]. In this paper we show how we can reach these kind of results and extensions in a easier and systematic way by using decorrelation theory introduced in [9, 10, 12–14].

In order to compare the schemes we study the threshold number of rounds for having randomness, the theoretical minimal number of secure rounds against attacks which are limited to two chosen plaintexts or ciphertexts (which plays a crucial role in the security against differential and linear cryptanalysis), and the practical minimal number of secure rounds when we use an efficient decorrelation module (as in DFC [5]) for primitives.

2 Decorrelation Theory and Randomness of Iterated Ciphers

2.1 Definitions and Basic Properties

The goal of decorrelation theory is to provide some kinds of formal proof of security on block ciphers. This section describes the essential definitions and lemmas in decorrelation theory to prove the randomness of iterated ciphers.

Definition 1 (d-wise distribution matrix). *Given a random function F from a set $\mathcal{M}_1$ to a set $\mathcal{M}_2$ and an integer d, we define the "d-wise distribution matrix" of F as the following $\mathcal{M}_1^d \times \mathcal{M}_2^d$-matrix.*

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

where $x_i \in \mathcal{M}_1$ and $y_i \in \mathcal{M}_2$ for $i = 1, \ldots, d$

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

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

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 [9], the infinity-associated matrix norm $|||.|||_\infty$ was considered. This facilitated the proof of the security against non-adaptive iterated attacks. The following matrix norms $||.||_a$ and $||.||_s$ are dedicated to adaptive chosen plaintext attacks and chosen plaintext and ciphertext attacks, respectively. The former corresponds to pseudo-randomness and the latter corresponds to super-pseudorandomness.

Definition 3 ($||.||_a$ norm). *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*

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

Definition 4 ($||.||_s$ norm). *Similarly, we define the $||.||^s$ norm by*

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

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

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

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 $\mathcal{A}^{\mathcal{O}}$ which can send $\mathcal{M}_1$-element queries to the oracle O and receive $\mathcal{M}_2$-element responses, and which finally outputs 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 of F and G induces a distribution of $\mathcal{A}^F$ 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

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

We consider the class Cl_a^d of adaptive distinguishers limited to d queries. Similarly, when F and G are permutations, we also consider the extension Cl_s^d 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

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

Lemma 5 (Equivalence with the best advantage). *For any random functions F and G we have*

$$||[F]^d - [G]^d||_a = 2 \cdot \underset{\mathrm{Cl}_a^d}{\mathrm{BestAdv}}(F, G),$$

and when F and G are permutations we also have

$$||[F]^d - [G]^d||_s = 2 \cdot \underset{\mathrm{Cl}_s^d}{\mathrm{BestAdv}}(F, G).$$

Lemma 6 (Multiplicativity). *For any f and g, denote by $f \circ g$ their composition. For any independent random functions $F_1, \ldots, F_r$ we have*

$$\mathrm{DecF}^d(F_1 \circ \cdots \circ F_r) \leq \mathrm{DecF}^d(F_1) \cdots \mathrm{DecF}^d(F_r).$$

For any independent random permutations $C_1, \ldots, C_r$ we have

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

There are some known functions with quite small decorrelation biases called decorrelation modules [11]. Here is an example of decorrelation module called the NUT-IV decorrelation module.

Lemma 7 (NUT-IV Decorrelation Module [14]). *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*

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

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

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

For better efficiency in implementations, we will only consider prime integers q in this paper. We can refer to Noilhan [8] for implementation issues.

2.2 Basic Tools

The randomness of a cipher constructed using random primitives such as decorrelation modules can be proven using decorrelation theory. In order to deduce an upper bound on the decorrelation bias of the cipher from an upper bound on the decorrelation bias of these primitives, we use the following lemma.

Lemma 8 (Reduction to the randomness of ideal constructions [14]). *Let d be an integer, $F_1, \ldots, F_r$ be r independent random function oracles, and $C_1, \ldots, C_s$, $D_1, \ldots, D_t$ be $s+t$ independent random permutation oracles. We let $\Omega^{F_1,\ldots,F_r,C_1,\ldots,C_s,D_1,\ldots,D_t}$ be an oracle which can access to the previous oracles and from each query x defines an output $G(x)$. We assume that Ω is such that the number of queries to F_i and C_j is limited to some integer a_i and b_j respectively, and the number of queries to D_k or D_k^{-1} is limited to c_k in total for any $i = 1, \ldots, r$, $j = 1, \ldots, s$ and $k = 1, \ldots, t$. We let F_i^* (resp. C_j^*, D_k^*) be independent uniformly distributed random functions (resp. permutations) on the same range as F_i (resp. C_j, D_k) and we let G^**

the function defined by $\Omega^{F_1^*,\ldots,F_r^*,C_1^*,\ldots,C_s^*,D_1^*,\ldots,D_t^*}$. *We have*

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

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

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

Lemma 9 ([15]). *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*

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

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 10 ([15]). *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* $\mathrm{DecP}^d_{||.||_s}(F) \leq 2\epsilon + 2d^2(\#\mathcal{M})^{-1}$.

2.3 Examples

First this section studies how many rounds are required for Luby-Rackoff's randomness assuming round functions to be random ones. This is related to the "lack of randomness" provided by the upper level design. The required numbers of rounds for the Feistel scheme and some generalized Feistel schemes are shown in [16, Section 3.2].

Hereafter we use the following notations. I_n denotes the set of all n-bit strings, $\{0,1\}^n$. H_n denotes the set of all $I_n \mapsto I_n$ functions and P_n denotes the set of all such permutations. By $x \in_R X$ we mean that x is drawn randomly and uniformly from a finite set X.

Lemma 11 (Luby-Rackoff 1986 [6]). *Let* F_1^*, F_2^*, F_3^*, F_4^* *be four independent random functions on* $\{0,1\}^{\frac{m}{2}}$ *with uniform distribution. We have*

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

Here $\Psi(F_1, \ldots, F_r)$ *is the notation introduced by Luby and Rackoff in order to denote a Feistel scheme where the* i*-th round function is* F_i.

This lemma can be formally proven by using Lemma 9 and 10. From Lemma 6 and 8 this is generalized for a permutation on $\{0,1\}^m$ consisting of r rounds of Feistel transformations:

$$\mathrm{DecP}^d_{||.||_a}(\Psi(F_1, \ldots, F_r)) \leq \left(2d^2 \cdot 2^{-\frac{m}{2}} + 3 \max_i \mathrm{DecF}^d_{||.||_a}(F_i)\right)^{\lfloor \frac{r}{3} \rfloor}$$
$$\mathrm{DecP}^d_{||.||_s}(\Psi(F_1, \ldots, F_r)) \leq \left(2d^2 \cdot 2^{-\frac{m}{2}} + 4 \max_i \mathrm{DecF}^d_{||.||_a}(F_i)\right)^{\lfloor \frac{r}{4} \rfloor}$$

for any independent functions $F_1, \ldots, F_r \in H_{\frac{m}{2}}$. This leads to the following conclusions about the regular Feistel scheme with $m = 128$.

– The **threshold number of rounds** for having a security result is 3 for pseudorandomness and 4 for super-pseudorandomness, when $d \ll 2^{32}$.
– The **theoretical minimal number of secure rounds** for having decorrelation bias of 2^{-m} is $\frac{3m}{\frac{m}{2}-1-2\log_2 d}$ for pseudorandomness and $\frac{4m}{\frac{m}{2}-1-2\log_2 d}$ for super-pseudorandomness, when $d \ll 2^{32}$. This leads to 9 and 12 rounds, respectively, for $d = 2$.
– When using the NUT-IV decorrelation module with $d = 2$ in each round (as for instance Peanut98 [9] or DFC), the minimal number of rounds for having decorrelation bias of 2^{-m} is 9 for the $||.||_a$ norm and 12 for the $||.||_s$ norm (we use $q = 2^{64} + 13$ as in the NUT-IV decorrelation module).

Here we used an arbitrary threshold of 2^{-m} for the decorrelation bias which will be used in order to compare different schemes. Since 2^{-m} leads to a security connected with exhaustive search on m bits, we believe it is a relevant objective criterion for comparing schemes. We also focused on $d = 2$ which leads to security against differential and linear cryptanalysis.

3 Several Cases

3.1 CAST256-like Feistel Scheme

CAST-256 is an AES candidate based on a generalized Feistel scheme which was called "Type-1 transformation" by Zheng-Matsumoto-Imai [16] and denoted by Ψ_1. Formally, we define $\Psi_1 \in H_m$ as $\Psi_1()(x) = x$ and

$$\Psi_1(f_1, \ldots, f_r)(x_1, \ldots, x_k) = \\ \Psi_1(f_2, \ldots, f_r)(f_1(x_1) + x_2, x_3, x_4, \ldots, x_k, x_1)$$

for any primitive set $f_1, \ldots, f_r \in H_{\frac{m}{k}}$. Here k is the number of branches and r is the number of rounds.

Lemma 12 (Zheng-Matsumoto-Imai 1989 [16]). *For independent uniformly distributed random functions $F_1^*, \ldots, F_{3k-2}^* \in_R H_{\frac{m}{k}}$ and an integer d, we have*

$$\mathrm{DecP}^d_{||.||_a}(\Psi_1(F_1^*, \ldots, F_{2k-1}^*)) \leq 2(k-1)d^2 \cdot 2^{-\frac{m}{k}}$$
$$\mathrm{DecP}^d_{||.||_s}(\Psi_1(F_1^*, \ldots, F_{3k-2}^*)) \leq 2(k-1)d^2 \cdot 2^{-\frac{m}{k}}$$

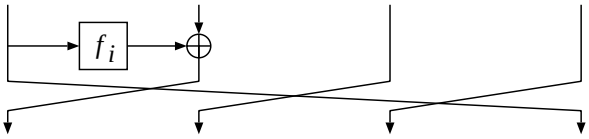

Fig. 1. CAST256-like Feistel Scheme

Proof (sketch). We use Lemma 9 for evaluating $\mathrm{DecF}^d_{||.||_a}$.

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 $y_i^j \neq y_{i'}^j$ for $j > 1$ 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 $\mathrm{DecF}^d_{||.||_a}(F) \leq 2(k-1)d(d-1)2^{-\frac{m}{k}}$.

Here, 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, from $\mathrm{DecF}^d_{||.||_a}(C^*) \leq d(d-1)2^{-m}$ and the triangular inequality we have

$$\mathrm{DecP}^d_{||.||_a}(F) \leq \mathrm{DecF}^d_{||.||_a}(F) + \mathrm{DecP}^d_{||.||_a}(F^*) \leq \mathrm{DecF}^d_{||.||_a}(F) + d^2 2^{-m}.$$

We then notice that the obtained upper bound for $\mathrm{DecF}^d_{||.||_a}$ can be written $\mathrm{DecF}^d_{||.||_a}(F) \leq Ad(d-1)2^{-\frac{m}{k}}$ for some $A \geq 2$. For $d \leq A2^{m-\frac{m}{k}}$ we thus obtain $\mathrm{DecP}^d_{||.||_a}(F) \leq Ad^2 2^{-\frac{m}{k}}$. For larger d, this bound is greater than $A^3 2^{m\left(2-\frac{3}{k}\right)}$ which is greater than 8 since $m \geq k \geq 2$. Since $\mathrm{DecP}^d_{||.||_a}(F)$ is always less than 2, the bound is thus still valid.

For $\mathrm{DecP}_{||.||_s}$, we add $k-1$ more rounds and we study the probability that we turn into $\mathcal{Y}$ if we invert them on $y_1, \ldots, y_d$. The result comes from Lemma 10. □

Thus the required number of rounds for CAST256-like scheme is proven to be $2k-1$, where k is the number of branches. That is, the required numbers of rounds for the Feistel scheme and CAST256-like scheme are 3 and 7, respectively.

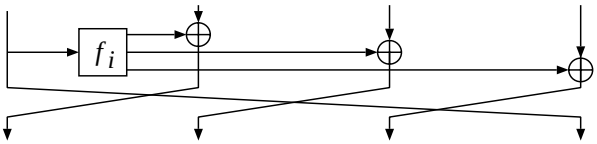

Fig. 2. MARS-like Feistel Scheme

This leads to the following conclusions about the CAST256-like scheme with $k = 4$ branches and $m = 128$.

- The **threshold number of rounds** is 7 for pseudorandomness and 10 for super-pseudorandomness, when $d \ll 2^{16}$.
- For $d = 2$, the **theoretical minimal number of secure rounds** is 35 for pseudorandomness and 50 for super-pseudorandomness.
- For $d = 2$ and the NUT-IV decorrelation module with $q = 2^{32} + 15$, the minimal number of rounds is 42 for the $||.||_a$ norm and 50 for the $||.||_s$ norm.

3.2 MARS-like Feistel Scheme

Similarly, we define MARS-like generalized Feistel scheme denoted by $\Psi'_1 \in H_m$ as $\Psi'_1()(x) = x$ and

$$\Psi'_1(f_1, \ldots, f_r)(x_1, \ldots, x_k) =$$
$$\Psi'_1(f_2, \ldots, f_r)(f_1^2(x_1) + x_2, f_1^3(x_1) + x_3, \ldots, f_1^k(x_1) + x_k, x_1)$$

where $f_i = (f_i^2, \ldots, f_i^k)$, $f_i^2, \ldots, f_i^k \in H_{\frac{m}{k}}$.

Lemma 13. *For independent uniformly distributed random functions $F_i^{j*} \in_R H_{\frac{m}{k}}$ for $i = 1, \ldots, 2k$ and $j = 2, \ldots, k$ and an integer d, we have*

$$\mathrm{DecP}^d_{||.||_a}(\Psi'_1(F_1^*, \ldots, F_{k+1}^*)) \leq 2d^2 \cdot 2^{-\frac{m}{k}}$$
$$\mathrm{DecP}^d_{||.||_s}(\Psi'_1(F_1^*, \ldots, F_{2k}^*)) \leq 2d^2 \cdot 2^{-\frac{m}{k}}$$

Proof (sketch). Using Lemma 9 we let $\mathcal{Y}$ be the set of all $(y_1, \ldots, y_d)$ such that $y_i^k \neq y_j^k$ for $i \neq j$. We get $\epsilon_1 = \frac{d(d-1)}{2} 2^{-\frac{m}{k}}$. We focus on the event that the first output after k rounds leads to no collision. We get $\epsilon_2 = \frac{d(d-1)}{2} 2^{-\frac{m}{k}}$.

For $\mathrm{DecP}^d_{||.||_s}$ we use the same event. □

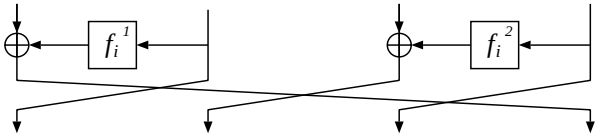

Fig. 3. RC6-like Feistel Scheme

This leads to the following conclusions about the MARS-like scheme with $k = 4$ branches and $m = 128$.

- The **threshold number of rounds** is 5 for pseudorandomness and 8 for super-pseudorandomness, when $d \ll 2^{16}$.
- For $d = 2$, the **theoretical minimal number of secure rounds** is 25 for pseudorandomness and 40 for super-pseudorandomness.
- For $d = 2$ and the NUT-IV decorrelation module with $q = 2^{32} + 15$, the minimal number of rounds is 25 for the $||.||_a$ norm and 40 for the $||.||_s$ norm.

3.3 RC6-like Feistel Scheme

The RC6 block cipher is designed to be secure by mixing operations that are efficiently implemented on most modern processors: addition/subtraction, exclusive-or, multiplication, and rotation rather than by using a general scheme with pseudorandom primitives. However, the structure of RC6 can be regarded as a generalized Feistel scheme, which is similar to "Type-2 transformation" called by Zheng-Matsumoto-Imai [16] assuming that primitives are independent random functions. Formally, as the RC6-like Feistel scheme $\Psi_2 \in H_m$ is defined for k even and r a multiple of $\frac{k}{2}$, by $\Psi_2()(x) = x$ and

$$\Psi_2(f_1, \ldots, f_r)(x_1, \ldots, x_k) =$$
$$\Psi_2(f_2, \ldots, f_r)(x_2, f_1^2(x_4) + x_3, \ldots, x_{k-2}, f_1^{\frac{k}{2}}(x_k) + x_{k-1}, x_k, f_1^1(x_2) + x_1),$$

where $f_i = (f_i^1, \ldots, f_i^{\frac{k}{2}}), f_i^1, \ldots, f_i^{\frac{k}{2}} \in H_{\frac{m}{k}}$.

Lemma 14. *For independent uniformly distributed random functions $F_1^*, \ldots, F_{k^2}^* \in_R H_{\frac{m}{k}}$ and an integer d, we have*

$$\mathrm{DecP}^d_{||.||_a}(\Psi_2(F_1^*, \ldots, F^*_{\frac{k}{2}(k+1)})) \leq \frac{k^2}{2} d^2 \cdot 2^{-\frac{m}{k}}$$

$$\mathrm{DecP}^d_{||.||_s}(\Psi_2(F_1^*,\ldots,F_{k^2}^*)) \leq \frac{k^2}{2} d^2 \cdot 2^{-\frac{m}{k}}$$

Proof (sketch). Similarly, we use Lemma 9 for evaluating $\mathrm{DecP}^d_{||.||_a}$. For Ψ_2 we let $\mathcal{Y}$ be the set of all y such that $y_i^j \neq y_{i'}^j$ for odd 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 even 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 $\mathrm{DecF}^d_{||.||_a}(F) \leq \frac{k^2}{2} d(d-1) 2^{-\frac{m}{k}}$. For $\mathrm{DecP}^d_{||.||_s}$, we add $k-1$ more rounds and study the probability that we turn into $\mathcal{Y}$ if we invert them on $y_1,\ldots,y_d$. The result comes from Lemma 10. □

This leads to the following conclusions about the RC6-like scheme with $k = 4$ branches and $m = 128$.

- The **threshold number of rounds** is 5 for pseudorandomness and 8 for super-pseudorandomness, when $d \ll 2^{16}$.
- For $d = 2$, the **theoretical minimal number of secure rounds** is 25 for pseudorandomness and 40 for super-pseudorandomness.
- For $d = 2$ and the NUT-IV decorrelation module with $q = 2^{32} + 15$, the minimal number of rounds is 25 for the $||.||_a$ norm and 40 for the $||.||_s$ norm.

3.4 SQUARE-like Scheme

In this paper we discuss only the Rijndael scheme. The pseudorandomness of other SQUARE-like schemes will be described in the full paper. Let us formalize the Rijndael scheme on k^2 values by

$$\Sigma(f_1,\ldots,f_r)(x_1,\ldots,x_{k^2}) =$$
$$\Sigma(f_2,\ldots,f_r)(\mathrm{MixCol}(\mathrm{ShiftRow}(f_1^1(x_1),\ldots,f_1^{k^2}(x_{k^2}))))$$

where $f_i = (f_i^1,\ldots,f_i^{k^2})$, $[[f_i^1,\ldots,f_i^{k^2} \in H_{\frac{m}{k^2}}$, the ShiftRow transformation is a fixed linear transformation on the rows of a $k \times k$ matrix which consists in mixing them, and the MixCol transformation is a fixed linear transformation on the columns [3].

Lemma 15. *For independent uniformly distributed random functions $F_1^*,\ldots,F_5^*$ and an integer d, we have*

$$\mathrm{DecP}^d_{||.||_a}(\Sigma(F_1^*,\ldots,F_3^*)) \leq 2k^2 d^2 \cdot 2^{-\frac{m}{k^2}}$$
$$\mathrm{DecP}^d_{||.||_s}(\Sigma(F_1^*,\ldots,F_5^*)) \leq 2k^2 d^2 \cdot 2^{-\frac{m}{k^2}}$$

Table 1. Comparison of randomness of several schemes (when $d = 2, k = 4, m = 128$)

Scheme	Feistel	CAST256-like	MARS-like	RC6-like	Rijndael
Threshold number of rounds for p.r.	3	7	5	5	3
Threshold number of rounds for s.p.r.	4	10	8	8	5
Theoretical min. number of secure rounds for p.r.	9	35	25	25	384
Theoretical min. number of secure rounds for s.p.r.	12	50	40	40	640
Example	Twofish, DFC, E2	CAST-256	MARS	RC6	Rijndael

Note: "p.r." and "s.p.r." mean pseudorandomness and super-pseudorandomness, respectively.

Thus achieving decorrelation to the order $d \geq \frac{1}{k\sqrt{2}} 2^{\frac{m}{2k^2}}$ does not seem possible with this design. (For $m = 128$ and $k = 4$, this is $d = 2\sqrt{2}$.)

Proof (sketch). We use Lemma 9 for evaluating $\mathrm{DecP}^d_{||.||_a}$. We let $\mathcal{Y}$ be the set of all $y = (y_1, \ldots, y_d)$ which take different values on all positions. We have $\epsilon_1 = k^2 \frac{d(d-1)}{2} 2^{-\frac{m}{k^2}}$. We consider the event that after two rounds we obtain different values on all positions. Provided that the MixCol transformation has good diffusion properties we obtain $\epsilon_2 = k^2 \frac{d(d-1)}{2} 2^{-\frac{m}{k^2}}$. □

This leads to the following conclusions about the Rijndael scheme with $k^2 = 4^2$ branches and $m = 128$.

- The **threshold number of rounds** is 3 for pseudorandomness and 5 for super-pseudorandomness, when $d \ll 3$.
- For $d = 2$, the **theoretical minimal number of secure rounds** is 384 for pseudorandomness and 640 for super-pseudorandomness.
- For $d = 2$ and the NUT-IV decorrelation module with $q = 2^8 + 1$, the minimal number of rounds is ∞ for the $||.||_a$ norm and ∞ for the $||.||_s$ norm.

4 Conclusion

We studied randomness provided by several schemes used for block ciphers. We focused on the schemes for AES candidates, in particular (see Table 1). The result on randomness provided by each scheme is a

good measure for the security from a randomness viewpoint but the readers should take care that it doesn't show the actual security of the ciphers which adopt the scheme. To study the intrinsic security provided by the general scheme, we decomposed the ciphers into the general scheme and internal primitives, ignoring some components which we considered do not affect its randomness. We also assumed that internal primitives are ideal random ones.

The results in Table 1 show that the Feistel scheme is the best in that the required number of rounds for pseudorandomness and super-pseudorandomness is the smallest. However, in comparing the randomness among several schemes we should take account of the computational cost of random primitives. For example, for the Feistel scheme we assume the random functions on $\{0,1\}^{64}$, and for the CAST256-like, MARS-like, and RC6-like schemes, we assume the random functions on $\{0,1\}^{32}$, whose computational cost is much cheaper than the former. Under the same assumption of the computational cost of random functions on $\{0,1\}^{32}$, the MARS-like scheme is the best.

In our result we notice that the schemes which use random primitives with a smaller input/output sizes are less secure, which is not surprising because the randomness bias is larger in these cases. We should interpret these conclusions with great care. Indeed, our results do not mean that Rijndale or Serpent[1] is not secure, or less secure than regular Feistel schemes. They rather mean that the latter can benefit from stronger security arguments: we can prove that an efficient attack against — say Twofish — must use an unexpected property of the round function, whereas an attack against Serpent may hold for any set of (random) S-boxes.

[1] A preliminary study suggested that the Serpent scheme requires too many rounds for randomness, because the size of primitives is too small (4 bits). The details are discussed in the full paper.

References

1. E. Biham, A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.
2. L. Carter, M. Wegman. Universal Classes of Hash Functions. *Journal of Computer and System Sciences*, vol.18, pp.143–154, 1979.
3. J. Daemen, V. Rijmen. AES Proposal: Rijndael.
   URL: `http://www.esat.kuleuven.ac.be/~rijmen/rijndael/`
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. M. Luby, C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM Journal on Computing*, vol. 17, pp. 373–386, 1988.
7. M. Matsui. The First Experimental Cryptanalysis of the Data Encryption Standard. In *Advances in Cryptology CRYPTO'94*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 839, pp. 1–11, Springer-Verlag, 1994.
8. F. Noilhan. Software Optimization of Decorrelation Module. To appear in the proceedings of SAC' 99, Springer-Verlag.
9. 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.
10. 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`
11. S. Vaudenay. The Decorrelation Technique Home-Page.
    URL: `http://www.dmi.ens.fr/~vaudenay/decorrelation.html`
12. 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.
13. S. Vaudenay. On the Lai-Massey Scheme. *Advances in Cryptology — ASIACRYPT'99*, Singapore, Lecture Notes in Computer Science 1716, pp.8–19, Springer-Verlag, 1999.
14. 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`
15. S. Vaudenay. On Provable Security for Conventional Cryptography. Invited talk. To appear in the proceedings of ICISC' 99, LNCS, Springer-Verlag.
16. Y. Zheng, T. Matsumoto, H. Imai. On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses (Extended Abstract). *Advances in Cryptology — CRYPTO'89*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 435, pp.461–480, Springer-Verlag, 1990.