Generic Attacks on Misty Schemes

Valérie Nachef[1], Jacques Patarin[2], Joana Treger[3]

[1] Department of Mathematics
University of Cergy-Pontoise
CNRS UMR 8088
2 avenue Adolphe Chauvin, 95011 Cergy-Pontoise Cedex, France
[2] Université de Versailles
45 avenue des Etats-Unis, 78035 Versailles Cedex, France
[3] Université de Versailles
45 avenue des Etats-Unis, 78035 Versailles Cedex, France
valerie.nachef@u-cergy.fr
jacques.patarin@prism.uvsq.fr
joana.Treger@prism.uvsq.fr

Abstract. Misty schemes are classic cryptographic schemes used to construct pseudo-random permutations from $2n$ bits to $2n$ bits by using d pseudo-random permutations from n bits to n bits. These d permutations will be called the "internal" permutations, and d is the number of rounds of the Misty scheme. Misty schemes are important from a practical point of view since for example, the Kasumi algorithm based on Misty schemes has been adopted as the standard block cipher in the third generation mobile systems. In this paper we describe the best known "generic" attacks on Misty schemes, i.e. attacks when the internal permutations do not have special properties, or are randomly chosen. We describe known plaintext attacks (KPA), non-adaptive chosen plaintext attacks (CPA-1) and adaptive chosen plaintext and ciphertext attacks (CPCA-2) against these schemes. Some of these attacks were previously known, some are new. When $d = 5$ rounds, it is shown in [6] that a CPA-1 exists with complexity 2^n. We will present completely different attacks with $d = 5$ and the same complexity. We will also present new attacks for $d \leq 4$ and $d \geq 6$. For $d \geq 6$ the complexity will be greater than 2^{2n}, so these attacks will be useful only when n is small.

Key words: Misty permutations, pseudo-random permutations, generic attacks on encryption schemes, Block ciphers.

1 Introduction

A secure block cipher can be seen as a specific implementation of a pseudo-random permutation. They are generally defined by using a recursive construction process. The most studied way to build pseudo-random permutations from previously (and generally smaller) random functions or permutations is the d-round Feistel construction, that we will denote ψ^d: $f = \psi^d(f_1, \ldots, f_d)$, where

$f_1, \ldots, f_d$ are functions from n bits to n bits, and f is a permutation from $2n$ bits to $2n$ bits. However, there exist other well known constructions such as for example Massey and Lai's scheme used in IDEA ([7]), unbalanced Feistel schemes with expanding or contracting internal functions ([13, 14]), and the Misty construction that we will analyze in this paper. We will denote by M^d, or M_L^d a Misty scheme of d rounds: $f = M^d(f_1, \ldots, f_d)$, where $f_1, \ldots, f_d$ are permutations from n bits to n bits, and f is a permutation from $2n$ bits to $2n$ bits (precise definitions will be given in Section 2). From a practical point of view, it is interesting to study the security of these Misty schemes since this structure is used in real life block ciphers, such as Matsui's Misty block cipher [8], as well as in the Kasumi variant of Misty adopted as standard block cipher for encryption and integrity protection in third generation mobile systems ([2]). In this paper we will study "generic" attacks on Misty schemes, i.e. attacks when the internal permutations $f_1, \ldots, f_d$ do not have special properties, or are randomly chosen. In real block ciphers $f_1, \ldots, f_d$ are never pseudo-random, and there are therefore often better attacks than the generic ones. However, generic attacks are very interesting since they point on general properties of the structure, not on specific problems of the $f_1, \ldots, f_d$. We can consider that they give a minimum number of rounds needed in these schemes for a given wanted security: generally the security with specific $f_1, \ldots, f_d$ is smaller or at best equal compared to that with random $f_1, \ldots, f_d$ since the attacks on random $f_1, \ldots, f_d$ generally also apply to specific $f_1, \ldots, f_d$. (When it is not the case, the security might appear to be based an a very specific and maybe dangerous instantiation). A general presentation of generic attacks on Feistel schemes ([10, 19]) and unbalanced Feistel schemes ([13, 14]) already exists, but no similar presentation and analysis for Misty schemes was written so far. Some specific results on Misty scheme attacks or security have been already published ([5, 15–18]). Sometimes the previously found attacks are the best known attacks (it is even possible to prove in some cases that they are the best possible attacks). However, as we will see in this paper, sometimes some new and better attacks exist, for example with 4 or more rounds. From a theoretical point of view, analyzing generic attacks on Misty schemes is interesting because Misty schemes have many similarities, but also many differences compared with Feistel schemes ψ^d ([10, 19]), unbalanced Feistel schemes with expanding functions F_k^d ([14]) and Butterfly and Benes schemes ([3, 12]). For Feistel schemes ψ^d, the best known generic attacks are "2-point attacks", i.e. attacks using correlations on (many) pairs of messages such as differential attacks [10, 19]. For unbalanced Feistel schemes with expanding functions the best known generic attacks are "2-point", "4-point", or rectangle attacks with 6, 8, 10,... points (see [14]). For Butterfly schemes, the best known generic attacks are "4-point" attacks ([3, 12]). Here for Misty schemes, the best known attacks will sometimes be 2-point attacks, sometimes "4-point" attacks, and they will be based sometimes on the properties of the first n bits of output (S) and sometimes on the Xor of the first n bits of output and the last n bits of output ($S \oplus T$), combined with the properties of the input $[L, R]$. In fact it was not obvious before making a specific and precise analysis of Misty schemes

if these schemes were more or less secure than for example Feistel schemes ψ^d for a given number of rounds. The paper is organized as follows. In Section 2, we give notations, definitions and general properties of Misty schemes. In Section 3, we detail attacks against 1, 2, 3 and 4 rounds. Section 4 is devoted to the study of attacks on 5 rounds. In section 5, we give attacks on 6 rounds. In section 6, we explain how to make a complete study of the 2-point attacks. Our final results are summarized in Section 7.

2 Notations, Definitions and Properties

2.1 Notations

Basic Notations. We use the following notations:

- $I_n = \{0,1\}^n$ is the set of the 2^n strings of length n.
- For $a, b \in I_n$, $[a, b]$ will be the string of length $2n$ which is the concatenation of a and b.
- For $a, b \in I_n$, $a \oplus b$ stands for the bitwise exclusive-or of a and b.
- $\circ$ is the composition of functions.
- The set of all functions from I_n to I_n is F_n. Thus $|F_n| = 2^{n \cdot 2^n}$.
- The set of all permutations from I_n to I_n is B_n. Thus $B_n \subset F_n$ and $|B_n| = (2^n)!$.

L and R Schemes.

- Let f_1 be a permutation of B_n. Let L, R, S and T be elements in I_n. Then by definition: $M_L(f_1)([L, R]) = [S, T] \Leftrightarrow S = R$ and $T = R \oplus f_1(L)$.
  Let $f_1, \ldots, f_d$ be d bijections of B_n. We define:
  $M_L^d(f_1, \ldots, f_d) = M_L(f_d) \circ \ldots \circ M_L(f_2) \circ M_L(f_1)$.
  The permutation $M_L^d(f_1, \ldots, f_d)$ is called a "Misty L scheme with d rounds".

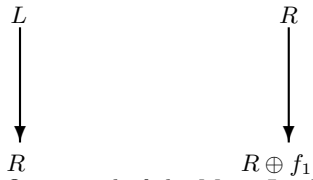

Fig. 1. One round of the Misty L scheme

- Similarly there is a slightly different construction named the Misty R scheme. By definition:
  $M_R(f_1)([L, R]) = [S, T] \Leftrightarrow S = R \oplus f_1(L)$ and $T = f_1(L)$.
  $M_R^d(f_1, \ldots, f_d) = M_R(f_d) \circ \ldots \circ M_R(f_2) \circ M_R(f_1)$.
  The permutation $M_R^d(f_1, \ldots, f_d)$ is called a "Misty R scheme with d rounds".

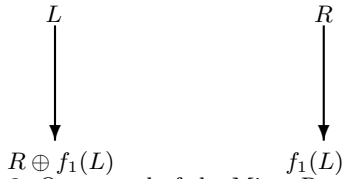

Fig. 2. One round of the Misty R scheme

M_L^d is the "classic" Misty scheme used in cryptography. Therefore when we will call "Misty scheme" we will refer to M_L^d (and not M_R^d). This paper is mainly about M_L^d but we will also rapidly present the (few) security differences between M_R^d and M_L^d. Note that we do not include the $FL/FL-1$ functions unlike Kasumi block ciphers.

Messages and Attacks In our attacks, we denote by m the number of input/output messages that we use. $\forall i,\ 1 \leq i \leq m$, we denote by $[L_i, R_i]$ the cleartext of message i, and by $[S_i, T_i]$ the ciphertext of this message i. Without loss of generality we can always assume that the messages $[L_i, R_i]$ are pairwise distinct ($L_i = L_j$ and $i \neq j \Rightarrow R_i \neq R_j$). In 2-point attacks (respectively 4-point attacks) we use pairs of messages (respectively 4-tuples of messages).

2.2 Some General Properties of the M_L and M_R Schemes

Inversion. Let $f_1 \in B_n$. Let $\Lambda(f_1)$, or simply Λ, be the permutation of B_{2n} such that
$\forall [L, R] \in I_{2n},\ \Lambda([L, R]) \stackrel{def}{=} [f_1(L), R]$. We have $\left(\Lambda(f_1)\right)^{-1} = \Lambda(f_1^{-1})$.

Let μ be the permutation of B_{2n} such that $\forall [L, R] \in I_{2n},\ \mu([L, R]) \stackrel{def}{=} [R, L \oplus R]$. We have $\mu^2([L, R]) = [L \oplus R, L]$ and $\mu^3([L, R]) = [L, R]$. Therefore $\mu^3 = Id$, and $\mu^{-1} = \mu^2$.

We see that: $M_L = \mu \circ \Lambda$ and $M_R = \mu^{-1} \circ \Lambda$. Therefore, $M_L^{-1}(f_1) = \Lambda(f_1^{-1}) \circ \mu^{-1} = \mu \circ M_R(f_1^{-1}) \circ \mu^{-1}$. Then for d rounds, we have:
$M_L^{-1}(f_1, \ldots, f_d) = \mu \circ M_R(f_d^{-1}, \ldots, f_1^{-1}) \circ \mu^{-1}$.
This property shows that the inverse of a M_L function is a M_R function, after composing by μ and μ^{-1} on the inputs and outputs. Thus, the security of M_L and M_R will be the same for all attacks where the inputs and outputs have the same possibilities. For example, in KPA (known plaintext attacks), CPCA-1 (non adaptive chosen plaintext and chosen ciphertext attacks) and CPCA-2 (adaptive chosen plaintext and chosen ciphertext attacks) the security of generic M_L and M_R schemes will be the same. In CPA-1 (non adaptive chosen plaintext attacks) and CPA-2 (adaptive chosen plaintext attacks) the security may be different. In this paper we will concentrate the analysis on the classical Misty M_L, and just rapidly give the differences in CPA for M_R.

Formulas for the M_L schemes, definition of the "internal" variable X^i.

1 round. For one round, we have: $\begin{cases} S = R \\ T = R \oplus f_1(L) \end{cases}$. We define $X^1 = R \oplus f_1(L)$.

2 rounds. For 2 rounds, we have: $\begin{cases} S = R \oplus f_1(L) \\ T = R \oplus f_1(L) \oplus f_2(R) \end{cases}$, or alternatively: $\begin{cases} S = X^1 \\ T \oplus S = f_2(R) \end{cases}$. We write $X^2 = R \oplus f_1(L) \oplus f_2(R) = X^1 \oplus f_2(R)$.

d rounds. More generally, for d rounds, we have: $\begin{cases} S = X^{d-1} \\ T \oplus S = f_d(X^{d-2}) \end{cases}$, where the X^i variables are defined by induction: $X^{-1} = L$, $X^0 = R$, and $\forall k \in \mathbb{N},\ k \geq 1,\ X^k = X^{k-1} \oplus f_k(X^{k-2})$.

For message number i, we will denote the value of X^k on this message by $X^k(i)$, or simply X_i^k. For example, $X_i^1 = X^1(i) = R_i \oplus f_1(L_i)$ and $X_i^2 = X^2(i) = R_i \oplus f_1(L_i) \oplus f_2(R_i)$.

Without loss of generality, we can choose messages in the attacks such that $L_i = L_j \Rightarrow R_i \neq R_j$. Then we can notice that:

- for all $i \neq j$, $L_i = L_j \Rightarrow X_i^1 \neq X_j^1$ (but we can have $L_i = L_j$ and $X_i^2 = X_j^2$).
- For all $i \neq j$, $R_i = R_j \Rightarrow X_i^1 \neq X_j^1$ and $X_i^2 \neq X_j^2$ (but we can have $R_i = R_j$ and $X_i^3 = X_j^3$).
- For all $i \neq j$, $X_i^1 = X_j^1 \Rightarrow X_i^2 \neq X_j^2$ and $X_i^3 \neq X_j^3$ (but we can have $X_i^1 = X_j^1$ and $X_i^4 = X_j^4$).
- etc.

A useful "4-point" property. Let $[L_1, R_1]$, $[L_2, R_2]$, $[L_3, R_3]$, $[L_4, R_4]$ be four messages such that $L_1 \neq L_2$, $R_1 \neq R_2$, $L_3 = L_1$, $R_3 = R_2$, $L_4 = L_2$, $R_1 = R_4$. Therefore we have the 4 messages $[L_1, R_1]$, $[L_2, R_2]$, $[L_1, R_2]$, $[L_2, R_1]$.

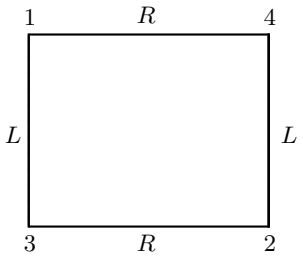

Fig. 3. The equalities in L and R for the "4-point" property

Lemma 1. *For such 4 messages, we always have:*

$$X_1^1 \oplus X_2^1 \oplus X_3^1 \oplus X_4^1 = X_1^2 \oplus X_2^2 \oplus X_3^2 \oplus X_4^2 = 0$$

$$X_1^3 \oplus X_2^3 \oplus X_3^3 \oplus X_4^3 = f_3(X_1^1) \oplus f_3(X_2^1) \oplus f_3(X_3^1) \oplus f_3(X_4^1)$$

(We also have $X_1^4 \oplus X_2^4 \oplus X_3^4 \oplus X_4^4 = X_1^3 \oplus X_2^3 \oplus X_3^3 \oplus X_4^3 \oplus f_4(X_1^2) \oplus f_4(X_2^2) \oplus f_4(X_3^2) \oplus f_4(X_4^2)$*)*

Proof: These properties are immediately deduced from the definition of the internal variables X^1, X^2, X^3, X^4 and from the fact that $L_3 = L_1$, $R_3 = R_2$, $L_4 = L_2$, $R_4 = R_1$. For all i:

$$\begin{array}{ll} X_i^1 \stackrel{def}{=} R_i \oplus f_1(L_i) & X_i^3 \stackrel{def}{=} X_i^2 \oplus f_3(X_i^1) \\ X_i^2 \stackrel{def}{=} R_i \oplus f_1(L_i) \oplus f_2(R_i) & X_i^4 \stackrel{def}{=} X_i^3 \oplus f_4(X_i^2). \end{array},$$

□

3 Attacks on M_L^d, $1 \leq d \leq 4$

We will give one attack for each case. Other attacks are performed in the extended version of this paper.

3.1 1 Round

After one round, we have $S = R$. This gives an attack with one message. We just have to check if $S = R$. With a Misty scheme, this happens with probability 1 and with a random permutation with probability $\frac{1}{2^n}$.

3.2 2 Rounds

After 2 rounds we have: $S = R \oplus f_1(L)$ and $T \oplus S = f_2(R)$.

CPA-1 using S. We choose two messages $[L_1, R_1]$ and $[L_2, R_2]$ such that $L_1 = L_2$ and we check if $S_1 \oplus S_2 = R_1 \oplus R_2$. For a Misty scheme this happens with probability 1 and for a random permutation with probability $\frac{1}{2^n}$. This is a CPA-1 with $m = 2$ and $O(1)$ computations.

KPA using S. The CPA-1 can be transformed into a KPA with $m = O(\sqrt{2^n})$ and $O(\sqrt{2^n})$ computations: if $m = O(\sqrt{2^n})$ then by the birthday paradox, we find with a good probability i, j such that $L_i = L_j$ and then we check if $S_i \oplus S_j = R_i \oplus R_j$. There also exists an attack using $S \oplus T$ with the same complexity.

3.3 3 Rounds

For 3 rounds, we have: $S = X^2 = R \oplus f_1(L) \oplus f_2(R)$ and $T \oplus S = f_3(X^1)$.

4-point CPA-1 and KPA using S. There is a CPA-1 with $m = 4$ messages. This attack was already published in [16], but we recall it here for sake of completeness. We choose 4 messages $[L_1, R_1]$, $[L_2, R_2]$, $[L_3, R_3]$, $[L_4, R_4]$ such that $L_3 = L_1$, $R_3 = R_2$, $L_4 = L_2$, $R_1 = R_4$ as in Section 2.2. From lemma 1 of Section 2.2, we have $X_1^2 \oplus X_2^2 \oplus X_3^2 \oplus X_4^2 = 0$, i.e. $S_1 \oplus S_2 \oplus S_3 \oplus S_4 = 0$. With a Misty scheme this happens with probability 1 and with a random permutation with probability $\frac{1}{2^n}$. Thus we have a CPA-1 with $m = 4$ on M_L^3. We can transform this CPA-1 into a KPA. When $m \simeq 2^n$, we can get with a non negligible probability 4 pairwise distinct indices (i, j, k, l) such that $L_i = L_j$, $L_k = L_l$; $R_i = R_k$, $R_j = R_l$ (since $\frac{m^4}{2^{4n}}$ is not negligible if $m \simeq 2^n$) and then we check if $S_i \oplus S_j \oplus S_k \oplus S_l = 0$.
Remark: There are 2-point KPA using $S \oplus T$ or S with the same complexity.

CPCA-2 with $m = 3$. We now give a CPCA-2 with $m = 3$ messages. As far as we know, this attack is new. It is inspired from [10] and [16].
Message 1: we choose $[L_1, R_1]$ randomly and get $[S_1, T_1]$.
Message 2: we choose $[S_2, T_2]$ such that $T_1 \oplus S_1 = T_2 \oplus S_2$ and obtain $[L_2, R_2]$ (inverse query: CPCA-2). Since $T \oplus S = f_3(X^1)$ and f_3 is a bijection we have $T_1 \oplus S_1 = T_2 \oplus S_2 \Leftrightarrow X_1^1 = X_2^1 \Leftrightarrow R_1 \oplus f_1(L_1) = R_2 \oplus f_1(L_2)$.
Message 3: We choose $[L_3, R_3] = [L_1, R_2]$ and we get $[S_3, T_3]$ (direct query). It is easy to check that $S_2 \oplus S_3 = R_1 \oplus R_2 \Leftrightarrow X_1^1 = X_2^1$. Thus for a Misty scheme, $S_2 \oplus S_3 = R_1 \oplus R_2$ appears with probability one and with probability about $\frac{1}{2^n}$ for a random permutation. This gives a CPCA-2 with $m = 3$ and $O(1)$ computations.

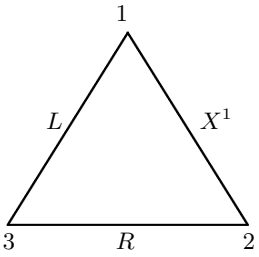

Fig. 4. The equalities in the CPCA-2 attack of M_L^3 with $m = 3$

3.4 4 Rounds

For 4 rounds, we have: $\begin{cases} S = X^2 = R \oplus f_1(L) \oplus f_2(R) \oplus f_3(R \oplus f_1(L)) \\ T \oplus S = f_4(X^2) = f_4(R \oplus f_1(L) \oplus f_2(R)) \end{cases}$.

CPCA-2 with $m = 4$ using $S \oplus T$. Here there is a CPCA-2 with $m = 4$ messages. (This attack was already published in [16], but we recall it here for sake of completeness).
Message 1: we randomly choose $[L_1, R_1]$ and get $[S_1, T_1]$.

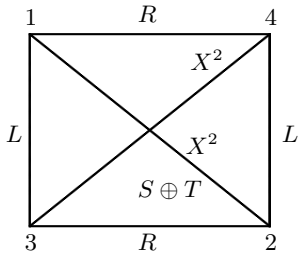

Fig. 5. The equalities in the CPCA-2 attack of M_L^4 with $m = 4$

Message 2: we choose $[S_2, T_2]$ such that $T_1 \oplus S_1 = T_2 \oplus S_2$. We obtain $[L_2, R_2]$. (Inverse query: this is a CPCA-2). Note that since $T_1 \oplus S_1 = T_2 \oplus S_2$, we have $X_1^2 = X_2^2$ (since $T \oplus S = f_4(X^2)$ and f_4 is a bijection).
Messages 3 and 4: we choose $[L_3, R_3]$ and $[L_4, R_4]$ such that $[L_3, R_3] = [L_1, R_2]$ and $[L_4, R_4] = [L_2, R_1]$. (Direct queries). Then from the "4-point property" (Section 2.2, lemma 1), we have $X_1^2 \oplus X_2^2 \oplus X_3^2 \oplus X_4^2 = 0$. Moreover since here $X_1^2 = X_2^2$, we have: $X_3^2 = X_4^2$, hence this gives $S_3 \oplus T_3 = S_4 \oplus T_4$. This equality will appear with probability 1 on a M_L^4, and with probability $\frac{1}{2^n}$ on a random permutation. This is a CPCA-2 with $m = 4$ and $O(1)$ computations.

This attack can be transformed in CPA-1 and KPA. But there exist better attacks, exposed below.

2-point attack using $S \oplus T$ with $\sqrt{2^n}$ computations in CPA-1 and 2^n in KPA. This attack may be new. However since it is a simple impossible differential attack, it was not difficult to find.

In CPA-1, we generate m messages such that $\forall i,\ 1 \leq i \leq m,\ R_i = 0$ (or R_i constant). Then we check if there exist $i, j,\ i \neq j$ such that $S_i \oplus T_i = S_j \oplus T_j$. With a random permutation, from the birthday paradox, we will have such collisions when $m \geq O(\sqrt{2^n})$. However on a M_L^4 this is impossible: we have $S \oplus T = f_4(R_{\oplus} f_1(L) \oplus f_2(R))$. Thus, since f_4 and f_1 are permutations, we get

$$\begin{cases} S_i \oplus T_i = S_j \oplus T_j \\ R_i = R_j \end{cases} \Leftrightarrow \begin{cases} R_i = R_j \\ L_i = L_j \end{cases},$$

which is impossible if $i \neq j$.

This CPA-1 can be immediately transformed in a KPA in $O(2^n)$: we look if there are some indices $i \neq j$ such that $T_i \oplus S_i = T_j \oplus S_j$ and $R_i = R_j$. In KPA, for a random permutation this will occur when $m^2 \geq 2^{2n}$, i.e. when $m \geq 2^n$ and with a M_L^4 this will never happen.

4 Attacks on 5 Rounds, With a Complexity Better Than 2^{2n}

4.1 4-point attacks.

For 5 rounds, we have: $\begin{cases} S = X^4 \\ T \oplus S = f_5(X^3) \end{cases}$. There are CPA-1 and KPA on M_L^5 with a complexity $\ll 2^{2n}$. Therefore, to avoid all generic attacks on Misty schemes with a complexity $\ll 2^{2n}$, at least 6 rounds have to be used.

Remark: For Feistel schemes ([10]) the result is similar: we need at least 6 rounds to avoid all attacks with complexity $\ll 2^{2n}$ (there are CPA-1 on ψ^5 in $O(2^n)$, and KPA in $O(2^{\frac{3n}{2}})$). The same holds for Feistel schemes with internal permutations ([19]), with same CPA-1 and KPA complexities (though different attacks). However, the attacks on ψ^5 and M_L^5 are *very* different: on ψ^5 they are 2-point attacks, but on M_L^5, they are 4-point attacks in CPA-1 and in KPA. Moreover, from the computations of Appendix B, we can prove that *all* 2-point attacks on M_L^5 have a complexity greater than 2^{2n}. Therefore it is not possible to find better 2-point attacks since no other 2-point attack exists.

CPA-1 on M_L^5, with complexity $O(2^n)$ The attack works as follows. We choose only 2 values for L: L_1 and L_2. Then, we choose $\simeq 2^n$ values for R_i (i.e. almost all the possible values for R_i). Therefore we have $m \simeq 2 \cdot 2^n$ messages. We count the number $\mathcal{N}$ of (R_i, R_j) values, $R_i \neq R_j$ such that with the 4 following messages:

$$i : [L_1, R_i],\ j : [L_1, R_j],\ i' : [L_2, R_i],\ j' : [L_2, R_j], \text{ we have : } \begin{cases} S_i \oplus T_i = S_j \oplus T_j \\ S_{i'} \oplus T_{i'} = S_{j'} \oplus T_{j'} \end{cases}$$

Remark: The complexity to compute $\mathcal{N}$ is in $O(2^n)$ since for all R_i value, we compute $[S_i, T_i] = M_L^5([L_1, R_i])$ and $[S_{i'}, T_{i'}] = M_L^5([L_2, R_i])$, store i at the address $[S_i \oplus T_i, S_{i'} \oplus T_{i'}]$ and count the collisions.

We are going to show that for a M_L^5, this number $\mathcal{N}$ is about twice the number we get for a random permutation. Since for a random permutation, we have $\mathcal{N} \simeq \frac{m^2}{2^{2n}}$, we will be able to distinguish when the probability to have $\mathcal{N} \geq 1$ is not negligible, i.e. when $m \geq 2^n$. We can also try another $[L_1, L_2]$; for each $[L_1, L_2]$ the probability of success of this attack is not negligible.

We have $S \oplus T = f_5(X^3)$ and f_5 is a permutation. Therefore:

$$\begin{cases} S_i \oplus T_i = S_j \oplus T_j \\ S_{i'} \oplus T_{i'} = S_{j'} \oplus T_{j'} \end{cases} \Leftrightarrow \begin{cases} X_i^3 = X_j^3 \\ X_{i'}^3 = X_{j'}^3 \end{cases}.$$

Now from the "4-point property" of Section 2.2 (lemma 1), we know that

$$\begin{cases} X_i^1 \oplus X_j^1 \oplus X_{i'}^1 \oplus X_{j'}^1 = 0 \quad (1) \\ X_i^3 \oplus X_j^3 \oplus X_{i'}^3 \oplus X_{j'}^3 = f_3(X_i^1) \oplus f_3(X_j^1) \oplus f_3(X_{i'}^1) \oplus f_3(X_{j'}^1) \quad (2) \end{cases}.$$

Note that $X^1 = f_1(L_1) \oplus R_1$. So $X_i^1 = X_j^1$ is impossible because $L_i = L_j$ and $X_i^1 = X_{i'}^1$ because $R_i = R_{i'}$. However we can have $X_i^1 = X_{j'}^1$ (with probability

$\simeq \frac{1}{2^n}$), and if this occurs from (1), then we will also have $X_j^1 = X_{i'}^1$ and if it follows (2), we will have $X_i^3 \oplus X_j^3 \oplus X_{i'}^3 \oplus X_{j'}^3 = 0$ (3).

We now see that for a M_L^5, we have two possibilities to get $\begin{cases} X_i^3 = X_j^3 \\ X_{i'}^3 = X_{j'}^3 \end{cases}$:

1. It can occur for random reasons when $X_i^1 \neq X_{j'}^1$ (probability about $\frac{1}{2^{2n}}$ when R_i and R_j are fixed),
2. It can occur as a consequence of $X_i^1 = X_{j'}^1$ and $X_i^3 = X_j^3$ (probability also about $\frac{1}{2^{2n}}$ when R_i and R_j are fixed).

Thus $\mathcal{N}$ for M_L^5 is about twice $\mathcal{N}$ for a random permutation, as announced. This shows that we can distinguish a random permutation from a M_L^5 in CPA-1 with $m \simeq 2^n$ messages and $O(2^n)$ computations, as claimed.

Transformation into a KPA The previous attack can be transformed into a KPA with complexity $O(2^{\frac{3n}{2}})$: we count the number $\mathcal{N}$ of (i, j, i', j') such that

$$\begin{cases} L_i = L_j \\ L_{i'} = L_{j'} \neq L_i \end{cases} \text{ and } \begin{cases} R_i = R_{i'} \\ R_j = R_{j'} \neq R_i \end{cases} \text{ and } \begin{cases} S_i \oplus T_i = S_j \oplus T_j \\ S_{i'} \oplus T_{i'} = S_{j'} \oplus T_{j'} \end{cases}$$

We have $\mathcal{N} \simeq \frac{m^4}{2^{6n}}$ for a random permutation, and $\mathcal{N} \simeq 2\frac{m^4}{2^{6n}}$ for a M_L^5. Therefore this KPA succeeds when $m \geq 2^{\frac{3n}{2}}$.

Remarks:

1. We have implemented these attacks and obtained a confirmation of our results. Details are given in Appendix C.
2. In [5], H. Gilbert and M. Minier proved CPCA-2 security for M_L^5 when $m \leq \sqrt{2^n}$.

4.2 Saturation Attack

This attack was suggested to us by [1] and is related to the attacks published in [6]. For 5 rounds, we have: $S = R \oplus f_1(L) \oplus f_2(R) \oplus f_3(R \oplus f_1(L)) \oplus f_4(R \oplus f_1(L) \oplus f_2(R))$. We choose 2^n messages $[L, R]$ such that $R = 0$ for all messages and L takes all the possible values. Then we compute the Xor of all resulting values S. With a Misty scheme we get 0 with probability 1 since f_1, f_2, f_3 and f_4 are permutations. For a random permutation, we get 0 with probability $\frac{1}{2^n}$. This gives a CPA-1 with complexity $O(2^n)$. We can notice that if instead of M_L^5, we use a function G such that $G = M_L^5$ except on a few points and on these few points G is purely random, this attack fails unlike our new attacks presented above.

5 Attacks in $O(2^{2n})$ on 6 Rounds

In order to distinguish M_L^d (or M_L^d generators i.e. generators of M_L^d permutations) from random even permutations of B_{2n}, 6 rounds is the maximum number

of rounds for which we know attacks in $O(2^{2n})$ computations. (This bound 2^{2n} is important since it is the total number of possible inputs $[L, R]$). The attack will be a *2-point attack* based on $S \oplus T$.

The attack is based on the following theorem.

Theorem 1 *Let $[L_1, R_1]$ and $[L_2, R_2]$ be two messages such that $R_1 = R_2$ and $L_1 \neq L_2$. Let p_1 be the probability that $S_1 \oplus T_1 = S_2 \oplus T_2$ if we have a M_L^6 and p_2 be the probability that $S_1 \oplus T_1 = S_2 \oplus T_2$ if we have a random permutation. Then $p_1 = \frac{2^n-2}{(2^n-1)^2}$ and $p_2 = \frac{1}{2^n+1}$. Therefore p_1 is slightly larger than p_2.*

Proof: For a random permutation, we have $2^{4n} - 2^{2n}$ possibilities for $[S_1, T_1, S_2, T_2]$ (since $S_1 = S_2 \Rightarrow T_1 \neq T_2$), and we have $2^{2n}(2^n - 1)$ of these solutions that satisfy $S_1 \oplus T_1 = S_2 \oplus T_2$ (1) (since we have 2^{2n} possibilities for S_1 and T_1, and then $2^n - 1$ possibilities for $S_2 \neq S_1$). Thus $p_2 = \frac{2^{2n}(2^n-1)}{2^{4n}-2^{2n}} = \frac{2^n-1}{2^{2n}-1} = \frac{1}{2^n+1}$. For a M_L^6, we have (since $R_1 = R_2$):

$$\begin{aligned} S_1 \oplus T_1 = S_2 \oplus T_2 &\Leftrightarrow f_6(X_1^4) = f_6(X_2^4) \\ &\Leftrightarrow X_1^4 = X_2^4 \\ &\Leftrightarrow f_1(L_1) \oplus f_3(R_1 \oplus f_1(L_1)) \oplus f_4(R_1 \oplus f_1(L_1) \oplus f_2(R_1)) \\ &\quad = f_1(L_2) \oplus f_3(R_2 \oplus f_1(L_2)) \oplus f_4(R_2 \oplus f_1(L_2) \oplus f_2(R_2)) \end{aligned}$$

Let α be the probability that $f_1(L_1) \oplus f_3(R_1 \oplus f_1(L_1)) = f_1(L_2) \oplus f_3(R_1 \oplus f_1(L_2))$ (2). We have $\alpha = \frac{1}{2^n-1}$. Indeed, $L_1 \neq L_2$ and f_1 being a bijection imply $f_1(L_1) \oplus f_1(L_2) \neq 0$. Moreover, f_3 is a bijection and $R_1 = R_2$, thus $f_3(R_1 \oplus f_1(L_2)) \oplus f_3(R_1 \oplus f_1(L_1))$ can take any value but 0 with probability $\frac{1}{2^n-1}$. When (2) occurs, (1) is impossible, since f_1 and f_4 are bijections and $L_1 \neq L_2$. When (2) does not occur, the probability to have (1) is exactly $\frac{1}{2^n-1}$, since f_1 and f_3 are bijections. So we have $p_1 = (1 - \alpha) \cdot \frac{1}{2^n-1}$. This gives $p_1 = \frac{2^n-2}{(2^n-1)^2}$ as claimed. □

Let us now go back to our attack. We count the number $\mathcal{N}$ of messages (i, j), $i < j$ such that $R_i = R_j$ and $S_i \oplus T_i = S_j \oplus T_j$. In KPA, for random permutations, we have $E(\mathcal{N}) = \frac{m(m-1)}{2 \cdot 2^{2n}}$ where m is the number of messages. The standard deviation is[4] $\sigma(\mathcal{N}) = O(\sqrt{E(\mathcal{N})}) = O(\frac{m}{2^n})$. For a M_L^6, we have from theorem 1 above $E(\mathcal{N}) \simeq \frac{m(m-1)}{2 \cdot 2^{2n}}\left(1 + \frac{1}{2^n}\right)$. Therefore, we can distinguish when $\frac{m^2}{2^{3n}} \geq \sigma(\mathcal{N})$, i.e. when $\frac{m^2}{2^{3n}} \geq O(\frac{m}{2^n})$, i.e. $m \geq O(2^{2n})$. The complexity of this KPA is $O(2^{2n})$ (same complexity in CPA-1 and CPCA-2).

Remarks:

1. If we attack a single permutation M_L^6, then $m \leq 2^{2n}$ since 2^{2n} is the total number of possible messages $[L, R] \in I_{2n}$. When the attack needs $m \simeq 2^{2n}$ messages, it has a fixed non-negligible probability of success (not near 0). If

[4] This can be proved by using the "covariance formula": $V(\sum_i X_i) = \sum_i V(X_i) + \sum_{i \neq j} Cov(X_i, X_j)$ (#)

we want to have for example a probability of success as near to 1 as wanted, we can assume that we attack M_L^6 generators (with many permutations).

2. There exist 4-point KPA on 6 rounds with the same complexity.

6 On the Use of the "h Coefficients" and 2-point Attacks

In the previous sections, we have studied 2-point attacks or 4-point attacks. As mentioned in Section 4, for 5 rounds, there is no 2-point attack with a complexity similar as the complexity of the 4-point attack. We briefly explain this fact and give an example for 6 rounds. More details are given in Appendix B.

We will systematically analyze all the probability deviation in the M_L^d inputs/outputs compared with truly random permutation of B_{2n}. We only make the analysis for pairs of messages $[L_1, R_1] \to [S_1, T_1]$ and $[L_2, R_2] \to [S_2, T_2]$ (with $[L_1, R_1] \neq [L_2, R_2]$ and $[S_1, T_1] \neq [S_2, T_2]$). We find this way the best "two point attacks", i.e. attacks that use a large number m of messages but that only use correlations on pairs of these messages (such as differential attacks for instance). We will denote by $H(L_1, R_1, L_2, R_2)$, or simply H, the number of internal permutations $(f_1, \ldots, f_d)$ such that:
$M_L^d(f_1, \ldots, f_d)([L_1, R_1]) = [S_1, T_1]$ and $M_L^d(f_1, \ldots, f_d)([L_2, R_2]) = [S_2, T_2]$.
The mean value for H is $\frac{|B_n|^d}{2^{2n}(2^{2n}-1)}$ since there are $2^{2n}(2^{2n}-1)$ values for (S_1, T_1, S_2, T_2) such that $[S_1, T_1] \neq [S_2, T_2]$. We will write $h = \frac{H \cdot 2^{4n}}{|B_n|^d}$, and $\overset{\circ}{1}$ stands for the mean value of h: $\overset{\circ}{1} = \frac{1}{1-\frac{1}{2^{2n}}} = \frac{2^{2n}}{2^{2n}-1}$ and $\epsilon = h - \overset{\circ}{1}$. In the following is explained how to evaluate the different H values, or equivalently the different h or ϵ values. The complete computations are done in Appendix B.

6.1 One Round

For M_L^1, we have: $S = R$ and $T = R \oplus f_1(L)$. Let (C) be the following conditions:
$\begin{cases} S_1 = R_1 \text{ and } S_2 = R_2, \\ L_1 = L_2 \Leftrightarrow T_1 \oplus R_1 = T_2 \oplus R_2. \end{cases}$ When (C) is not satisfied, $H = 0$. When (C) is satisfied, if $L_1 \neq L_2$, $H = \frac{|B_n|}{2^n(2^n-1)}$, and if $L_1 = L_2$, $H = \frac{|B_n|}{2^n}$.

6.2 More Rounds

For two or more rounds, we will distinguish between the following 13 cases (we can check that all possibilities correspond to exactly one of these cases, since $[L_1, R_1] \neq [L_2, R_2]$ and $[S_1, T_1] \neq [S_2, T_2]$).

$1 : L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 \neq S_1 \oplus S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2$
$2 : L_1 \neq L_2, R_1 = R_2, S_1 \neq S_2, (\text{then } R_1 \oplus R_2 \neq S_1 \oplus S_2), S_1 \oplus S_2 \neq T_1 \oplus T_2$
$3 : L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 \neq S_1 \oplus S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2$
$4 : L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 = S_1 \oplus S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2$
$5 : L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 = S_1 \oplus S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2$
$6 : L_1 \neq L_2, R_1 \neq R_2, S_1 = S_2, (\text{then } R_1 \oplus R_2 \neq S_1 \oplus S_2) S_1 \oplus S_2 \neq T_1 \oplus T_2$
$7 : L_1 \neq L_2, R_1 = R_2, S_1 = S_2, (\text{then } R_1 \oplus R_2 = S_1 \oplus S_2), S_1 \oplus S_2 \neq T_1 \oplus T_2$
$8 : L_1 = L_2, R_1 \neq R_2, S_1 = S_2, (\text{then } R_1 \oplus R_2 \neq S_1 \oplus S_2) S_1 \oplus S_2 \neq T_1 \oplus T_2$
$9 : L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 \neq S_1 \oplus S_2, S_1 \oplus S_2 = T_1 \oplus T_2$
$10 : L_1 \neq L_2, R_1 = R_2, S_1 \neq S_2, R_1 \oplus R_2 \neq S_1 \oplus S_2, S_1 \oplus S_2 = T_1 \oplus T_2$
$11 : L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 \neq S_1 \oplus S_2, S_1 \oplus S_2 = T_1 \oplus T_2$
$12 : L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 = S_1 \oplus S_2, S_1 \oplus S_2 = T_1 \oplus T_2$
$13 : L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 = S_1 \oplus S_2, S_1 \oplus S_2 = T_1 \oplus T_2$

We will denote by h_i^d, $1 \leq i \leq 13$, or simply by h_i when d is clearly fixed, the value of h in case i. (Similarly,ϵ_i^d, or ϵ_i denotes the value of ϵ in case i). These values are computed by induction (see Appendix B).

6.3 Example of Applications

Let us try to attack M_L^6 with ϵ_{10} (see Appendix B for the notations). First, we have to evaluate ϵ_{10} for 6 rounds. From $(E12)$ we know that $\epsilon_{10}^6 = \epsilon_9^4$. Thus, $\epsilon_{10}^6 = \frac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} \simeq \frac{1}{2^n}$. Case 10 is when $R_1 = R_2$ and $S_1 \oplus S_2 = T_1 \oplus T_2$. $\epsilon_{10}^6 \simeq \frac{1}{2^n}$ means that instead of having in KPA about $\frac{m^2}{2^{2n}}$ messages in this case 10, we will have about $\frac{m^2}{2^{2n}}(1+\frac{1}{2^n})$ such messages. The standard deviation in the case of two point attacks is about the square root of the mean value[5], hence here $\sigma = O(\frac{m}{2^n})$, and we will distinguish when $\frac{m^2}{2^{2n}} \cdot \frac{1}{2^n} \geq \frac{m}{2^n}$, i.e. when $m \geq O(2^{2n})$. This is exactly the two point attacks described in Section 5.

Remarks:

1. From the ϵ_{10}^6 value we can also easily recompute the probabilities p_1 and p_2 of Section 4. $p_2 = \frac{2^{2n}(2^n-1)}{2^{4n}} \overset{\circ}{1}$, since we have $2^{2n}(2^n-1)$ values (S_1, T_1, S_2, T_2) such that $S_1 \oplus S_2 = T_1 \oplus T_2$. This gives $p_2 = \frac{1}{2^n+1}$. Similarly, $p_1 = \frac{2^{2n}(2^n-1)}{2^{4n}}(\overset{\circ}{1} + \epsilon_{10})$, gives $p_1 = \frac{2^n-2}{(2^n-1)^2}$.
2. Theorem 1 of Section 5 can be seen as a property of the h_{10} coefficient, for 6 rounds of Misty.

7 Summary of the Best Known Generic Attacks on Misty Schemes

Our results are summarized in Table 1. In this table, we do not not mention CPA-2 and CPCA-1 since the best known results for these attacks are the same as for CPA-1.

[5] this can be proved from the covariance formula # seen in Section 5

Table 1. Minimum number A of computations needed to distinguish a Misty generator M_L^d from random even permutations of B_{2n}. For simplicity we denote 2^α for $O(2^\alpha)$.

	KPA	CPA-1	CPCA-2
M_L^1	1	1	1
M_L^2	$\sqrt{2^n}$	2	2
M_L^3	2^n	4	3
M_L^4	2^n	$\sqrt{2^n}$	4
M_L^5	$2^{3n/2}$	2^n	2^n
M_L^6	2^{2n}	2^{2n}	2^{2n}
M_L^7	2^{4n}	2^{4n}	2^{4n}
M_L^8	2^{4n}	2^{4n}	2^{4n}
M_L^9	2^{6n}	2^{6n}	2^{6n}
M_L^{10}	2^{6n}	2^{6n}	2^{6n}
M_L^d, d odd, $d \geq 9$	$2^{(d-3)n}$	$2^{(d-3)n}$	$2^{(d-3)n}$
M_L^d, d even, $d \geq 8$	$2^{(d-4)n}$	$2^{(d-4)n}$	$2^{(d-4)n}$

For Misty R schemes, M_R^d, the number of computations is the same, except for 3 rounds in CPA-1, where the best known attack is in $O(\sqrt{2^n})$ computations for M_R^3 (instead of 4 for M_L^3)

8 Conclusion

In this paper we presented different kinds of attacks on Misty schemes and our final results are summarized in Section 7. More attacks are given in the extended version of this paper. It is really fascinating to see how many different kind of attacks exist on Misty schemes: there are 2-points attacks on S, 2-points attacks on $S \oplus T$, 4-points attacks on S, 4-points attacks on $S \oplus T$, saturation attacks, brute force attacks, attacks on the signature since Misty schemes are even permutations (see the extended version). This is completely different than for Feistel schemes with internal functions [10], or also Feistel schemes with internal permutations [19]. It is really not obvious to see which attacks give the best complexity before making a systematic and precise analysis.

There are still many open problems on generic Misty schemes. For example, several gaps remain between the proof of security in $O(\sqrt{2^n})$ (birthday bound) obtained in [5, 15, 17, 18] and the best known attacks. For a security less than or equal to 2^n, generalizations of what was done on ψ^k (cf [11, 9]) are probably possible.

References

1. Personal Anonymous Communication.
2. Specification of the 3GPP Confidentiality and Integrity Algorithm KASUMI. Document available on http://www.etsi.org/.

3. William Aiello and Ramarathnam Venkatesan. Foiling Birthday Attacks in Length-Doubling Transformations - Benes: A Non-Reversible Alternative to Feistel. In Ueli M. Maurer, editor, *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 307–320. Springer-Verlag, 1996.
4. Don Coppersmith. Luby-Rackoff: Four Rounds is not enough. Technical report, Technical Report RC20674, IBM Research Report, December 1996.
5. Henri Gilbert and Marine Minier. New Results on the Pseudorandomness of Some Blockcipher Constructions. In Mitsuru Matsui, editor, *Fast Software Encrytion – FSE '01*, volume 2355 of *Lecture Notes in Computer Science*, pages 248–266. Springer-Verlag, 2001.
6. Lars Knudsen and David Wagner. Integral Cryptanalysis. In Joan Daemen and Vincent Rijmen, editors, *Fast Software Encrytion – FSE '2002*, volume 2365 of *Lecture Notes in Computer Science*, pages 112–127. Springer-Verlag, 2002.
7. Xuejia. Lai and James.L. Massey. A Proposal for a New Block Encrytption Standard. In Ivan Damgård, editor, *Advances in Cryptology – EUROCRYPT '90*, volume 473 of *Lecture Notes in Computer Science*, pages 389–404. Springer-Verlag, 1991.
8. Mitsuru Matsui. New Block Encrytpion Algorithm. In Eli Biham, editor, *Fast Software Encrytion – FSE '97*, volume 1267 of *Lecture Notes in Computer Science*, pages 54–68. Springer-Verlag, 1997.
9. Ueli Maurer and Krzysztof Pietrzak. The Security of Many-Round Luby-Rackoff Pseudo-Random Permutations. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT '2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 544–561. Springer-Verlag, 2003.
10. Jacques Patarin. Generic Attacks on Feistel Schemes. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 222–238. Springer-Verlag, 2001.
11. Jacques Patarin. Security of Random Feistel Schemes with 5 or more rounds. In Matthiew K. Franklin, editor, *Advances in Cryptology – CRYPTO '2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 106–122. Springer-Verlag, 2004.
12. Jacques Patarin. A Proof of Security in $O(2^n)$ for the Benes Schemes. In Serge Vaudenay, editor, *Progress in Cryptology – AFRICACRYPT '2008*, volume 5023 of *Lecture Notes in Computer Science*, pages 209–220. Springer-Verlag, 2008.
13. Jacques Patarin, Valérie Nachef, and Côme Berbain. Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions. In Xuejia Lai and Kefei Chen, editors, *Advances in Cryptology – ASIACRYPT '2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 396–411. Springer-Verlag, 2006.
14. Jacques Patarin, Valérie Nachef, and Côme Berbain. Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions. In Kaoru Kurosawa, editor, *Advances in Cryptology – ASIACRYPT '2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 325–341. Springer-Verlag, 2007.
15. Gilles Piret and Jean-Jacques Quisquater. Security of the MISTY Structure in the Luby-Rackoff Model: Improved results. In Helena Handschuh and Anwar Hasan, editors, *Selected Areas in Cryptography– SAC '04*, volume 3357 of *Lecture Notes in Computer Science*, pages 100–115. Springer-Verlag, 2005.
16. Kouichi Sakurai and Yuliang Zheng. On Non-Pseudorandomness from Block Ciphers with Provable Immunity Against Linear Cryptanalysis. In *IEICE Trans. Fundamentals*, volume E80-A,n.1, January 1997.
17. M. Sugita. Pseudorandomness of a Block Cipher MISTY. Technical report, Technical Report of IEIECE, ISEC 96-9.

18. M. Sugita. Pseudorandomness of a Block Cipher with Recursive Strictures. Technical report, Technical Report of IEIECE, ISEC 97-9.
19. Joana Treger and Jacques Patarin. Generic Attacks on Feistel Networks with Internal Permutations. In Bart Preneel, editor, *Progresses in Cryptology – AFRICACRYPT '09*, Lecture Notes in Computer Science. Springer-Verlag, 2009.

A Attacks for 7 rounds and more than 7 rounds

The attacks that we have seen for 6 rounds can be extended for $d \geq 7$ rounds in order to distinguish M_L^d generators from random permutations of B_{2n} generators. When $d \geq 7$ the complexity of the best known attacks are strictly greater than 2^{2n} and we will use λ permutations of the generator with $\lambda > 1$.

2-point Attacks when d is even, $d \geq 8$.

Theorem 2 *Let $[L_1, R_1]$ and $[L_2, R_2]$ be two messages such that $R_1 = R_2$ and $L_1 \neq L_2$. Let p_1 be the probability that $S_1 \oplus T_1 = S_2 \oplus T_2$ if we have a M_L^d, d even, $d \geq 6$ and p_2 be the probability that $S_1 \oplus T_1 = S_2 \oplus T_2$ if we have a random permutation. Then $p_1 - p_2 = \frac{(-1)^{\frac{d}{2}+1}}{(2^n)^{\frac{d}{2}-2}} + O\Big(\frac{1}{(2^n)^{\frac{d}{2}-1}}\Big)$.*

Proof: This can be easily proved directly by induction (it is just a generalization of what we did for Theorem 1), or by using the ϵ_{10} values that we compute in Appendix B. □

Let us now go back to the attacks. We count the number $\mathcal{N}$ of messages i, j, $i < j$ that belong to the same permutation and such that $R_i = R_j$ and $S_i \oplus T_i = S_j \oplus T_j$.

In KPA, for λ random permutations with m messages per permutation we have: $E(\mathcal{N}) = \lambda \frac{m(m-1)}{2 \cdot 2^{2n}}$ and the standard deviation is $\sigma(\mathcal{N}) = O(\frac{m\sqrt{\lambda}}{2^n})$. (The fact that $\sigma(\mathcal{N}) = \sqrt{E(\mathcal{N})}$ can easily be proved from the "covariance formula" (#) of Section 5). For a M_L^d, d even, $d \geq 6$, we will have $E(\mathcal{N}) \simeq \lambda \frac{m(m-1)}{2 \cdot 2^{2n}} \Big(1 + \frac{(-1)^{\frac{d}{2}+1}}{(2^n)^{\frac{d}{2}-2}}\Big)$ (cf Theorem 2 above). Therefore we can distinguish when: $\frac{\lambda m^2}{2^{n\frac{d}{2}}} \geq \sigma(\mathcal{N}) = 0(\frac{m\sqrt{\lambda}}{2^n})$, i.e. $\sqrt{\lambda} m \geq 2^{n(\frac{d}{2}-1)}$, or $\lambda m^2 \geq 2^{n(d-2)}$. With $m \simeq 2^{2n}$, this gives $\lambda \geq 2^{n(d-6)}$ and a complexity $\lambda \cdot 2^{2n} = 2^{n(d-4)}$.
Conclusion: when d is even and $d \geq 6$, we can distinguish M_L^d generators from truly random permutation generators of B_{2n} with a complexity in $O(2^{n(d-4)})$.

2-point attack when d is odd, $d \geq 7$. When d increases, the security of M_L^d can only increase, since we have compositions of permutations with independent secret values $f_1, \ldots, f_d$. Since M_L^{d+1} can be attacked in $O(2^{n(d+1-4)}) = O(2^{n(d-3)})$ from the result above, when d is odd the security of M_L^d generators is at maximum in $O(2^{n(d-3)})$. This value $O(2^{n(d-3)})$ can be achieved by computing the number $\mathcal{N}$ of messages i, j, $i < j$ that belong to the same permutation and

such that $R_i = R_j$ and $S_i \oplus T_i = S_j \oplus T_j$. (This is the same attack as for d even, but with complexity $O(2^{n(d-3)})$ instead of $O(2^{n(d-4)})$). This 2-point attack using $S \oplus T$ is based on the coefficient ϵ_{10} that is computed in Appendix B. When d is odd, another attack, with the same complexity $O(2^{n(d-3)})$ is obtained by computing the number $\mathcal{N}$ of messages i, j, $i < j$ that belong to the same permutation and such that $L_i = L_j$ and $S_i \oplus T_i = S_j \oplus T_j$. This 2-point attack using $S \oplus T$ is based on the ϵ_{11} coefficient that is computed in Appendix B. The complexity of these attacks ($O(2^{n(d-3)})$) can be easily proved by induction (this is a simple generalization of the 2-point attack given for 6 rounds), or by using the evaluation for the ϵ_{10} and ϵ_{11} coefficients that we compute in Appendix B.

4-point attack when $d \geq 7$. The 4-point attacks given for $d = 6$ can be generalized to attack M_L^d generators for $d \geq 7$. For $d = 6$ and $d = 7$ this will just give the same complexity as the 2-point attacks. For $d \geq 8$ the complexity will be worse. In fact, when $d \geq 6$ the best known 4-point attacks have a complexity of $O(2^{(2d-10)n})$ and this is worse than the complexity $O(2^{(d-4)n})$ for d even or $O(2^{(d-3)n})$ for d odd of the 2-point attacks when $d \geq 8$. (We do not give much details for these 4-point attacks when $d \geq 7$ since the complexities are equal or worse than those of the 2-point attacks).

B Computation of the "h Coefficients"

In this appendix, we give more details about the computation of the "h coefficients" presented in Section 6.

B.1 2 Rounds

For 2 rounds, we have $S = R \oplus f_1(L)$ and $T \oplus S = f_2(R)$. We can easily compute the h_i values and the $\epsilon_i = h_i - \overset{\circ}{1}$ values. We get for 2 rounds:

$$h_1 = \frac{2^{2n}}{(2^n-1)^2} \; ; \; \epsilon_1 = \frac{2 \cdot 2^{2n}}{(2^n-1)^2(2^n+1)} \simeq \frac{2}{2^n}$$
$$h_2 = 0 \quad ; \quad \epsilon_2 = \frac{-2^{2n}}{(2^n-1)(2^n+1)} \simeq -1$$
$$h_3 = 0 \quad ; \quad \epsilon_3 = -\overset{\circ}{1} \simeq -1$$
$$h_4 = 0 \quad ; \quad \epsilon_4 = -\overset{\circ}{1} \simeq -1$$
$$h_5 = \frac{2^{2n}}{2^n-1} \quad ; \quad \epsilon_5 = \frac{2^{3n}}{(2^n-1)(2^n+1)} \simeq 2^n$$
$$h_6 = \frac{2^{2n}}{(2^n-1)^2} \; ; \; \epsilon_6 = \frac{2 \cdot 2^{2n}}{(2^n-1)^2(2^n+1)} \simeq \frac{2}{2^n}$$
$$h_7 = 0 \quad ; \quad \epsilon_7 = -\overset{\circ}{1} \simeq -1$$
$$h_8 = 0 \quad ; \quad \epsilon_8 = -\overset{\circ}{1} \simeq -1$$
$$h_9 = 0 \quad ; \quad \epsilon_9 = -\overset{\circ}{1} \simeq -1$$
$$h_{10} = \frac{2^{2n}}{2^n-1} \; ; \; \epsilon_{10} = \frac{2^{3n}}{(2^n-1)(2^n+1)} \simeq 2^n$$
$$h_{11} = 0 \quad ; \quad \epsilon_{11} = -\overset{\circ}{1} \simeq -1$$
$$h_{12} = 0 \quad ; \quad \epsilon_{12} = -\overset{\circ}{1} \simeq -1$$
$$h_{13} = 0 \quad ; \quad \epsilon_{13} = -\overset{\circ}{1} \simeq -1$$

B.2 Induction

Using the fact that M_L^{d+1} is the composition of a M_L^d, and our values of H for M_L^1, we get induction formulas on the h_i coefficients (for $d \geq 2$).

To simplify the notations, we will denote h_i^d by h_i and h_i^{d+1} by h'_i. With these notations, the induction formulas are:

$$(D1)\begin{cases} h'_1 = \frac{1}{2^n-1}[(2^n-3)h_1 + h_2 + h_4] \\ h'_2 = \frac{1}{2^n-1}[(2^n-2)h_3 + h_5] \\ h'_3 = h_1 \\ h'_4 = \frac{1}{2^n-1}[(2^n-2)h_1 + h_2] \\ h'_5 = h_4 \end{cases}$$

$$(D2)\begin{cases} h'_6 = \frac{1}{2^n-1}[(2^n-2)h_6 + h_7] \\ h'_7 = h_8 \\ h'_8 = h_6 \end{cases} \qquad (D3)\begin{cases} h'_9 = \frac{1}{2^n-1}[(2^n-3)h_9 + h_{10} + h_{12}] \\ h'_{10} = \frac{1}{2^n-1}[(2^n-2)h_{11} + h_{13}] \\ h'_{11} = h_9 \\ h'_{12} = \frac{1}{2^n-1}[(2^n-2)h_9 + h_{10}] \\ h'_{13} = h_{12} \end{cases}$$

From these equations we can compute all the h_i^d values, for any $d \geq 2$ by induction from the previous values. We will continue the evaluation in order to see how small the ϵ values are.

We have, for all S_1, T_1, S_2, T_2: $\sum_{L_1,R_1,L_2,R_2} H(L,R,S,T) = |B_n|^d$ $(D4)$ since each output comes from exactly one input. Similarly, for all L_1, R_1, L_2, R_2: $\sum_{S_1,T_1,S_2,T_2} H(L,R,S,T) = |B_n|^d$ $(D5)$ since each input gives exactly one output. With $h = \frac{H \cdot 2^{4n}}{|B_n|^d}$ we obtain: For all S, T: $\sum_{L,R} h(L,R,S,T) = 2^{4n}$ $(D6)$. For all L, R: $\sum_{S,T} h(L,R,S,T) = 2^{4n}$ $(D7)$. When we specify S, T, $(D6)$ gives 3 equations on the h_i values:

- When $S_1 \neq S_2$ and $S_1 \oplus S_2 \neq T_1 \oplus T_2$:
  $(2^n-1)(2^n-2)h_1 + (2^n-1)h_2 + (2^n-2)h_3 + (2^n-1)h_4 + h_5 = 2^{2n}$ $(D8)$
- When $S_1 = S_2$ and $S_1 \oplus S_2 \neq T_1 \oplus T_2$: $(2^n-1)h_6 + h_7 + h_8 = \frac{2^{2n}}{2^n-1}$ $(D9)$.
- When $S_1 \oplus S_2 = T_1 \oplus T_2$ and $S_1 \neq S_2$:
  $(2^n-1)(2^n-2)h_9 + (2^n-1)h_{10} + (2^n-2)h_{11} + (2^n-1)h_{12} + h_{13} = 2^{2n}$ $(D10)$.

Similarly, when we specify values L, R, $(D7)$ gives 3 equations on the h_i values:

- When $L_1 \neq L_2$ and $R_1 \neq R_2$:
  $(2^n-1)(2^n-2)h_1 + (2^n-1)h_4 + (2^n-1)h_6 + (2^n-2)h_9 + h_{12} = 2^{2n}$ $(D11)$.
- When $L_1 = L_2$ and $R_1 \neq R_2$:
  $(2^n-1)(2^n-2)h_3 + (2^n-1)h_5 + (2^n-1)h_8 + (2^n-2)h_{11} + h_{13} = 2^{2n}$ $(D12)$
- When $R_1 = R_2$ and $L_1 \neq L_2$: $(2^n-1)h_2 + h_7 + h_{10} = \frac{2^{2n}}{2^n-1}$ $(D13)$

Indices 1,2,3,4,5. From $(D1)$ and $(D8)$, and by using the ϵ_i variables instead of the h_i variables, $\epsilon_i = h_i - \overset{\circ}{1}$, we get:

$$(E1)\begin{cases} \epsilon'_1 = \frac{(2^n-3)\epsilon_1}{2^n-1} + \frac{\epsilon_2}{2^n-1} + \frac{\epsilon_4}{2^n-1} \\ \epsilon'_2 = (-2^n+2)\epsilon_1 - \epsilon_2 - \epsilon_4 \\ \epsilon'_4 = \frac{(2^n-2)\epsilon_1}{2^n-1} + \frac{\epsilon_2}{2^n-1} \end{cases} \quad (E2)\begin{cases} \epsilon'_3 = \epsilon_1 \\ \epsilon'_5 = \epsilon_4 \end{cases}$$

From these equations, we can compute all the ϵ_i values by induction, but we want more: we want to evaluate how fast the ϵ_i values decrease. We have: $\epsilon'_1 - \epsilon'_4 = \frac{-(\epsilon_1-\epsilon_4)}{2^n-1}$. Thus, by induction: $(\epsilon_1 - \epsilon_4) = \frac{(-1)^k \cdot 2^{2n}}{(2^n-1)^k}$ $(E3)$. Moreover, if we denote $\epsilon''_i = \epsilon_i^{d+2}$, $\epsilon'_i = \epsilon_i^{d+1}$, $\epsilon_i = \epsilon_i^d$, we have:
$(E4)$ $\epsilon''_1 = \frac{-\epsilon_1 - 2\epsilon'_1 + \epsilon'_4}{2^n-1}$ $\epsilon''_2 = \epsilon_1 + \epsilon'_1 + \epsilon'_4; \epsilon''_4 = \frac{-\epsilon_1 - \epsilon'_1}{2^n-1}$.
$(E5)$ $\epsilon'_3 = \epsilon_1$ $\epsilon'_5 = \epsilon_4$.

These equations show that the ϵ_i values globally decrease by a factor of about 2^n every 2 rounds (for the indices $1, 2, 3, 4, 5$).

Indices 6,7,8. From $(D2)$ and $(D9)$, and by using the ϵ_i variables instead of the h_i variables, $\epsilon_i = h_i - \overset{\circ}{1}$,
$(E6)$ $\epsilon'_6 = \frac{-\epsilon_6 - \epsilon_8}{2^n-1}$, $\epsilon'_8 = \epsilon_6$, and $(E7)$ $\epsilon'_7 = \epsilon_8$
These equations show that ϵ_6, ϵ_7, ϵ_8 will decrease by a factor about 2^n each time we add two rounds.

Indices 9,10,11,12,13. From $(D3)$ and $(D10)$, and by using the ϵ_i variables instead of the h_i variables ($\epsilon_i = h_i - \overset{\circ}{1}$), we get:

$$(E8) \begin{cases} \epsilon'_9 = \frac{2^n-3}{2^n-1}\epsilon_9 + \frac{\epsilon_{10}}{2^n-1} + \frac{\epsilon_{12}}{2^n-1} \\ \epsilon'_{10} = (-2^n+2)\epsilon_9 - \epsilon_{10} - \epsilon_{12} \\ \epsilon'_{12} = \frac{2^n-2}{2^n-1}\epsilon_9 + \frac{\epsilon_{10}}{2^n-1} \end{cases} \quad (E9) \begin{cases} \epsilon'_{11} = \epsilon_9 \\ \epsilon_{13} = \epsilon_{12} \end{cases}$$

Moreover by induction from $(E8)$ and the initial values for 2 rounds, we get $\epsilon_9 = \epsilon_{12}$ (thus $h_9 = h_{12}$). Thus we have:
$(E10)$ $\epsilon'_9 = \frac{2^n-2}{2^n-1}\epsilon_9 + \frac{\epsilon_{10}}{2^n-1}$ $\epsilon'_{10} = (-2^n+1)\epsilon_9 - \epsilon_{10} = \epsilon_{11}$.
$(E11)$ $\epsilon'_{11} = \epsilon_9$ $\epsilon'_{13} = \epsilon_9$ $\epsilon_{12} = \epsilon_9$.
If we denote $\epsilon''_i = \epsilon_i^{d+2}$, we have: $\epsilon''_{10} = \frac{-\epsilon_{10} - \epsilon'_{10}}{2^n-1} = \epsilon_9$ $(E12)$
These equations $(E11), (E12)$, show that $\epsilon_9, \epsilon_{10}, \epsilon_{11}, \epsilon_{12}, \epsilon_{13}$ globally decrease by a factor 2^n every two rounds. With the formulas above, we can compute all the values ϵ_i and evaluate ϵ_i for any round.

Expression as power of complex numbers. It is also possible to formulate all the ϵ_i by using these two complex numbers β and λ:
$\lambda = \frac{1}{2(2^n-1)}(-1 + i\sqrt{4 \cdot 2^n - 5})$ $\beta = \frac{2^{2n}}{(2^n-1)(2^n+1)}(2^n + \frac{i(2^n-2)}{\sqrt{4 \cdot 2^n - 5}})$.
λ, $\overline{\lambda}$ and $\frac{-1}{2^n-1}$ are the 3 eigenvalues that occur in the induction relation among the variables, and we have $|\lambda| = \frac{1}{\sqrt{2^n-1}}$, and $\lambda^2(2^n-1) + \lambda + 1 = 0$. Let $Re(z)$ be the real value of a complex number z. Then, after d rounds, we have:

$$\begin{aligned} \epsilon_1^d &= \frac{(-1)^d \cdot 2^{2n}}{(2^n-1)^{d+1}} + Re(\beta \cdot \lambda^{d+2}) \\ \epsilon_2^d &= Re(\lambda^d \beta) = \epsilon_9^d \\ \epsilon_3^d &= \frac{(-1)^{d+1} \cdot 2^{2n}}{(2^n-1)^d} + Re(\beta \cdot \lambda^{d+1}) = \epsilon_1^{d-1} \end{aligned}$$

$$
\begin{array}{lcccl}
\epsilon_4^d & = & \frac{(-1)^{d+1}\cdot 2^{2n}(2^n-2)}{(2^n-1)^{d+1}} + Re(\beta\cdot\lambda^{d+2}) & = & \epsilon_1^d + \frac{(-1)^{d+1}\cdot 2^{2n}}{(2^n-1)^d} \\
\epsilon_5^d & = & \frac{(-1)^{d}\cdot 2^{2n}(2^n-2)}{(2^n-1)^{d}} + Re(\beta\cdot\lambda^{d+1}) & = & \epsilon_4^{d-1} \\
\epsilon_6^d & = & Re(\lambda^{d+1}\beta) & = & \epsilon_9^{d+1} \\
\epsilon_7^d & = & Re(\lambda^{d-1}\beta)) & = & \epsilon_9^{d-1} \\
\epsilon_8^d & = & Re(\lambda^{d}\beta) & = & \epsilon_9^{d} \\
\epsilon_9^d & = & Re(\lambda^{d}\beta) & & \\
\epsilon_{10}^d & = & Re(\lambda^{d-2}\beta) & = & \epsilon_9^{d-2} \\
\epsilon_{11}^d & = & Re(\lambda^{d-1}\beta) & = & \epsilon_9^{d-1} \\
\epsilon_{12}^d & = & Re(\lambda^{d}\beta) & = & \epsilon_9^{d} \\
\epsilon_{13}^d & = & Re(\lambda^{d-1}\beta) & = & \epsilon_9^{d-1}
\end{array}
$$

C Experimental Results

We implemented our new 4-point attack on 5-round L schemes described in Section 4. For each test we ran, we generated some messages (i, j, k, l) and then checked the number of collisions $S_i \oplus T_i = S_j \oplus T_j$ and $S_k \oplus T_k = S_l \oplus T_l$ obtained, for all 4-tuples of messages (i, j, k, l) verifying $L_i = L_j$, $L_k = L_l$, $R_i = R_k$, $R_j = R_l$. Note that we considered only one 4-tuple amongst (i, j, k, l), (j, i, l, k), (l, k, j, i) and (k, l, i, j). Table 2 summarizes the results obtained.

The length of the messages considered in this implementation is 32 bits (blocs of length $n = 16$). To simulate random permutations, we used Feistel schemes with a number of rounds between 20 and 50.

Table 2. Average of the number of collisions of type $S_i \oplus T_i = S_j \oplus T_j$ and $S_k \oplus T_k = S_l \oplus T_l$ obtained in the case of a M_L scheme or a random permutation.

	Average of the number of collisions $S_i \oplus T_i = S_j \oplus T_j$ and $S_k \oplus T_k = S_l \oplus T_l$ obtained in the case of a M_L scheme	Average of the number of collisions $S_i \oplus T_i = S_j \oplus T_j$ and $S_k \oplus T_k = S_l \oplus T_l$ obtained in the case of a random permutation
$3 \cdot 2^n$ messages $\{[L,R], L=a,b,c,\ R,\in I_n\}$	1	0.23
$4 \cdot 2^n$ messages $\{[L,R], L=a,b,c,\ R \in I_n\}$	1.6	0.84
$5 \cdot 2^n$ messages $\{[L,R], L=a,b,c,d,e,\ R \in I_n\}$	3.15	1.3

As claimed in Section 4, we obtain two times more collisions in the case of a L scheme than in the case of a random permutation. Therefore, we are able to distinguish most of the 5 round L schemes from a random permutation with $O(2^n)$ messages.