Generic Attacks on Misty Schemes
-5 rounds is not enough-

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 blockcipher 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. One important result of this paper is that we will show that when $d = 5$ rounds, there exist such attacks with a complexity strictly less than 2^{2n}. Consequently, at least 6 rounds are necessary to avoid these generic attacks on Misty schemes. When $d \geq 6$ we also describe some attacks on Misty generators, i.e. attacks where more than one Misty permutation is required.

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 function (or permutations) is the d-round Feistel construction, that we will denote ψ^d: $f = \psi^d(f_1, \dots, f_d)$, where $f_1, \dots, f_d$ 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 ([5]), unbalanced Feistel schemes with expanding or contracting internal functions ([12], [13]), 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: $f = M^d(f_1, \dots, f_d)$, where $f_1, \dots, f_d$ 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 [6], as well as in the Kasumi variant of Misty adopted as standard block cipher for encryption and integrity protection in third generation mobile systems ([1]). 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 not always pseudo-random, and therefore there are 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 applied 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 ([8]) and unbalanced Feistel schemes ([12], [13]) already exist, but no similar presentation and analysis for Misty schemes was written so far. Some specific results on Misty schemes attacks or security have been already published ([4], [14], [15], [16], [17] ...). Sometimes the attacks previously found 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 (cf [8]), unbalanced Feistel schemes with expanding functions F_k^d (cf [13]) and Butterfly and Benes schemes (cf [2], [10]). For Feistel schemes ψ^d, the best known generic attacks are "2 point attacks", i.e. attacks that use correlations on (many) pairs of messages (such as differential attacks), cf [8]. 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 (cf [13]). For Butterfly schemes, the best known generic attacks are "4 points" attacks (cf [2], [10]). Here for Misty schemes, the best known attacks will be sometimes "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 secure or less secure than for example Feistel schemes ψ^d for a given number of rounds. Our final results will be summarized in Appendix G.

2 Notation

We use the following notation

- $I_n = \{0,1\}^n$ 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 bit by bit exclusion 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 $|B_n| = (2^n)!$.

Let f_1 be a permutation of B_n. Let L, R, S and T be elements in I_n. Then by definition

$$M_L(f_1)([L, R] = [S, T] \Leftrightarrow S = R \text{ and } T = R \oplus f_1(L)$$

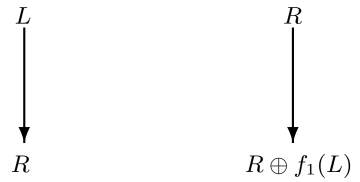

Fig. 1. One round of the Misty L scheme

Let $f_1, \ldots, f_d$ be d bijections of B_n. Then by definition:

$$M_L^d(f_1, \ldots, f_d) = M_L(f_d) \circ \ldots \circ M_L(f_2) \circ M_L(f_1)$$

The permutation $M_L^d(f_1, \ldots, f_d)$ is called a "Misty L scheme with d rounds".

Similarly there is a slightly different construction named the Misty R scheme. By definition

$$M_R(f_1)([L, R] = [S, T] \Leftrightarrow S = R \oplus f_1(L) \text{ and } T = f_1(L)$$

$$M_R^d(f_1, \ldots, f_d) = M_R(f_d) \circ \ldots \circ M_R(f_2) \circ M_R(f_1)$$

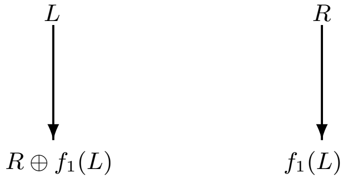

Fig. 2. One round of the Misty R scheme

The permutation $M_R^d(f_1, \ldots, f_d)$ is called a "Misty R scheme with d rounds". 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.

Messages

In our attacks, we will denote by m the number of input/output messages that we will use. $\forall i,\ 1 \leq i \leq m$, we will denote by $[L_i, R_i]$ the cleartext of message i, and by $[S_i, T_i]$ the ciphertext of this message i. Without loosing generality we can always assume that the messages $[L_i, R_i]$ are pairwise distinct ($L_i = L_j \,\text{and}\, i \neq j \Rightarrow R_i \neq R_j$)

3 Some general Properties of the M_L and M_R schemes

3.1 Inversion

Let $f_1 \in B_n$. Let $\Lambda(f_1)$, or simply Λ, be the permutation of B_{2n} such that $\forall [L, R] \in I_{2n},\ \Lambda([L, R]) \overset{def}{=} [f_1(L), R]$.

Let μ be the permutation of B_{2n} such that $\forall [L, R] \in I_{2n},\ \mu([L, R]) \overset{def}{=} [R, L \oplus R]$.

We have $\big(\Lambda(f_1)\big)^{-1} = \Lambda(f_1^{-1})$.

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

$$\begin{cases} M_L = \mu \circ \Lambda \\ M_R = \mu^{-1} \circ \Lambda \end{cases}$$

Therefore $M_L^{-1}(f_1) = \Lambda(f^{-1}) \circ \mu^{-1} = \mu \circ M_R(f_1^{-1}) \circ \mu^{-1}$. 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 an M_R function, after composition by μ on the inputs and outputs. This shows that 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 give rapidly the difference in CPA for the Misty variant M_R.

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

1 round : $\begin{cases} S = R \\ T = R \oplus f_1(L) \end{cases}$ We will denote $X^1 = R \oplus f_1(L)$

2 rounds : $\begin{cases} S = R \oplus f_1(L) \\ T = R \oplus f_1(L) \oplus f_2(R) \end{cases}$

Alternatively : $\begin{cases} S = X^1 \\ T \oplus S = f_2(R) \end{cases}$ We will denote $X^2 = R \oplus f_1(L) \oplus f_2(R) = X^1 \oplus f_2(R)$

3 rounds : $\begin{cases} S = R \oplus f_1(L) \oplus f_2(R) \\ T = S \oplus f_3(R \oplus f_1(L)) \end{cases}$

Alternatively : $\begin{cases} S = X^2 \\ T \oplus S = f_3(X^1) \end{cases}$ We will denote $X^3 = X^2 \oplus f_3(X^1)$

4 rounds : $\begin{cases} S = R \oplus f_1(L) \oplus f_2(R) \oplus f_3(R \oplus f_1(L)) \\ T = S \oplus f_4(R \oplus f_1(L) \oplus f_2(R)) \end{cases}$

Alternatively : $\begin{cases} S = X^3 \\ T \oplus S = f_4(X^2) \end{cases}$ We will denote $X^4 = X^3 \oplus f_4(X^2)$

More generally, for d rounds: $\begin{cases} S = X^{d-1} \\ T \oplus S = f_d(X^{d-2}) \end{cases}$ 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 loosing 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.

3.3 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 $[L_1, R_1]$, $[L_2, R_2]$, $[L_1, R_2]$, $[L_2, R_1]$

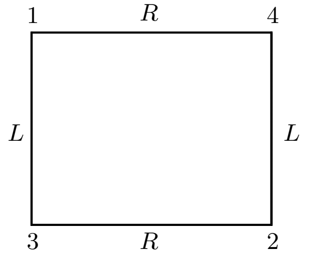

Fig. 3. The equalities in L and R for the "4 point" property

Theorem 1 *For such 4 messages, we always have:*

$$\begin{aligned}
&X_1^1 \oplus X_2^1 \oplus X_3^1 \oplus X_4^1 = 0\\
&X_1^2 \oplus X_2^2 \oplus X_3^2 \oplus X_4^2 = 0\\
&X_1^3 \oplus X_2^3 \oplus X_3^3 \oplus X_4^3 = f_3(X_1^1) \oplus f_3(X_2^1) \oplus f_3(X_3^1) \oplus f_3(X_4^1)
\end{aligned}$$

(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,

$$\begin{aligned}
X_i^1 &\overset{def}{=} R_i \oplus f_1(L_i)\\
X_i^2 &\overset{def}{=} R_i \oplus f_1(L_i) \oplus f_2(R_i)\\
X_i^3 &\overset{def}{=} X_i^2 \oplus f_3(X_i^1)\\
X_i^4 &\overset{def}{=} X_i^3 \oplus f_4(X_i^2)
\end{aligned}$$

□

4 Attacks on M_L^d, $1 \le d \le 4$

4.1 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 one and with a random permutation with probability $\frac{1}{2^n}$.

4.2 2 rounds

After 2 rounds we have: $\begin{cases} S = R \oplus f_1(L) \\ T \oplus S = f_2(R) \end{cases}$
We will describe two attacks: one using S and one using $S \oplus T$.

First attack: on S

We choose two messages $[L_1, R_1]$ and $[L_2, R_2]$ such that $L_1 = L_2$ and we check if $S_1 \oplus S_2 = R_1 \oplus R_2$. With a Misty scheme this happens with probability one and with a random permutation with probability $\frac{1}{2^n}$. This is a CPA-1 with $m = 2$ and $O(1)$ complexity. This attack can be transformed into a KPA with $m = O(\sqrt{2^n})$ and $O(\sqrt{2^n})$ complexity: if $m = O(\sqrt{2^n})$ then by the birthday paradox with a good probability we can find two indices i, j such that $L_i = L_j$ and then we check if $S_i \oplus S_j = R_i \oplus R_j$.

Second attack: on $S \oplus T$

We choose two messages $[L_1, R_1]$ and $[L_2, R_2]$ such that $R_1 = R_2$ and we check if $S_1 \oplus S_2 = T_1 \oplus T_2$. The complexity is the same as for the first attack ($m = 2$ in CPA-1 and $m = O(\sqrt{2^n})$ in KPA).

4.3 3 rounds

Here $\begin{cases} S = X^2 = R \oplus f_1(L) \oplus f_2(R) \\ T \oplus S = f_2(X^1) \end{cases}$

First attack: 4 points on S

Here there is a CPA-1 with $m = 4$ messages. (This attack was already published in [15]. We give 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 3.3. Then we have seen (cf Section 3.3) that $X_1^2 \oplus X_2^2 \oplus X_3^2 \oplus X_4^2$, i.e. here $S_1 \oplus S_2 \oplus S_3 \oplus S_4 = 0$. With a Misty scheme this happens with probability one 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 $S_i \oplus S_j \oplus S_k \oplus S_l = 0$.

Second attack (for KPA only): 2 points on $S \oplus T$

In CPA-1 the previous attack is the best one. However in KPA we can succeed when $m \simeq 2^n$ by other ways: we can check if there exist i, j, $1 \le i \le m$, $1 \le j \le m$, $i \ne j$, such that $[T_i \oplus S_i = T_j \oplus S_j$ and $L_i = L_j]$ (or such that $[T_i \oplus S_i = T_j \oplus S_j$ and $R_i = R_j]$). This never occurs on a M_L^3 (since $T_i \oplus S_i = T_j \oplus S_j \Leftrightarrow f_3(X_i^1) = f_3(X_j^1) \Leftrightarrow X_i^1 = X_j^1$ and this implies that $L_i \ne L_j$ and $R_i \ne R_j$). However this will occur with a non negligible probability for a random permutation when $m^2 \ge 2^{2n}$. The KPA complexity is here in $O(2^n)$ (same KPA complexity as before).

Third attack (for KPA only): 2 points on S

Similarly, we can check if there exist i, j, $i \ne j$ such that $[R_i = R_j$ and $S_i = S_j]$ (or $[L_i = L_j$ and $S_i \oplus S_j = R_i \oplus R_j]$). This never occurs on a M_L^3 (since f_1 and f_2 are permutations and $L_i = L_j \Rightarrow R_i \ne R_j$). The KPA complexity is here in $O(2^n)$ as above.

Fourth Attack: CPCA-2 with $m = 3$

We give now a CPCA-2 with $m = 3$ messages. (This attack seems new. It is inspired from [8] and [15].)

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 $T_1 \oplus S_1 = T_2 \oplus S_2$. We obtain $[L_2, R_2]$. (Inverse query: this is a 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 $[S_3, T_3]$ (this is a 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 with a Misty scheme, $S_2 \oplus S_3 = R_1 \oplus R_2$ appear with probability one and with a probability about $\frac{1}{2^n}$ with a random permutation. This gives a CPCA-2 with $m = 3$ and $O(1)$ complexity.

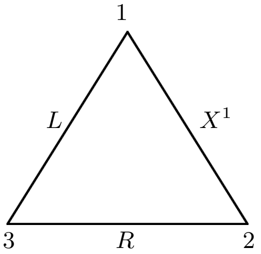

Fig. 4. The equalities in the CPCA-2 attack of M_L^3 with $m = 3$

4.4 4 rounds

Here $\begin{cases} S = X^2 = R \oplus f_1(L) \oplus f_2(R) \oplus f_3(R \oplus f_1(L)) \\ T \oplus S = f_4(X^2) = f_4(R \oplus f_1(L) \oplus f_2(R)) \end{cases}$

First attack: CPCA-2 with $m = 4$ (on $S \oplus T$)

Here there is a CPCA-2 with $m = 4$ messages. (Note: this attack was already published in [15]. We give it here for sake of completeness).

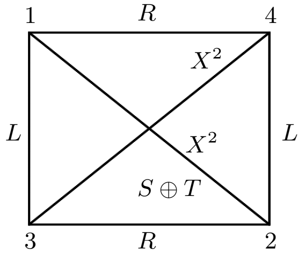

Fig. 5. The equalities in the CPCA-2 attack of M_L^4 with $m = 4$

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 $T_1 \oplus S_1 = T_2 \oplus S_2$. 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" of Section 3.3 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 one 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 $O(1)$ complexity.

Transformation in CPA-1

We can easily modify this CPCA-2 with $m = 4$ in a CPA-1 with $m = O(\sqrt{2^n})$ like this: we first look to find i, j, $i \neq j$ such that $T_i \oplus S_i = T_j \oplus S_j$ (this will occur when $m \geq O(\sqrt{2^n})$, and then we proceed as above on messages $[L_i, R_i]$, $[L_j, R_j]$, $[L_i, R_j]$, $[L_j, R_i]$.

Transformation in KPA

We need four pairwise distinct indices (i,j,k,l) such that $L_i = L_k$, $L_j = L_l$, $R_i = R_l$, $R_j = R_k$ and $T_i \oplus S_i = T_j \oplus S_j$. In KPA we will have this when $m^4 \geq 2^{5n}$, i.e. this is a KPA in $m \geq O(2^{\frac{5n}{4}})$. As we will see now, there exists better KPA for M_L^4.

Second attack: 2 point attack on $S \oplus T$ with KPA complexity in 2^n and CPA-1 in $\sqrt{2^n}$

This attack may be new. However since it is a simple impossible differential attack, it was not difficult to find. We generate m messages such that $\forall i,\ 1 \leq i \leq m,\ R_i = 0$ (or R_i constant). Then we look if there exist $i, j,\ i \neq j$ such that $S_i \oplus T_i = S_j \oplus T_j$. With a random permutation we will have such collisions when $m \geq O(\sqrt{2^n})$ (from the birthday paradox). However on a M_L^4 this is impossible since

$$\begin{cases} S_i \oplus T_i = S_j \oplus T_j \\ R_i = R_j \end{cases} \Leftrightarrow \begin{cases} f_4\left(R_i \oplus f_1(L_i) \oplus f_2(R_i)\right) = f_4(R_j \oplus f_1(L_j) \oplus f_2(R_j)) \\ R_i = R_j \end{cases}$$
$$\Leftrightarrow R_i = R_j \text{ and } L_i = L_j$$

since f_4 and f_1 are permutations and this is impossible if $i \neq j$. This CPA-1 in $O(\sqrt{2^n})$ 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.

Third attack: 4 point attack on S with CPA-1 complexity in $\sqrt{2^n}$

(Note: this attack may be new. However the previous attacks are better in CPCA-2 or in KPA, and in CPA-1 this attack has just the same complexity as the second attack above.) We choose 2 values for L: L_1 and L_2. We choose $\simeq \sqrt{2^n}$ random values for R_i. Therefore we have here $m \simeq 2\sqrt{2^n}$. The attack proceeds as follows: we count the number $\mathcal{N}$ of (i,j) such that: $S(L_1,R_i) \oplus S(L_2,R_i) = S(L_1,R_j) \oplus S(L_2,R_i)$. As we will see below, this number $\mathcal{N}$ is about twice for a M_L^4 compared with $\mathcal{N}$ for a random permutation. Therefore we can distinguish in $O(\sqrt{2^n})$ messages. The complexity of this algorithm is also in $O(\sqrt{2^n})$: for all i, $1 \leq i \leq \sqrt{2^n}$, we store the values $S(L_1,R_i) \oplus S(L_2,R_i)$ and we count the collisions. We have:

$$S(L_1,R_i) \oplus S(L_2,R_i) \oplus S(L_1,R_j) \oplus S(L_2,R_j) =$$

$$f_3(R_i \oplus f_1(L_1)) \oplus f_3(R_i \oplus f_1(L_2)) \oplus f_3(R_j \oplus f_1(L_1)) \oplus f_3(R_j \oplus f_1(L_2))$$

We see that for fixed i and j, this can occur with probability $\frac{1}{2^n}$, but also if $R_i \oplus f_1(L_1) = R_j \oplus f_1(L_2)$ and this has also probability $\frac{1}{2^n}$. Therefore the number $\mathcal{N}$ will be twice for a M_L^4 than for a random permutation, as claimed. (Remark: in KPA the complexity will be in $2^{\frac{5n}{4}}$ and the second attack is better in KPA.)

5 Attacks on 5 rounds

Here $\begin{cases} S = X^4 \\ T \oplus S = f_5(X^3) \end{cases}$

We will now see that on M_L^5 there are CPA-1 and KPA 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 are must be used. As far as we know, this result is new and the attacks that we will present for $d \geq 5$ are new.

This result gives the subtitle of this paper: -5 rounds is not enough for Misty- since usually when we build a pseudo-random permutation from $2n$ bits to $2n$ bits we want security greater than 2^{2n}.

Remark. It can be noticed that for Feistel schemes (cf [8])the result is similar: we need at least 6 rounds to avoid all the attacks with complexity $\ll 2^{2n}$ (since there are CPA-1 on ψ^5 with a complexity in $O(2^n)$, and KPA in $O(2^{\frac{3n}{2}})$). However the attacks on ψ^5 and M_L^5 are **very** different: the attacks on ψ^5 are 2 point attacks, but the attacks on M_L^5 are 4 point CPA-1 and KPA or Saturation CPA-1. Moreover, from the computations that we will do in Appendix D, we can prove that **all** the 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 they do not exist.

5.1 Four point Attacks

The attack on M_L^5, CPA-1 with complexity 2^n.
We choose only 2 values for L: L_1 and L_2. 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. The attack proceeds like this: we count the number $\mathcal{N}$ of (R_i, R_j) values, $R_i \neq R_j$ such that with the 4 messages

$$i : [L_1, R_i],\ j : [L_1, R_j],\ i' : [L_2, R_i],\ j' : [L_2, R_j]$$

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 values R_i we compute $[S_i, T_i] = M_L^5[L_1, R_i]$ and $[S_{i'}, T_{i'}] = M_L^5[L_2, R_i]$, we store i at the address $[S_i \oplus T_i, S_{i'} \oplus T_{i'}]$ and we count the collisions.)
As we will see, for a M_L^5, this number 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 the probability to have $\mathcal{N} \geq 1$ is not negligible, i.e. when $m \geq 2^n$. (We can also try another $[L_1, L_2]$. However, for each $[L_1, L_2]$ the probability of success of this attack is not negligible.)
Here $S \oplus T = f_5(X^3)$ 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 3.3, we know that

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

Notice that it is impossible to have $X_i^1 = X_j^1$ (since $L_i = L_j$) and it is also impossible to have $X_i^1 = X_{i'}^1$ (since $R_i = R_{i'}$). However we can have $X_i^1 = X_{j'}^1$ (with probability about $\frac{1}{2^n}$), and if this occurs from (1) we will also have also $X_j^1 = X_{i'}^1$ and from (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 $\begin{cases} X_i^3 = X_j^3 \\ X_{i'}^3 = X_{j'}^3 \end{cases}$: this 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), or 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). This $\mathcal{N}$ for M_L^5 is about twice as $\mathcal{N}$ for a random permutation, as claimed. 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 in KPA

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

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

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

We have implemented these attacks and this confirms our results. Details are given in Appendix E.

Remark. In [4], H. Gilbert and M. Minier proved CPCA-2 security for M_L^5 when $m \leq \sqrt{2^n}$.

5.2 Saturation Attack

We thank the anonymous referee of Crypto 2009 for pointing out this CPA-1. 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 $[R, L]$ 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 $O(2^n)$. However tis attack is unstable. This means that if we replace a few points of the function G such that $S = G(L)$ by truly random values, the attack fails. (For more details on stable and unstable attacks, see [11]).

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

6 rounds is the maximum number of rounds such that we know attacks in $O(2^{2n})$ computations in order to distinguish M_L^d (or M_L^d generators i.e. generators of M_L^d permutations) from random permutations of B_{2n} with an even signature. (This bound 2^{2n} is important since it is the total number of possible inputs $[L, R]$.)

First Attack: 2 point attack on $S \oplus T$

This attack will be based on the following theorem.

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^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 $p_1 = \frac{1}{2^n} - \frac{1}{2^{3n}} + O(\frac{1}{2^{4n}})$ and $p_2 = \frac{1}{2^n} - \frac{1}{2^{2n}} + O(\frac{1}{2^{3n}})$. Therefore p_1 is slightly larger than p_2: $p_1 - p_2 = \frac{1}{2^{2n}} + O(\frac{1}{2^{3n}})$.*

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 $S_1 \oplus T_1 = S_2 \oplus T_2$ (since we have 2^{2n} possibilities for S_1 and T_1, and then $2^n - 1$ possibilities for $S_2 \neq S_1$). So

$p_2 = \frac{2^{2n}(2^n-1)}{2^{4n}-2^{2n}} = \frac{2^n-1}{2^{2n}-1} = \frac{1}{2^n+1} = \frac{1}{2^n} - \frac{1}{2^{2n}} + O(\frac{1}{2^{3n}})$ as claimed.
For a M_L^6, we have

$$\begin{aligned} S_1 \oplus T_1 = S_2 \oplus T_2 &\Leftrightarrow f_6(X_1^4) = f_6(X_2^4) \\ &\Leftrightarrow X_1^4 = X_2^4 \\ &\Leftrightarrow R_1 \oplus f_1(L_1) \oplus f_2(R_1) \oplus f_3(R_1 \oplus f_1(L_1)) \oplus f_4(R_1 \oplus f_1(L_1) \oplus f_2(R_1)) \\ &= R_2 \oplus f_1(L_2) \oplus f_2(R_2) \oplus f_3(R_2 \oplus f_1(L_2)) \oplus f_4(R_2 \oplus f_1(L_2) \oplus f_2(R_2))) \\ &\Leftrightarrow f_1(L_1) \oplus f_3(R_1 \oplus f_1(L_1)) \oplus f_4(R_1 \oplus f_1(L_1) \oplus f_2(R_1)) \\ &= f_1(L_2) \oplus f_3(R_1 \oplus f_1(L_2)) \oplus f_4(R_1 \oplus f_1(L_2) \oplus f_2(R_1)) \quad (1) \end{aligned}$$

(since $R_1 = R_2$)
Let α be the probability that $f_1(L_1) \oplus f_3(R_1 \oplus f_1(L_1)) = f_1(L_2) \oplus f_3(R_1 \oplus f_1(L_2)) \quad (2)$. We have $\alpha = \frac{1}{2^n-1}$, because $L_1 \neq L_2$ and f_1 is a bijection, so $f_1(L_1) \oplus f_1(L_2) \neq 0$, and $f_3(R_1 \oplus f_1(L_2)) \oplus f_3(R_1 \oplus f_1(L_1))$ can take any value but 0 with probability $\frac{1}{2^n-1}$ (since f_3 is a bijection and $L_1 \neq L_2$). 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 $p_1 = \frac{2^n-2}{(2^n-1)^2} = \frac{1}{2^n} - \frac{1}{2^{3n}} + O(\frac{1}{2^{4n}})$ as claimed. □

Remark: in Appendix D, we will compute all the "h coefficient" related to deviations on "2 point" attacks. Theorem 2 can be seen as a property of the coefficient h_{10} with 6 rounds of Misty.

Application to the attack

We will count the number $\mathcal{N}$ of messages (i, j), $i < j$ such that $\begin{cases} R_i = R_j \\ S_i \oplus T_i = S_j \oplus T_j \end{cases}$
In KPA, for random permutations , we will have $E(\mathcal{N}) = \frac{m(m-1)}{2 \cdot 2^{2n}}$ where m is the number of messages. The standard deviation is $\sigma(\mathcal{N}) = O(\sqrt{E(\mathcal{N})}) = O(\frac{m}{2^n})$. This can be proved by using the "covariance formula":

$$V(\sum_i X_i) = \sum_i V(X_i) + \sum_{i \neq j} Cov(X_i, X_j) \quad (\#)$$

For a M_L^6, we will have $E(\mathcal{N}) \simeq \frac{m(m-1)}{2 \cdot 2^{2n}}\left(1+\frac{1}{2^n}\right)$ (cf Theorem 2 above). 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 attack is in $O(2^{2n})$ in KPA (same complexity in CPA-1 and CPCA-2).
Remark. If we attack a single permutation M_L^6, then $m \leq 2^{2n}$ since 2^{2n} is the total number of possible messages $[L, R] \in I_{2n}$. Then when $m \simeq 2^{2n}$, this attack has a fixed probability of success not negligible (i.e. not near 0). If we want to increase this probability for example in order to have a probability of success as near to 1 as wanted, we can assume that we attack M_L^6 generators, with more than one permutation.

Second attack: 4 points on $S \oplus T$

We describe the attack in KPA (the complexity will be the same in CPA). The attack proceeds as follows: we count the number $\mathcal{N}$ of 4-uples of pairwise distinct indices (i, j, k, l) such that

$$(\star) \begin{cases} L_i = L_j \\ L_k = L_l (\neq L_i) \\ R_i = R_k \\ R_j = R_l (\neq R_i) \\ S_i \oplus T_i = S_k \oplus T_k \\ S_j \oplus T_j = S_l \oplus T_l \end{cases}$$

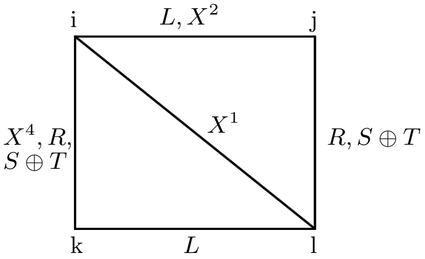

Fig. 6. The structure of the 4 point attack on M_L^6

We will see that there is tiny deviation (in $\frac{1}{2^n}$) of $E(\mathcal{N})$ for a M_L^6 compared from a truly permutation, and we will see how to use this deviation in $O(2^{2n})$ complexity. For a random permutation in KPA, we have $E(\mathcal{N}) \simeq \frac{m^4}{2^{6n}}$ with a standard deviation $\sigma(\mathcal{N}) = O(\sqrt{E(\mathcal{N})}) = O(\frac{m^2}{2^{3n}})$.
Remark. The proof that the standard deviation is here again in the square root of the mean value can be obtained from the covariance formula (#). We give here just the main idea of the proof. Essentially, this comes from the fact that the terms of $Cov_{i\neq j}(X_i, X_j)$ will have a small contribution in the computation of $V(\sum_i X_i)$ since the variables will be near independent. This is because when we have a structure of 4 messages (i, j, k, l) that satisfy $(\star)$ it is little help to find now more easily another (i', j', k', l') that satisfy $(\star)$ because l is fixed when (i, j, k) are fixed (from $L_l = L_k$ and $R_l = R_j$). So, if we remove one point, for example j, we have to remove another point for example l. Now from i, j, with 2 equations (1 in R, 1 in $S \oplus T$), we need to find another j, l with 4 equations (1 in R, 2 in L, 1 in $S \oplus T$). It is therefore as easy to start again from a new i, j, k, l than to keep i and j. ($\frac{m^4}{4^{6n}}$ is larger than $\frac{m^2}{2^{4n}}$ since here $m \geq 2^n$).
For a M_L^6 we have $S \oplus T = f_6(X^4)$ and f_6 is a bijection. So

$$\begin{cases} S_i \oplus T_i = S_k \oplus T_k \\ S_j \oplus T_j = S_l \oplus T_l \end{cases} \Leftrightarrow \begin{cases} X_i^4 = X_k^4 \\ X_j^4 = X_l^4 \end{cases}$$

Now from the "4 point property" of Section 3.3, we know that if $L_i = L_j$, $L_k = L_l$, $R_i = R_k$, $R_j = R_l$, we will have:
$X_i^1 \oplus X_j^1 \oplus X_k^1 \oplus X_l^1 = 0$
$X_i^2 \oplus X_j^2 \oplus X_k^2 \oplus X_l^2 = 0$
$X_i^4 \oplus X_j^4 \oplus X_k^4 \oplus X_l^4 = f_3(X_i^1) \oplus f_3(X_j^1) \oplus f_3(X_k^1) \oplus f_3(X_l^1) \oplus f_4(X_i^2) \oplus f_4(X_j^2) \oplus f_4(X_k^2) \oplus f_4(X_l^2)$
So $(\star)$ is also implied by

$$(\star\star) \begin{cases} L_i = L_j \\ L_k = L_l (\neq L_i) \\ R_i = R_k \\ R_j = R_l (\neq R_i) \\ X_i^1 = X_l^1 \\ X_i^2 = X_j^2 \\ X_i^4 = X_k^4 \end{cases}$$

Figure 6 illustrates $(\star)$ and $(\star\star)$. So $(\star)$ can appear when $(\star\star)$ is not satisfied with about the same probability as before, or when $(\star\star)$ is satisfied. We see that for a M_L^6 there will be about

$\frac{m^4}{2^{7n}}$ more solutions satisfying $(\star)$ than for a random permutation. Then, the attack will succeed if $\frac{m^4}{2^{7n}} \geq \sigma(\mathcal{N}) = O(\frac{m^2}{2^{3n}})$, i.e. when $m \geq O(2^{2n})$ as claimed. (This is the same complexity as the first attack).

Third Attack

This attack was also suggested by the anonymous referee of Crypto 2009. Here we count the total number of pairs $([L_1, R_1]; [L_2, R_2])$ such that

$$(\#) \begin{cases} R_1 & = R_2 \\ S_1 & \oplus T_1 = S_2 \oplus T_2 \end{cases}$$

and we check if this number is even. We now show that this is always the case with a Misty scheme. More precisely, we prove that we we have a pair satisfying $(\#)$, we can construct another pair which also satisfies the same conditions. We proceed as follows. Suppose that we have $([L_1, R_1]; [L_2, R_2])$ verifying $(\#)$. After 2 rounds, the input $[L_1, R_1]$ produces $[X_1^1, X_1^2]$ and the input $[L_2, R_2]$ produces $[X_2^1, X_2^2]$. Moreover we have the following relations:

$$\begin{array}{ll} X_1^1 = R_1 \oplus f_1(L_1) & X_2^1 = R_2 \oplus f_1(L_2) \\ X_1^2 = X_1^1 \oplus f_2(R_1) & X_2^2 = X_2^1 \oplus f_2(R_2) \end{array}$$

Since f_2 is a permutation we have $R_1 = R_2 \Leftrightarrow X_1^1 \oplus X_2^1 \oplus X_1^2 \oplus X_2^2 = 0$. Let $[L', R']$ be the message which gives $[X_2^1, X_1^2]$ after 2 rounds. Similarly, $[L'', R'']$ is the message which gives $[X_1^1, X_2^2]$ after 2 rounds. After 6 rounds, the output corresponding to the input $[L', R']$ is denoted by $[S', T']$ and the output corresponding to the input $[L'', R'']$ is denoted by $[S'', T'']$. Since $R' = f_2^{-1}(X_2^1 \oplus X_1^2)$, $R'' = f_2^{-1}(X_1^1 \oplus X_2^2)$ and $X_1^1 \oplus X_2^1 \oplus X_1^2 \oplus X_2^2 = 0$, we obtain $R' = R''$. Since $R_1 = R_2$, we have: $S_1 \oplus T_1 = S_2 \oplus T_2 \Leftrightarrow f_1(L_1) \oplus f_3(X_1^1) \oplus f_4(X_1^2) = f_1(L_2) \oplus f_3(X_2^1) \oplus f_4(X_2^2)$.
In order to have $S' \oplus T' = S'' \oplus T''$, we have to show that $f_1(L') \oplus f_3(X_2^1) \oplus f_4(X_1^2) = f_1(L'') \oplus f_3(X_1^1) \oplus f_4(X_2^2)$. But since $f_1(L') = R_2 \oplus f_1(L_2) \oplus R'$, $f_1(L'') = R_1 \oplus f_1(L_1) \oplus R''$, $R_1 = R_3$ and $R' = R''$, this is equivalent to show $S_1 \oplus T_1 = S_2 \oplus T_2$. Therefore $([L', R']; [L'', R''])$ satisfy $(\#)$. This proves that with a Misty schemes, the number such pairs is always even. This gives an attack with complexity $O(2^{2n})$. However this attack is unstable.

7 Conclusion

Our final results have been summarized in Appendix G. These results were not obvious before making specific and precise analysis of Misty schemes, since for Misty schemes we have efficient 2 point and 4 point attacks (as previously noticed), and since it was not obvious that the h coefficient used in the attacks decrease in about $\frac{1}{2^n}$ each time we add two more rounds for M_L^d as for ψ^d. If we compare our final results for M_L^d with the best known generic attacks on classical Feistel schemes ψ^d (cf Table 2 of Appendix F and Table 3 of Appendix G), we see that the final complexities are often similar, with however often a change of one round , sometimes in one direction, and sometimes in the other direction. For example, M^3 is less secure than ψ^3 in CPA-1, and M^4 is less secure than ψ^4 in CPCA-2, but the best known attacks on M^7 are less efficient than for ψ^7 generators.

There are still many open problem on generic Misty schemes. For example, there are many gaps between the proof of security in $O(\sqrt{2^n})$ (birthday bound) obtained in [4], [14], [16], [17] and the best known attacks. For a security less than or equal to 2^n, generalizations of what was done on ψ^k (cf [9], [7]) are probably possible, but for a security strictly greater than 2^n no real techniques of proofs are known (information bound).

References

1. Specification of the 3GPP Confidentiality and Integrity Algorithm KASUMI. Document available on http://www.etsi.org/.
2. 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.
3. Don Coppersmith. Luby-Rackoff: Four Rounds is not enough. Technical report, Technical Report RC20674, IBM Research Report, December 1996.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. Jacques Patarin. Generic Attacks for the Xor of k Random Permutations. *Cryptology ePrint archive: 2008/009: Listing for 2008*, 2008.
12. 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.
13. 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.
14. 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.
15. 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.
16. M. Sugita. Pseudorandomness of a Block Cipher MISTY. Technical report, Technical Report of IEIECE, ISEC 96-9.
17. M. Sugita. Pseudorandomness of a Block Cipher with Recursive Strictures. Technical report, Technical Report of IEIECE, ISEC 97-9.
18. 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.

Appendices

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 μ permutations of the generator with $\mu > 1$.

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

Theorem 3 *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 2), or by using the ϵ_{10} values that we compute in Appendix D. □

Application for the attack
We will count the number $\mathcal{N}$ of messages i, j, $i < j$ that belong to the same permutation and such that $\begin{cases} R_i = R_j \\ S_i \oplus T_i = S_j \oplus T_j \end{cases}$
In KPA, for μ random permutations with m messages per permutation we have: $E(\mathcal{N}) = \mu \frac{m(m-1)}{2 \cdot 2^{2n}}$ and the standard deviation is $\sigma(\mathcal{N}) = O(\frac{m\sqrt{\mu}}{2^n})$. (The fact that $\sigma(\mathcal{N}) = \sqrt{E(\mathcal{N})}$ can easily be proved from the "covariance formula" (#)) of Section 6. For a M_L^d, d even, $d \geq 6$, we will have $E(\mathcal{N}) \simeq \mu \frac{m(m-1)}{2 \cdot 2^{2n}} \Big(1 + \frac{(-1)^{\frac{d}{2}+1}}{(2^n)^{\frac{d}{2}-2}}\Big)$ (cf Theorem 3 above). Therefore we can distinguish when

$$\frac{\mu m^2}{2^{n\frac{d}{2}}} \geq \sigma(\mathcal{N}) = 0(\frac{m\sqrt{\mu}}{2^n})$$

i.e. $\sqrt{\mu} m \geq 2^{n(\frac{d}{2}-1)}$, or $\mu m^2 \geq 2^{n(d-2)}$. With $m \simeq 2^{2n}$, this gives $\mu \geq 2^{n(d-6)}$ and a complexity $\mu \cdot 2^{2n} = 2^{n(d-4)}$. 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 the composition 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 $\begin{cases} R_i = R_j \\ S_i \oplus T_i = S_j \oplus T_j \end{cases}$
(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 on $S \oplus T$ is based on the coefficient ϵ_{10} that we will compute in Appendix D. 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 $\begin{cases} L_i = L_j \\ S_i \oplus T_i = S_j \oplus T_j \end{cases}$ This 2 point attack on $S \oplus T$ is based on the coefficient ϵ_{11} that we will compute in Appendix D. The complexity of these attacks $O(2^{n(d-3)})$ can easily be proved by induction (this is a simple generalization of the 2 point attack given for 6 rounds), or by using the evaluation for the coefficients ϵ_{10} and ϵ_{11} that we compute in Appendix D.

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 2 points attacks. For $d \geq 8$ the complexity will be worse. In fact, when $d \geq 6$ the best known 4 point attacks have complexity in $O(2^{(2d-10)n})$ 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 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 for 2 points attacks).

B Signature of Misty schemes

Theorem 4 *When $n \geq 2$, Misty schemes M_L^d and M_R^d always have an even signature.*

Proof: We have seen at Section 3.1 that:

$$M_L^1 = \mu \circ \Lambda \text{ and } M_R^1 = \mu^{-1} \circ \Lambda,$$

with

$$\forall [L,R] \in I_{2n}, \Lambda[L,R] \overset{\text{def}}{=} [f_1(L), R]$$
$$\forall [L,R] \in I_{2n}, \mu[L,R] \overset{\text{def}}{=} [R, L \oplus R].$$

Let us denote by τ the permutation of B_{2n} such that

$$\forall [L,R] \in I_{2n}, \tau([L,R]) = [L \oplus R, R],$$

and by σ the permutation of B_{2n} such that

$$\forall [L,R] \in I_{2n}, \sigma([L,R]) = [R, L].$$

Then, $\mu = \sigma \circ \tau$, and $\tau^2 = Id$.

Signature of σ

All the cycles of σ have 1 or 2 elements since $\sigma \circ \sigma = Id$. We have 2^n cycles with one element since $\sigma([L,R]) = [L,R]$ if and only if $L = R$ (and a cycle with one element has an even signature). Thus we have $\frac{2^{2n}-2^n}{2}$ cycles with two elements. When $n \geq 2$, this number is even. Therefore, σ has an even signature if $n \geq 2$.

Signature of τ

Similarly, all the cycles of τ have one or two elements since $\tau \circ \tau = Id$.

We have 2^n cycles with one element since this is the number of $[L,R]$ such that $L = L \oplus R$, i.e. such that $R = 0$.

So we have $\frac{2^{2n}-2^n}{2}$ cycles with two elements and this is even if $n \geq 2$. Therefore τ has even signature if $n \geq 2$.

Signature of μ

Since $\mu = \sigma \circ \tau$, from the results on σ and τ we see that μ has an even signature if $n \geq 2$.

Signature of Λ

Let k be the number of cycles of the permutation f_1 with an even number of elements. Then $signature(f_1) = (-1)^k$. The number of cycles of Λ with an even number of elements is exactly $2^n \cdot k$, since we have 2^n possible values for R.

Then $signature(\Lambda) = (-1)^{2^n k}$, thus the signature of Λ is always even, $\forall n \geq 1$.

Signature of M_L^1 and M_R^1

Since $M_L^1 = \mu \circ \Lambda$ and $M_R^1 = \mu^{-1} \circ \Lambda$, from the results on μ and Λ, we see that M_L^1 and M_R^1 have an even signature if $n \geq 2$.

Signature of M_L^d and M_R^d

Since M_L^d is a composition of d permutations M_L^1, we see that Misty schemes M_L^d with any number d of rounds have always an even signature when $n \geq 2$. (Similarly for M_R^d). □

Theorem 5 *Let f be a permutation of B_{2n}. Then by using $\mathcal{O}(2^{2n})$ computations on the 2^{2n} input/output values of f, we can compute a signature of f.*

Proof: Just compute all the cycles c_i of f, $f = \prod_{i=1}^{\alpha} c_i$ and use the formula:

$$\text{signature}(f) = \prod_{i=1}^{\alpha} (-1)^{\text{length}(c_i)+1}.$$

□

Theorem 6 *Let G be a Misty generator. Then it is possible to distinguish G from a generator of truly random permutations of B_{2n} after $\mathcal{O}(2^{2n})$ computations on $\mathcal{O}(2^{2n})$ input/output values.*

Proof: This is a direct consequence of the Theorems 4 and 5. □

Remark: In table 3 of Appendix G we present the results to distinguish M_L^d from random permutations with an even signature, since for random permutations with an odd signature, the complexity is in $\mathcal{O}(2^{2n})$ if we have access to exactly all the 2^{2n} possible inputs and corresponding outputs. (If only two inputs/outputs are missing the signature cannot be computed. If only one is missing, it is not really missing: since we have a permutation, its output is the only output value not yet obtained).

C Brute force attacks on generic Misty schemes

A possible attack is the exhaustive search on the d round internal permutations $f_1, \ldots, f_d$ from B_n that have been used in th Misty construction.

We have $\mid B_n \mid^d = (2^n)!^d \simeq (2^{n \cdot 2^n} e^{-2^n} \sqrt{2\pi 2^n})^d$ (Stirling Formula). This value is between $2^{n \cdot 2^n \cdot d}$ and $2^{(n-2) \cdot 2^n \cdot d}$. If we have access to m input/output pairs $[L, R], [S, T]$, we will divide the number of possible $f_1, \ldots, f_d$ by about 2^{nm}. Therefore, we will find the solution $(f_1, \ldots, f_d)$ when nm is greater or equal to about $n \cdot 2^n \cdot d$, i.e. when m is greater or equal to about $2^n \cdot d$.

We see that for a fixed number of rounds d, when $m \geq \mathcal{O}(2^n)$ we will be able to distinguish M_L^d generators from truly random permutation generators if we have unbounded computing power but are limited to m input/output queries. We say that $\mathcal{O}(2^n)$ is the *information bound*.

Remark: Exhaustive search has a complexity between $2^{n \cdot 2^n \cdot d}$ and $2^{(n-2) \cdot 2^n \cdot d}$. In a version "in the middle" of this attack, it will be the square root of this complexity i.e. about $2^{\frac{n \cdot 2^n \cdot d}{2}}$, which is still completely impracticable.

D Computation of the "h coefficients"

All the attacks that we have presented in this paper can be (and has been) explained directly, without the results of this appendix D. In this Appendix D, we will prove that no better “2 point attacks” can exist. For this, we will proceed in a systematic analysis of all the probability deviation in the inputs/outputs from M_L^d compared with truly random permutation of B_{2n} when we analyze only two 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 can find like this all the best "two point attacks", i.e. attacks that can use a large number m of messages but that only use correlations on pairs of these messages (such as differential attack 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:

$$\begin{cases} M_L^d(f_1, \ldots, f_d)([L_1, R_1]) = [S_1, T_1] \\ M_L^d(f_1, \ldots, f_d)([L_2, R_2]) = [S_2, T_2] \end{cases}$$

The mean value for H is $\frac{|B_n|^d}{2^{2n}(2^{2n}-1)}$ since we have $2^{2n}(2^{2n}-1)$ values for (S_1, T_1, S_2, T_2) such that $[S_1, T_1] \neq [S_2, T_2]$.

- We will denote $h = \frac{H \cdot 2^{4n}}{|B_n|^k}$.
- We will denote by $\overset{\circ}{1}$ the mean value of h: $\overset{\circ}{1}= \frac{1}{1-\frac{1}{2^{2n}}} = \frac{2^{2n}}{2^{2n}-1}$.
- We will denote $\epsilon = h - \overset{\circ}{1}$.

The aim of this Appendix D is to evaluate the different values H, or equivalently the different values h or ϵ.

D.1 One round

For M_L^1, we have:

$$\begin{cases} S = R \\ T = R \oplus f_1(L) \end{cases}$$

Let (C) be the following conditions:

$$(C) \begin{cases} S_1 = R_1 \\ S_2 = R_2 \\ L_1 = L_2 \iff T_1 \oplus R_1 = T_2 \oplus R_2 \end{cases}$$

When (C) is not satisfied, $H = 0$. When (C) is satisfied, $H = \frac{|B_n|}{2^n(2^n-1)}$, if $L_1 \neq L_2$, and $H = \frac{|B_n|}{2^n}$, if $L_1 = L_2$.

D.2 More rounds

For two rounds or more, we will distinguish between these 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 $[S_1, T_1] \neq [S_2, T_2]$).

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

We will denote by h_i^d, $1 \leq i \leq 13$, or more 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).

2 rounds For 2 rounds, we have

$$\begin{cases} S = R \oplus f_1(L) \\ T \oplus S = f_2(R). \end{cases}$$

We can easily compute the h_i values and the $\epsilon_i = h_i - \overset{\circ}{1}$ values. We get for 2 rounds:

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

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:

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

$$(D2)\begin{cases} h'_6 = \frac{1}{2^n-1}[(2^n-2)h_6 + h_7] \\ h'_7 = h_8 \\ h'_8 = h_6 \end{cases}$$

$$(D3)\begin{cases} h'_9 = \frac{1}{2^n-1}[(2^n-3)h_9 + h_{10} + h_{12}] \\ h'_{10} = \frac{1}{2^n-1}[(2^n-2)h_{11} + h_{13}] \\ h'_{11} = h_9 \\ h'_{12} = \frac{1}{2^n-1}[(2^n-2)h_9 + h_{10}] \\ h'_{13} = h_{12} \end{cases}$$

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,

$$\sum_{L_1,R_1,L_2,R_2} H(L,R,S,T) =\mid B_n \mid^d \qquad (D4)$$

since each output comes from exactly one input. Similarly, for all L_1, R_1, L_2, R_2,

$$\sum_{S_1,T_1,S_2,T_2} H(L,R,S,T) =\mid B_n \mid^d \qquad (D5)$$

since each input gives exactly one output.

With $h = \frac{H \cdot 2^{4n}}{|B_n|^d}$ we obtain:

For all S, T: $\sum\limits_{L,R} h(L,R,S,T) = 2^{4n} \qquad (D6)$

For all L, R: $\sum\limits_{S,T} h(L,R,S,T) = 2^{4n} \qquad (D7)$

When we specify S, T, $(D6)$ gives 3 equations on the h_i values:

- When $S_1 \neq S_2$ and $S_1 \oplus S_2 \neq T_1 \oplus T_2$:

$$(2^n-1)(2^n-2)h_1 + (2^n-1)h_2 + (2^n-2)h_3 + (2^n-1)h_4 + h_5 = 2^{2n} \qquad (D8)$$

- When $S_1 = S_2$ and $S_1 \oplus S_2 \neq T_1 \oplus T_2$:

$$(2^n-1)h_6 + h_7 + h_8 = \frac{2^{2n}}{2^n-1} \qquad (D9)$$

- When $S_1 \oplus S_2 = T_1 \oplus T_2$ and $S_1 \neq S_2$:

$$(2^n-1)(2^n-2)h_9 + (2^n-1)h_{10} + (2^n-2)h_{11} + (2^n-1)h_{12} + h_{13} = 2^{2n} \qquad (D10)$$

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

- When $L_1 \neq L_2$ and $R_1 \neq R_2$:

$$(2^n-1)(2^n-2)h_1 + (2^n-1)h_4 + (2^n-1)h_6 + (2^n-2)h_9 + h_{12} = 2^{2n} \qquad (D11)$$

- When $L_1 = L_2$ and $R_1 \neq R_2$:

$$(2^n-1)(2^n-2)h_3 + (2^n-1)h_5 + (2^n-1)h_8 + (2^n-2)h_{11} + h_{13} = 2^{2n} \qquad (D12)$$

- When $R_1 = R_2$ and $L_1 \neq L_2$:

$$(2^n-1)h_2 + h_7 + h_{10} = \frac{2^{2n}}{2^n-1} \qquad (D13)$$

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:

$$(E1)\begin{cases} \epsilon_1' = \frac{(2^n-3)\epsilon_1}{2^n-1} + \frac{\epsilon_2}{2^n-1} + \frac{\epsilon_4}{2^n-1} \\ \epsilon_2' = (-2^n+2)\epsilon_1 - \epsilon_2 - \epsilon_4 \\ \epsilon_4' = \frac{(2^n-2)\epsilon_1}{2^n-1} + \frac{\epsilon_2}{2^n-1} \end{cases}$$
$$(E2)\begin{cases} \epsilon_3' = \epsilon_1 \\ \epsilon_5' = \epsilon_4 \end{cases}$$

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: $\epsilon_1' - \epsilon_4' = \frac{-(\epsilon_1-\epsilon_4)}{2^n-1}$. Therefore, by induction:

$$(\epsilon_1 - \epsilon_4) = \frac{(-1)^k \cdot 2^{2n}}{(2^n-1)^k} \qquad (E3)$$

Moreover, if we denote $\epsilon_i'' = \epsilon_i^{d+2}$, $\epsilon_i' = \epsilon_i^{d+1}$, $\epsilon_i = \epsilon_i^d$, we have:

$$(E4)\begin{cases} \epsilon_1'' = \frac{-\epsilon_1 - 2\epsilon_1' + \epsilon_4'}{2^n-1} \\ \epsilon_2'' = \epsilon_1 + \epsilon_1' + \epsilon_4' \\ \epsilon_4'' = \frac{-\epsilon_1 - \epsilon_1'}{2^n-1} \end{cases}$$
$$(E5)\begin{cases} \epsilon_3' = \epsilon_1 \\ \epsilon_5' = \epsilon_4 \end{cases}$$

These equations show that the ϵ_i values 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, $\epsilon_i = h_i - \overset{\circ}{1}$,

$$(E6)\begin{cases} \epsilon_6' = \frac{-\epsilon_6 - \epsilon_8}{2^n-1} \\ \epsilon_8' = \epsilon_6 \end{cases}$$
$$(E7)\ \epsilon_7' = \epsilon_8$$

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:

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

$$(E9)\begin{cases} \epsilon'_{11} = \epsilon_9 \\ \epsilon_{13} = \epsilon_{12} \end{cases}$$

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:

$$(E10)\begin{cases} \epsilon'_9 = \frac{2^n-2}{2^n-1}\epsilon_9 + \frac{\epsilon_{10}}{2^n-1} \\ \epsilon'_{10} = (-2^n+1)\epsilon_9 - \epsilon_{10} = \epsilon_{11} \end{cases}$$

$$(E11)\begin{cases} \epsilon'_{11} = \epsilon_9 \\ \epsilon'_{13} = \epsilon_9 \\ \epsilon_{12} = \epsilon_9 \end{cases}$$

If we denote $\epsilon''_i = \epsilon_i^{d+2}$, we have:

$$\epsilon''_{10} = \frac{-\epsilon_{10} - \epsilon'_{10}}{2^n - 1} = \epsilon_9 \qquad (E12)$$

These equations $(E11), (E12)$, show that $\epsilon_9, \epsilon_{10}, \epsilon_{11}, \epsilon_{12}, \epsilon_{13}$ will decrease by a factor 2^n every two rounds.

Example of values

We present here all the values ϵ_i for 3 rounds and 4 rounds. With the formulas above, we can compute all the values ϵ_i and evaluate ϵ_i for any round.

3 rounds

$$\begin{array}{lcc} \epsilon_1 = & \frac{-4\cdot 2^{2n}}{(2^n-1)^3(2^n+1)} & \simeq \frac{-4}{2^{2n}} \\ \epsilon_2 = & \frac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} & \simeq \frac{2}{2^n} \\ \epsilon_3 = & \frac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} & \simeq \frac{2}{2^n} \\ \epsilon_4 = & \frac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} & \simeq \frac{1}{2^n} \\ \epsilon_5 = - \overset{\circ}{1} = & \frac{-2^{2n}}{(2^n-1)(2^n+1)} & \simeq -1 \\ \epsilon_6 = & \frac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} & \simeq \frac{1}{2^n} \\ \epsilon_7 = - \overset{\circ}{1} = & \frac{-2^{2n}}{(2^n+1)(2^n-1)} & \simeq -1 \\ \epsilon_8 = & \frac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} & \simeq \frac{2}{2^n} \\ \epsilon_9 = & \frac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} & \simeq \frac{2}{2^n} \\ \epsilon_{10} = - \overset{\circ}{1} = & \frac{-2^{2n}}{(2^n-1)(2^n+1)} & \simeq -1 \\ \epsilon_{11} = & - \overset{\circ}{1} & \simeq -1 \\ \epsilon_{12} = & \frac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} & \simeq \frac{2}{2^n} \\ \epsilon_{13} = & - \overset{\circ}{1} & \simeq -1 \end{array}$$

4 rounds

$$\begin{aligned}
\epsilon_1 &= \tfrac{-2^{2n}(2^n-7)}{(2^n-1)^4(2^n+1)} \simeq \tfrac{-1}{2^{2n}}\\
\epsilon_2 &= \tfrac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} \simeq \tfrac{1}{2^{n}}\\
\epsilon_3 &= \tfrac{-4\cdot 2^{2n}}{(2^n-1)^3(2^n+1)} \simeq \tfrac{-4}{2^{2n}}\\
\epsilon_4 &= \tfrac{-2\cdot 2^{2n}(2^n-3)}{(2^n-1)^4(2^n+1)} \simeq \tfrac{-2}{2^{2n}}\\
\epsilon_5 &= \tfrac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} \simeq \tfrac{1}{2^{n}}\\
\epsilon_6 &= \tfrac{-2^{2n}(3\cdot 2^n-5)}{(2^n-1)^4(2^n+1)} \simeq \tfrac{-3}{2^{2n}}\\
\epsilon_7 &= \tfrac{2\cdot 2^{2n}}{(2^n+1)(2^n-1)^2} \simeq \tfrac{2}{2^{n}}\\
\epsilon_8 &= \tfrac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} \simeq \tfrac{1}{2^{n}}\\
\epsilon_9 &= \tfrac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} \simeq \tfrac{1}{2^{n}}\\
\epsilon_{10} &= -\overset{\circ}{1} \simeq -1\\
\epsilon_{11} &= \tfrac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} \simeq \tfrac{2}{2^{n}}\\
\epsilon_{12} &= \epsilon_9 \simeq \tfrac{2}{2^{n}}\\
\epsilon_{13} &= \epsilon_{11} \simeq \tfrac{2}{2^{n}}
\end{aligned}$$

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:

$$\begin{aligned}
\lambda &= \tfrac{1}{2(2^n-1)}(-1+i\sqrt{4\cdot 2^n-5})\\
\beta &= \tfrac{2^{2n}}{(2^n-1)(2^n+1)}(2^n+\tfrac{i(2^n-2)}{\sqrt{4\cdot 2^n-5}}).
\end{aligned}$$

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 $\mid \lambda \mid = \frac{1}{\sqrt{2^n-1}}$, 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:

$$\begin{aligned}
\epsilon_1^d &= \tfrac{(-1)^d\cdot 2^{2n}}{(2^n-1)^{d+1}} + Re(\beta\cdot\lambda^{d+2}) & &\\
\epsilon_2^d &= Re(\lambda^d\beta) &= &\ \epsilon_9^d\\
\epsilon_3^d &= \tfrac{(-1)^{d+1}\cdot 2^{2n}}{(2^n-1)^{d}} + Re(\beta\cdot\lambda^{d+1}) &= &\ \epsilon_1^{d-1}\\
\epsilon_4^d &= \tfrac{(-1)^{d+1}\cdot 2^{2n}(2^n-2)}{(2^n-1)^{d+1}} + Re(\beta\cdot\lambda^{d+2}) &= &\ \epsilon_1^d + \tfrac{(-1)^{d+1}\cdot 2^{2n}}{(2^n-1)^d}\\
\epsilon_5^d &= \tfrac{(-1)^{d}\cdot 2^{2n}(2^n-2)}{(2^n-1)^{d}} + Re(\beta\cdot\lambda^{d+1}) &= &\ \epsilon_4^{d-1}\\
\epsilon_5^d &= \tfrac{(-1)^{d}\cdot 2^{2n}(2^n-2)}{(2^n-1)^{d}} + Re(\beta\cdot\lambda^{d+1}) &= &\ \epsilon_4^{d-1}\\
\epsilon_6^d &= Re(\lambda^{d+1}\beta) &= &\ \epsilon_9^{d+1}\\
\epsilon_7^d &= Re(\lambda^{d-1}\beta)) &= &\ \epsilon_9^{d-1}\\
\epsilon_8^d &= Re(\lambda^d\beta) &= &\ \epsilon_9^d\\
\epsilon_9^d &= Re(\lambda^d\beta) & &\\
\epsilon_{10}^d &= Re(\lambda^{d-2}\beta) &= &\ \epsilon_9^{d-2}\\
\epsilon_{11}^d &= Re(\lambda^{d-1}\beta) &= &\ \epsilon_9^{d-1}\\
\epsilon_{12}^d &= Re(\lambda^d\beta) &= &\ \epsilon_9^d\\
\epsilon_{13}^d &= Re(\lambda^{d-1}\beta) &= &\ \epsilon_9^{d-1}
\end{aligned}$$

These expressions can be checked with:

$$\begin{aligned}
&\lambda\beta = \tfrac{2^{2n}}{(2^n-1)(2^n+1)}(-1+\tfrac{i}{\sqrt{4\cdot 2^n-5}}(2\cdot 2^n-1))\\
&\lambda^2\beta = \tfrac{2^{2n}}{(2^n-1)(2^n+1)}(-1-\tfrac{3i}{\sqrt{4\cdot 2^n-5}})\\
&\lambda^3\beta = \tfrac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)}(1+\tfrac{i(-2^n+2)}{\sqrt{4\cdot 2^n-5}})\\
&\lambda^4\beta = \tfrac{2^{2n}}{(2^n-1)^3(2^n+1)}(2^n-3+\tfrac{i(5\cdot 2^n-7)}{\sqrt{4\cdot 2^n-5}})\\
&\ldots
\end{aligned}$$

Examples of applications

Let us try to attack M_L^6 with ϵ_{10}. First we have to evaluate ϵ_{10} for 6 rounds. From $(E12)$ we know that $\epsilon_{10}^6 = \epsilon_9^4$. Thus, $\epsilon_{10}^6 = \frac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} \simeq \frac{1}{2^n}$. (Another possibility is to use the formula $\epsilon_{10}^6 = Re(\lambda^4\beta) \simeq \frac{1}{2^n}$).

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 of the order of $\frac{m^2}{2^{2n}}$ messages in this case 10, we will have about $\frac{m^2}{2^{2n}}(1+\frac{1}{2^n})$ such messages.

Here again, the standard deviation is about the square root of the mean value in two points attacks (this can be proved from the covariance formula # seen in Section 6), hence here $\sigma = \mathcal{O}(\frac{m}{2^n})$, and we will distinguish when $\frac{m^2}{2^{2n}} \cdot \frac{1}{2^n} \geq \frac{m}{2^n}$, i.e. when $m \geq \mathcal{O}(2^{2n})$. This is exactly the two point attacks described in Section 6.

Remark: from the value ϵ_{10}^6 we can also easily recompute the probabilities p_1 and p_2 of Section 6.

$p_2 = \frac{2^{2n}(2^n-1)}{2^{4n}} \overset{\circ}{1}$, 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 $p_1 = \frac{2^n-2}{(2^n-1)^2}$.

E Experimental results

We have implemented our new 4-point attack on 5-round L-schemes described in section 5. 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 verifying $L_i = L_j$, $L_k = L_l$, $R_i = R_k$, $R_j = R_l$.

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

Table 1 below gives the number of collisions of type $S_i \oplus T_i = S_j \oplus T_j$ and $S_k \oplus T_k = S_l \oplus T_l$ we obtained for 4-tuples of messages (i, j, k, l) after different steps:

- *Step 1* : At step 1, $3 \cdot 2^n$ messages have been evaluated (messages $[L, R]$, with $L = a, b, c$, a, b, c three different values, and R taking all possible value). After this step, $3 \cdot \frac{2^n(2^n-1)}{2}$ 4-tuples (i, j, k, l) have been considered, and for every such tuple, a test $S_i \oplus T_i = S_j \oplus T_j$ and $S_k \oplus T_k = S_l \oplus T_l$ has been done.
- *Step 2* : At step 2, $4 \cdot 2^n$ messages have been evaluated (messages $[L, R]$, with $L = a, b, c, d$, a, b, c, d four different values, and R taking all possible value). After this step, $6 \cdot \frac{2^n(2^n-1)}{2}$ 4-tuples (i, j, k, l) have been considered, and for every such tuple, a test $S_i \oplus T_i = S_j \oplus T_j$ and $S_k \oplus T_k = S_l \oplus T_l$ has been done.
- *Step 3* : At step 3, $5 \cdot 2^n$ messages have been evaluated (messages $[L, R]$, with $L = a, b, c, d, e$, a, b, c, d, e five different values and R taking all possible value). After this step, $10 \cdot \frac{2^n(2^n-1)}{2}$ 4-tuples (i, j, k, l) have been considered, and for every such tuple, a test $S_i \oplus T_i = S_j \oplus T_j$ and $S_k \oplus T_k = S_l \oplus T_l$ has been done.

Table 1. 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 both cases, after different steps

	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
Step 1 $3 \cdot 2^n$ messages $\frac{3 \cdot 2^n(2^n-1)}{2}$ tuples (i,j,k,l)tested	1	0.23
Step 2 $4 \cdot 2^n$ messages $\frac{6 \cdot 2^n(2^n-1)}{2}$ tuples (i,j,k,l)tested	1.6	0.84
Step 3 $5 \cdot 2^n$ messages $\frac{12 \cdot 2^n(2^n-1)}{2}$ tuples (i,j,k,l)tested	3.15	1.3

As claimed at Section 5, we obtained 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 $\mathcal{O}(2^n)$ messages.

F Comparison between Misty and Feistel Schemes

In order to compare our results of Table 3 in Appendix G with the known results on classical Feistel schemes ψ^d, we present in Table 2 the results for ψ^d (cf [8]). Let us recall here the definition of the (classical, i.e. balanced) Feistel schemes. Let $f_1 \in F_n$ (f_1 is not necessary a permutation unlike for Misty). By definition

$$\psi(f_1)([L,R] = [S,T] \Leftrightarrow S = R \text{ and } T = L \oplus f_1(R)$$

Let $f_1, \ldots, f_d$ be d bijections of F_n. Then by definition:

$$\psi(f_1, \ldots, f_d) = \psi(f_d) \circ \ldots \circ \psi(f_2) \circ \psi(f_1)$$

The permutation $\psi^k(f_1, \ldots, f_k)$ is called a “Feistel scheme with k rounds.”

Table 2. Minimum number A of computations needed to distinguish a Feistel generator ψ^d from random permutations with even signature of B_{2n}. This Table 2 (Feistel) is given here in order to compare it with Table 3.

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

All the values of Table 2 (Feistel schemes) can be obtained by using only 2 point attacks: 4 point attacks achieve sometimes the same complexity, but are never better in Feistel schemes, unlike in Misty schemes.

G Summary of the best known generic attacks on Misty schemes

We will use the following notation.

- A point on the left upside corner $\boxed{\begin{array}{ccc}\bullet & & \\ & A & \\ & & \end{array}}$ means that the value A can be obtained with a "4 point attack" (i.e. an attack that use correlation on inputs $[L, R]$ and output $[S, T]$ of 4 messages) from the expression of the S value (in L and R). We use the same notation for "3 point CPCA-2 attack" on M_L^3.
- A point on the right upside corner $\boxed{\begin{array}{ccc} & & \bullet \\ & A & \\ & & \end{array}}$ means that the value A can be obtained with a "4 point attack" from the expression $S \oplus T$ (in L and R).
- A point on the left downside corner $\boxed{\begin{array}{ccc} & & \\ & A & \\ \bullet & & \end{array}}$ means that the value A can be obtained with a "2 point attack" (i.e. correlation on pairs of messages) from the expression of the S value (in L and R), or by a "'1 point attack" from the expression of S (for one round M_L^1).
- A point on the right downside corner $\boxed{\begin{array}{ccc} & & \\ & A & \\ & & \bullet \end{array}}$ means that the value A can be obtained with a "2 point attack" from the expression of the $S \oplus T$ (in L and R).
- The double line between 5 and 6 rounds indicates that for more than 6 rounds, the best known values are greater than 2^{2n}.
- "New" means that the results is, as far as we know, new.

With these notations, the best known attacks on Misty schemes M_L^d are given in Table 3.

In Table 3 we did not mention CPA-2 and CPCA-1 since the best known results for these attacks are the same as for CPA-1.

• For Misty R schemes, M_R^d, the values A will be the same, except for 3 rounds in CPA-1, where the best known attack is in $A = \sqrt{2^n}$ for M_R^3 (instead of $A = 4$ for M_L^3).

• If we are looking not for the number of computations A, but for adversaries with unlimited computing power limited by m oracle queries, the best known attacks are given in Table 4. The bound $O(2^n)$ is here the "information bound": with unbounded computing power and $m \geq 2^n$ we can always distinguish (cf Appendix C).

Table 3. Minimum number A of computations needed to distinguish a Misty generator M_L^d from random permutations with an even signature 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 New
M_L^4	2^n New ●	● ● $\sqrt{2^n}$ New ●	● 4
M_L^5	● $2^{3n/2}$ New	● 2^n New	● 2^n New
M_L^6	● 2^{2n} New ●	● 2^{2n} New ●	● 2^{2n} New ●
M_L^7	● 2^{4n} ●New ●	● 2^{4n} ●New ●	● 2^{4n} ●New ●
M_L^8	2^{4n} New ●	2^{4n} New ●	2^{4n} New ●
M_L^9	2^{6n} ●New ●	2^{6n} ●New ●	2^{6n} ●New ●
M_L^{10}	2^{6n} New ●	2^{6n} New ●	2^{6n} New ●
M_L^d, d odd, $d \geq 9$	$2^{(d-3)n}$ ●New ●	$2^{(d-3)n}$ ●New ●	$2^{(d-3)n}$ ●New ●
M_L^d, d even, $d \geq 8$	$2^{(d-4)n}$ New ●	$2^{(d-4)n}$ New ●	$2^{(d-4)n}$ New ●

Table 4. Minimum number m of queries to distinguish M_L^d from a random permutation 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^n	2^n	2^n
M_L^6	2^n	2^n	2^n
M_L^6, $d \geq 6$	2^n	2^n	2^n