

Security of the Misty Structure Beyond the Birthday Bound

Jooyoung Lee

Faculty of Mathematics and Statistics
Sejong University, Seoul, Korea 143-747
jlee05@sejong.ac.kr

Abstract. In this paper, we first prove beyond-birthday-bound security for the Misty structure. Specifically, we show that an r -round Misty structure is secure against CCA attacks up to $O(2^{\frac{rn}{r+7}})$ query complexity, where n is the size of each round permutation. So for any $\epsilon > 0$, a sufficient number of rounds would guarantee the security of the Misty structure up to $2^{n(1-\epsilon)}$ query complexity.

Keywords: Misty structure, blockcipher, indistinguishability, pseudorandomness, coupling

1 Introduction

The Misty structure is a Feistel-type blockcipher structure used in Misty [9] and Kasumi [1]. It is known to be faster and more robust than the Feistel structure in terms of its resistance against linear and differential cryptanalysis. Its provable security also has been widely studied in the Luby and Rackoff model, where each round function is assumed to be a secret and truly random permutation [4, 5, 8, 9, 11, 18, 19]. In this model, Minier and Gilbert [11] showed that a 5-round Misty structure is secure against CCA attacks up to the birthday bound, i.e., $2^{\frac{n}{2}}$ query complexity for the size n of each round permutation.¹ Iwata et al. [5] showed that some of the five round permutations can be replaced by uniform ϵ -XOR universal permutations without losing its security. It is also shown that oracle access to some specific round permutations does not change the security. Piret and Quisquater [18] analyzed the security of the Misty structure when the round permutations are replaced by random involutions without fixed points. Lee and Koo [8] dropped the condition of having no fixed point and showed that such a construction is still secure.

However, all these results hold within the birthday bound. On the other hand, for the Feistel structure there has been a considerable progress in the research of its provable security in terms of the threshold query complexity. In a series of papers by Patarin [13–17], it was proved that a 6-round Feistel structure using n -bit random round functions is CCA-secure up to $2^{n(1-\epsilon)}$ query complexity for any $\epsilon > 0$. Morris, Rogaway and Stegers [12] took a novel approach based on a coupling technique to prove the security of maximally unbalanced Feistel structures beyond the birthday bound. This powerful technique is also used for the security proof of various types of generalized Feistel structures [3].

OUR CONTRIBUTION. In this paper, we prove beyond-birthday-bound security for the Misty structure. Specifically, we show that an r -round Misty structure is secure against CCA attacks up to $O(2^{\frac{rn}{r+7}})$ query complexity, where n is the size of each round permutation. So for any $\epsilon > 0$, a sufficient number of rounds would guarantee the security of the Misty structure up to $2^{n(1-\epsilon)}$ query complexity.

¹ In this work, we only consider the notion of “superpseudorandomness” that allows an adversary to make both forward and backward queries to the entire construction.

PROOF TECHNIQUES. Since the inverse of an L-Misty structure becomes an R-Misty structure with slight modification, we can view an L-Misty structure as a composition $F \circ G^{-1}$ for an L-Misty structure F and an R-Misty structure G , both of smaller numbers of rounds. Maurer, Pietrzak and Renner [10] proved that if two independent encryption schemes F and G are NCPA-secure, then $F \circ G^{-1}$ is CCA-secure. In this paper, we will use a combinatorial interpretation of this property given as Lemma 2 and 3.

As it turns out that a 4-round L-Misty structure has the same level of security as a 3-round R-Misty, we let the number of rounds $r = 7d$ for $d \geq 1$, and decompose an r -round L-Misty structure into a $4d$ -round L-Misty structure and the inverse of a $3d$ -round R-Misty structure. The NCPA-security of each component is proved by a coupling technique. Careful definition and analysis of couplings, given in the proof of Lemma 4, is the core of our security proof.

2 Preliminaries

2.1 Notations

For an integer $n \geq 1$, let $I_n = \{0, 1\}^n$ be the set of binary strings of length n . The set of all permutations on I_n will be denoted \mathcal{P}_n . We will usually write $N = 2^n$.

For two bitstrings x and y , $x||y$ denotes the concatenation of x and y . For a bitstring $x \in \{0, 1\}^{2n}$, x_L and x_R denote the unique n -bit strings such that $x = x_L||x_R$.

For a set T and an integer $s \geq 1$, T^{*s} denotes the set of all sequences that consists of s pairwise distinct elements of T . For integers $1 \leq s \leq t$, we will write $(t)_s = t(t-1) \cdots (t-s+1)$. If $|T| = t$, then $(t)_s$ becomes the size of T^{*s} .

2.2 Misty Structure

A 1-round L-Misty permutation is a $2n$ -bit permutation ϕ taking an n -bit permutation p as a round function and such that

$$\phi[p](u) = u_R || (p(u_L) \oplus u_R)$$

for $u \in \{0, 1\}^{2n}$. An r -round L-Misty structure is simply the composition of r 1-round L-Misty permutations, transforming r n -bit permutations p_1, \dots, p_r into a $2n$ -bit permutation

$$\phi^r[p_1, \dots, p_r] = \phi[p_r] \circ \cdots \circ \phi[p_1].$$

An r -round R-Misty structure ψ^r is similarly defined as the composition of r 1-round R-Misty permutations, where a 1-round R-Misty permutation transforms an n -bit permutation p into a $2n$ -bit permutation in the following manner.

$$\psi[p](u) = p(u_R) || (p(u_R) \oplus u_L)$$

for $u \in \{0, 1\}^{2n}$. 1-round L-Misty and R-Misty structures are illustrated in Figure 1.

Let f be a permutation on I_{2n} such that

$$f(u) = u_L || (u_L \oplus u_R).$$

Then we can check that $f \circ f = \iota$ and

$$f \circ \psi^r[p_r^{-1}, \dots, p_1^{-1}] \circ f \circ \phi^r[p_1, \dots, p_r] = \iota \tag{1}$$

where ι denotes the identity function on I_{2n} .

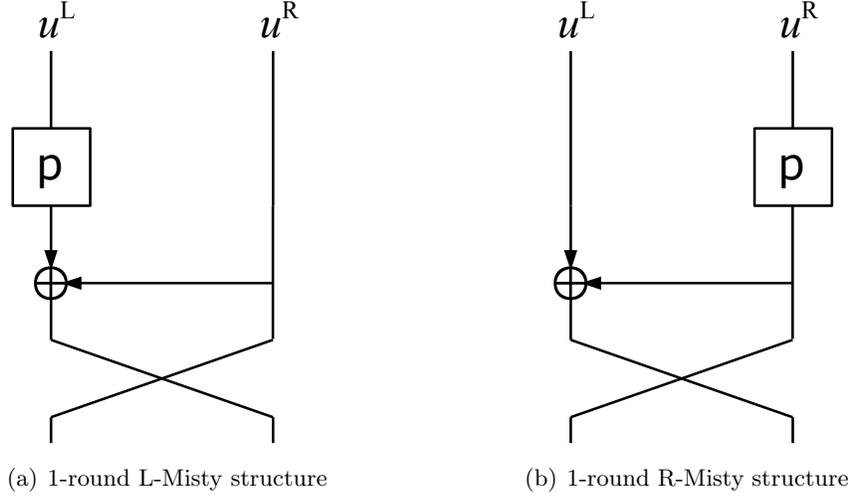


Fig. 1. Misty structures

2.3 Indistinguishability

Let $E \in \{\phi^r, \psi^r\}$ be an r -round Misty structure that makes oracle queries to r permutations $p_1, \dots, p_r \in \mathcal{P}_n$. So a set of r permutations $\Pi = (p_1, \dots, p_r) \in \mathcal{P}_n^r$ defines a permutation $E[\Pi]$ on $\{0, 1\}^{2n}$. In the *indistinguishability* framework, $E[\Pi]$ uses independent random permutations as round functions, while a permutation P is chosen uniformly at random from \mathcal{P}_{2n} . A distinguisher \mathcal{A} would like to tell apart two worlds $E[\Pi]$ and P by adaptively making forward and backward queries to the entire permutation. Formally, \mathcal{A} 's distinguishing advantage is defined by

$$\text{Adv}_E(\mathcal{A}) = \Pr \left[P \stackrel{\$}{\leftarrow} \mathcal{P}_{2n} : \mathcal{A}[P] = 1 \right] - \Pr \left[\Pi \stackrel{\$}{\leftarrow} \mathcal{P}_n^r : \mathcal{A}[E[\Pi]] = 1 \right].$$

For $q > 0$, we define

$$\text{Adv}_E(q) = \max_{\mathcal{A}} \text{Adv}_E(\mathcal{A})$$

where the maximum is taken over all adversaries \mathcal{A} making at most q queries. By the relation (1), we have

$$\text{Adv}_{\phi^r}(q) = \text{Adv}_{\psi^r}(q)$$

for any $r \geq 1$.

COMBINATORIAL FRAMEWORK. We assume that a distinguisher \mathcal{A} makes q queries to the permutation oracle and records a query history

$$\mathcal{Q} = (u^i, v^i)_{1 \leq i \leq q},$$

where (u^i, v^i) represents the evaluation obtained by the i -th query to the permutation oracle. So according to the instantiation, it implies either $E[\Pi](u^i) = v^i$ or $P(u^i) = v^i$. The query history \mathcal{Q} contains all the information that \mathcal{A} has obtained at the end of the attack. In this work, we will only consider information theoretic distinguishers. Therefore we can assume that a distinguisher is deterministic without making any redundant queries, and hence the output of \mathcal{A} can be regarded as a function of \mathcal{Q} , denoted $\mathcal{A}(\mathcal{Q})$.

If a permutation $E[\Pi]$ (resp. P) is consistent with \mathcal{Q} , i.e., $E[\Pi](u^i) = v^i$ (resp. $P(u^i) = v^i$) for every $i = 1, \dots, q$, then we will write $E[\Pi] \vdash \mathcal{Q}$ (resp. $P \vdash \mathcal{Q}$). Using these notations, we have

$$\text{Adv}_E(\mathcal{A}) = \sum_{\mathcal{A}(\mathcal{Q})=1} \Pr \left[P \stackrel{\$}{\leftarrow} \mathcal{P}_{2n} : P \vdash \mathcal{Q} \right] - \sum_{\mathcal{A}(\mathcal{Q})=1} \Pr \left[\Pi \stackrel{\$}{\leftarrow} \mathcal{P}_n^r : E[\Pi] \vdash \mathcal{Q} \right] \quad (2)$$

where the sum is taken over all the possible query history \mathcal{Q} such that $\mathcal{A}(\mathcal{Q}) = 1$.²

2.4 Coupling Technique

Given a finite event space Ω and two probability distributions μ and ν defined on Ω , the *total variation distance* between μ and ν , denoted $\|\mu - \nu\|$, is defined as

$$\|\mu - \nu\| = \frac{1}{2} \sum_{x \in \Omega} |\mu(x) - \nu(x)|.$$

The following definitions are also all equivalent.

$$\|\mu - \nu\| = \max_{S \subset \Omega} \{\mu(S) - \nu(S)\} = \max_{S \subset \Omega} \{\nu(S) - \mu(S)\} = \max_{S \subset \Omega} \{|\mu(S) - \nu(S)|\}.$$

A *coupling* of μ and ν is a distribution τ on $\Omega \times \Omega$ such that for all $x \in \Omega$, $\sum_{y \in \Omega} \tau(x, y) = \mu(x)$ and for all $y \in \Omega$, $\sum_{x \in \Omega} \tau(x, y) = \nu(y)$. In other words, τ is a joint distribution whose marginal distributions are respectively μ and ν . We will use the following two lemmas in the security proof.

Lemma 1. *Let μ and ν be probability distributions on a finite event space Ω , let τ be a coupling of μ and ν , and let (X, Y) be a random variable sampled according to distribution τ . Then $\|\mu - \nu\| \leq \Pr[X \neq Y]$.*

Lemma 2. *Let Ω be some finite event space and ν be the uniform probability distribution on Ω . Let μ be a probability distribution on Ω such that $\|\mu - \nu\| \leq \epsilon$. Then there is a set $S \subset \Omega$ such that*

1. $|S| \geq (1 - \sqrt{\epsilon})|\Omega|$,
2. $\mu(x) \geq (1 - \sqrt{\epsilon})\nu(x)$ for every $x \in S$.

The proof of the above lemmas is given in [6, 7]. For completeness, we include the same proof in Appendix A.

3 Security of the Misty Structure

In this section, we give only the security proof of an L-Misty structure since the security of L-Misty and R-Misty structures are equivalent. Specifically, we consider an r -round L-Misty structure ϕ^r , where r is a multiple of 7. We will write $r = l_1 + l_2$, where $l_1 = 4d$ and $l_2 = 3d$ for an integer $d \geq 1$. We begin with the following lemma.

² Here we only consider a “valid” query history that \mathcal{A} might produce by communicating with a permutation $P \in \mathcal{P}_{2n}$. For example, in a valid query history \mathcal{Q} , (x, y) and (x', y) with $x \neq x'$ could not be both contained in \mathcal{Q} .

Lemma 3. Let $E \in \{\phi^r, \psi^r\}$ and $\delta > 0$. Assume that for any query history \mathcal{Q} such that $|\mathcal{Q}| = q$, we have

$$p_1(\mathcal{Q}) \geq (1 - \delta)p_2(\mathcal{Q})$$

where

$$\begin{aligned} p_1(\mathcal{Q}) &= \Pr \left[\Pi \stackrel{\$}{\leftarrow} \mathcal{P}_n^r : E[\Pi] \vdash \mathcal{Q} \right], \\ p_2(\mathcal{Q}) &= \Pr \left[P \stackrel{\$}{\leftarrow} \mathcal{P}_{2n} : P \vdash \mathcal{Q} \right] = 1/(N^2)_q. \end{aligned}$$

Then we have

$$\text{Adv}_E(\mathcal{A}) \leq \delta.$$

Proof. By (2), we have

$$\begin{aligned} \text{Adv}_E(\mathcal{A}) &= \sum_{\mathcal{A}(\mathcal{Q})=1} p_2(\mathcal{Q}) - \sum_{\mathcal{A}(\mathcal{Q})=1} p_1(\mathcal{Q}) \\ &\leq \sum_{\mathcal{A}(\mathcal{Q})=1} p_2(\mathcal{Q}) - (1 - \delta) \sum_{\mathcal{A}(\mathcal{Q})=1} p_2(\mathcal{Q}) \\ &\leq \delta \sum_{\mathcal{A}(\mathcal{Q})=1} p_2(\mathcal{Q}) \leq \delta. \end{aligned}$$

Suppose that $\phi^r[\Pi] \vdash \mathcal{Q}$ for a set of permutations $\Pi = (p_1, \dots, p_r)$ and a query history $\mathcal{Q} = (u^i, v^i)_{1 \leq i \leq q}$. Let $\Pi_1 = (p_1, \dots, p_{l_1})$ and $\Pi_2 = (p_r^{-1}, \dots, p_{l_1+1}^{-1})$ (in reverse order). By (1), it follows that

$$\phi^{l_1}[\Pi_1] \vdash (u^i, w^i)_{1 \leq i \leq q} \text{ and } \psi^{l_2}[\Pi_2] \vdash (f(v^i), f(w^i))_{1 \leq i \leq q},$$

for some $\mathbf{w} = (w^i)_{1 \leq i \leq q} \in (I_{2n})^{*q}$. Therefore for a query history \mathcal{Q} , we have

$$\begin{aligned} p_1(\mathcal{Q}) &= \sum_{\mathbf{w} \in \Omega} \Pr \left[\Pi_1 \stackrel{\$}{\leftarrow} \mathcal{P}_n^{l_1}, \Pi_2 \stackrel{\$}{\leftarrow} \mathcal{P}_n^{l_2} : \phi^{l_1}[\Pi_1] \vdash (u^i, w^i)_{1 \leq i \leq q} \wedge \psi^{l_2}[\Pi_2] \vdash (f(v^i), f(w^i))_{1 \leq i \leq q} \right] \\ &= \sum_{\mathbf{w} \in \Omega} \Pr \left[\Pi \stackrel{\$}{\leftarrow} \mathcal{P}_n^{l_1} : \phi^{l_1}[\Pi] \vdash (u^i, w^i)_{1 \leq i \leq q} \right] \Pr \left[\Pi \stackrel{\$}{\leftarrow} \mathcal{P}_n^{l_2} : \psi^{l_2}[\Pi] \vdash (f(v^i), f(w^i))_{1 \leq i \leq q} \right] \end{aligned}$$

where $\Omega = (I_{2n})^{*q}$.

In order to lower bound each factor of the products appearing in the last equality, we define probability distributions $\mu_{\mathbf{s}}$ and $\lambda_{\mathbf{s}}$ for each $\mathbf{s} = (s^i)_{1 \leq i \leq q} \in \Omega$, where for each $\mathbf{w} = (w^i)_{1 \leq i \leq q} \in \Omega$,

$$\begin{aligned} \mu_{\mathbf{s}}(\mathbf{w}) &= \Pr \left[\Pi \stackrel{\$}{\leftarrow} \mathcal{P}_n^{l_1} : \phi^{l_1}[\Pi] \vdash (s^i, w^i)_{1 \leq i \leq q} \right], \\ \lambda_{\mathbf{s}}(\mathbf{w}) &= \Pr \left[\Pi \stackrel{\$}{\leftarrow} \mathcal{P}_n^{l_2} : \psi^{l_2}[\Pi] \vdash (s^i, w^i)_{1 \leq i \leq q} \right]. \end{aligned}$$

Using the coupling technique, we can upper bound the statistical distance between each of $\mu_{\mathbf{s}}$ and $\lambda_{\mathbf{s}}$ and the uniform probability distribution. The proof will be given at the end of this section.

Lemma 4. Let $\mu_{\mathbf{s}}$ and $\lambda_{\mathbf{s}}$ be the probability distributions defined as above, and let ν be the uniform probability distribution on $\Omega = (I_{2n})^{*q}$. Then we have $\|\mu_{\mathbf{s}} - \nu\| \leq \epsilon_1$ and $\|\lambda_{\mathbf{s}} - \nu\| \leq \epsilon_2$, where

$$\begin{aligned}\epsilon_1 &= \frac{N-1}{4(d+1)} \left(\frac{q}{N-q} + \frac{4q}{N-1} \right)^{d+1}, \\ \epsilon_2 &= \frac{N-1}{4(d+1)} \left(\frac{4q}{N-1} \right)^{d+1}.\end{aligned}$$

Applying Lemma 2 and 4 with $\mu = \mu_{\mathbf{s}}$ for $\mathbf{s} = \mathbf{u} = (u^i)_{1 \leq i \leq q}$, we have a subset $S_1 \subset \Omega$ such that $|S_1| \geq (1 - \sqrt{\epsilon_1})|\Omega|$ and

$$\Pr \left[\Pi \stackrel{\$}{\leftarrow} \mathcal{P}_n^{l_1} : \phi^{l_1}[\Pi] \vdash (u^i, w^i)_{1 \leq i \leq q} \right] \geq (1 - \sqrt{\epsilon_1})\nu(\mathbf{w}) = \frac{1 - \sqrt{\epsilon_1}}{(N^2)_q}$$

for every $\mathbf{w} \in S_1$.

Let $f(\mathbf{v}) = (f(v^i))_{1 \leq i \leq q}$ and $f(\mathbf{w}) = (f(w^i))_{1 \leq i \leq q}$. Again applying Lemma 2 and 4 with $\mu = \lambda_{\mathbf{s}}$ for $\mathbf{s} = f(\mathbf{v})$, we have a subset $S_2 \subset \Omega$ such that $|S_2| \geq (1 - \sqrt{\epsilon_2})|\Omega|$ and

$$\Pr \left[\Pi \stackrel{\$}{\leftarrow} \mathcal{P}_n^{l_2} : \psi^{l_2}[\Pi] \vdash (f(v^i), f(w^i))_{1 \leq i \leq q} \right] \geq (1 - \sqrt{\epsilon_2})\nu(f(\mathbf{w})) = \frac{1 - \sqrt{\epsilon_2}}{(N^2)_q}$$

for every $\mathbf{w} \in S_2$. Let $S = S_1 \cap S_2$. Since $|\Omega \setminus S_1| \leq \sqrt{\epsilon_1}|\Omega|$ and $|\Omega \setminus S_2| \leq \sqrt{\epsilon_2}|\Omega|$, we have

$$|\Omega \setminus S| = |\Omega \setminus (S_1 \cap S_2)| \leq |\Omega \setminus S_1| + |\Omega \setminus S_2| \leq (\sqrt{\epsilon_1} + \sqrt{\epsilon_2})|\Omega|,$$

or equivalently,

$$|S| \geq (1 - \sqrt{\epsilon_1} - \sqrt{\epsilon_2})|\Omega|.$$

Therefore it follows that

$$\begin{aligned}\mathfrak{p}_1(\mathcal{Q}) &= \sum_{\mathbf{w} \in \Omega} \Pr \left[\Pi \stackrel{\$}{\leftarrow} \mathcal{P}_n^{l_1} : \phi^{l_1}[\Pi] \vdash (u^i, w^i)_{1 \leq i \leq q} \right] \cdot \Pr \left[\Pi \stackrel{\$}{\leftarrow} \mathcal{P}_n^{l_2} : \psi^{l_2}[\Pi] \vdash (f(v^i), f(w^i))_{1 \leq i \leq q} \right] \\ &\geq (1 - \sqrt{\epsilon_1} - \sqrt{\epsilon_2})|\Omega| \cdot \left(\frac{1 - \sqrt{\epsilon_1}}{(N^2)_q} \right) \cdot \left(\frac{1 - \sqrt{\epsilon_2}}{(N^2)_q} \right) \\ &\geq (1 - 2\sqrt{\epsilon_1} - 2\sqrt{\epsilon_2})\mathfrak{p}_2(\mathcal{Q}).\end{aligned}$$

By Lemma 3 and the equivalence of ϕ^r and ψ^r , we have the following theorem.

Theorem 1. Let $\mathbf{E} \in \{\phi^r, \psi^r\}$ be an r -round Misty structure using r independent random n -bit permutations. If $r = 7d$ for $d \geq 1$, then

$$\text{Adv}_{\mathbf{E}}(q) \leq \sqrt{\frac{N-1}{d+1} \left(\frac{q}{N-q} + \frac{4q}{N-1} \right)^{d+1}} + \sqrt{\frac{N-1}{d+1} \left(\frac{4q}{N-1} \right)^{d+1}}.$$

ASYMPTOTIC INTERPRETATION. Assuming $q \leq N/2$, we can simplify the upper bound in Theorem 1 as

$$\text{Adv}_{\mathbf{E}}(q) \leq 2\sqrt{\frac{N-1}{d+1} \left(\frac{6q}{N-1} \right)^{d+1}} = 2\sqrt{\frac{(6q)^{d+1}}{(d+1)(N-1)^d}} \approx 2\sqrt{\frac{(6q)^{d+1}}{(d+1)N^d}}.$$

For a fixed parameter d , when $q \ll N^{\frac{d}{d+1}}$, the advantage $\text{Adv}_{\mathbb{E}}(q)$ gets close to 0.

PROOF OF LEMMA 4. Fix $\mathbf{s} = (s^i)_{1 \leq i \leq q}$ and for $m = 0, \dots, q$, define probability distributions π_m where for each $\mathbf{w} = (w^1, \dots, w^q) \in \Omega$,

$$\pi_m(\mathbf{w}) = \Pr \left[(u^{m+1}, \dots, u^q) \stackrel{\$}{\leftarrow} (I_{2n} \setminus \{s^1, \dots, s^m\})^{*(q-m)}, \right. \\ \left. II \stackrel{\$}{\leftarrow} \mathcal{P}_n^{l_1} : \phi^{l_1}[II] \vdash (s^i, w^i)_{1 \leq i \leq m} \wedge \phi^{l_1}[II] \vdash (u^i, w^i)_{m+1 \leq i \leq q} \right].$$

Then we can check that $\pi_0 = \nu$ and $\pi_q = \mu_{\mathbf{s}}$. Since

$$\|\mu_{\mathbf{s}} - \nu\| \leq \sum_{m=0}^{q-1} \|\pi_{m+1} - \pi_m\|, \quad (3)$$

we will focus on upper bounding $\|\pi_{m+1} - \pi_m\|$ for each $m = 0, \dots, q-1$. In order to couple π_{m+1} and π_m , we will define a random variable (T, V) on $\Omega \times \Omega$ by the sampling process described in Figure 2.

In this description, $D[j]$ and $R[j]$, all initialized as empty sets, represent the domain and the range of each round permutation p_j , respectively. Variable $p[j, x]$, initialized as \perp for every $1 \leq j \leq l_1$ and $x \in I_n$, records the evaluation of $p_j(x)$. Once evaluation $p_j(x) = y$ is determined by lazy sampling during the procedure $\mathbf{p}(j, x)$, then x and y are added to $D[j]$ and $R[j]$, respectively, and variable $p[j, x]$ is assigned y .

In lines 5 to 8, the first m elements that T and V share in common are initialized and faithfully updated. The $(m+1)$ -th elements of T and V are initialized in lines 9 and 10, and simultaneously updated in lines 11 to 25. The last $q-m-1$ elements of T and V are determined in lines 26 to 31 without any update process. As for this random variable, we point out some noteworthy properties.

1. In any case, the first m elements of T and V are equal.
2. If $t[l_1] = v[l_1]$, then $T = V$ at the end of the experiment.
3. By ignoring the steps used to sample V , we can check that T and V follow probability distributions π_{m+1} and π_m , respectively. Especially note that
 - (a) when $j \equiv 3 \pmod{4}$, the distribution of y' is uniform among the points in $I_n \setminus R[j]$, since Δ defines a perfect matching in

$$\{z \in I_n : z \notin R[j] \text{ and } z \oplus \Delta \notin R[j]\}$$

by connecting z and $z \oplus \Delta$,

- (b) if either $t[j-1]_L \in D[j]$ or $v[j-1]_L \in D[j]$, then the choice of y' is not affected by y in lines 22 and 23.

Therefore by Lemma 1, we have

$$\|\pi_{m+1} - \pi_m\| \leq \Pr[T \neq V] = \Pr[t[l_1] \neq v[l_1]]. \quad (4)$$

Since $t[j] = v[j]$ implies $t[j+1] = v[j+1]$ for every $0 \leq j \leq l_1 - 1$, we have

$$\Pr[t[l_1] \neq v[l_1]] \leq \prod_{h=0}^{d-1} \Pr \left[t[4h+4] \neq v[4h+4] \mid t[4h] \neq v[4h] \right]. \quad (5)$$

If any of $\mathbf{flag}_1[4h+3]$ and $\mathbf{flag}_2[4h+3]$ is not true, then we have

$$v[4h+4]_L = t[4h+3]_R = v[4h+3]_R = t[4h+4]_L.$$

Furthermore, if $t[4h+3]_R = v[4h+3]_R$ and $\mathbf{flag}_2[4h+4]$ is not true, then we have

$$t[4h+4]_R = v[4h+4]_R.$$

So the probability that $t[4h+4] \neq v[4h+4]$ is upper bounded by

$$\Pr[\mathbf{flag}_1[4h+3]] + \Pr[\mathbf{flag}_2[4h+3]] + \Pr[\mathbf{flag}_2[4h+4]]. \quad (6)$$

Since the probability of $\mathbf{flag}_1[4h+3]$ being true is upper bounded by the probability that $y \oplus \Delta \in \mathbf{R}[4h+3]$ for a random $y \stackrel{\$}{\leftarrow} I_n \setminus \mathbf{R}[4h+3]$, we have

$$\Pr[\mathbf{flag}_1[4h+3]] \leq \frac{q}{N-q}. \quad (7)$$

$\mathbf{flag}_2[4h+3]$ being true implies either $t[4h+2]_L \in \mathbf{D}[4h+3]$ or $v[4h+2]_L \in \mathbf{D}[4h+3]$. Again, $t[4h+2]_L \in \mathbf{D}[4h+3]$ implies

$$t[4h+2]_L = t[4h+1]_R = \mathbf{p}(4h+1, t[4h]_L) \oplus t[4h]_R = \mathbf{p}(4h+1, w^i[4h]_L) \oplus w^i[4h]_R$$

for some $i = 1, \dots, m$. Since $t[4h] \neq w^i[4h]$ for any $i = 1, \dots, m$, we can assume that $t[4h]_L \neq w^i[4h]_L$ in the above condition. Furthermore, since $\mathbf{p}(4h+1, \cdot)$ faithfully instantiates a truly random permutation, we have

$$\Pr[\mathbf{flag}_2[4h+3]] \leq \frac{2m}{N-1}. \quad (8)$$

With the same analysis, we also have

$$\Pr[\mathbf{flag}_2[4h+4]] \leq \frac{2m}{N-1}. \quad (9)$$

Then by (3), (4), (5), (6), (7), (8), (9), we obtain

$$\begin{aligned} \|\mu_{\mathbf{s}} - \nu\| &\leq \sum_{m=0}^{q-1} \left(\frac{q}{N-q} + \frac{4m}{N-1} \right)^d \\ &\leq \int_0^q \left(\frac{q}{N-q} + \frac{4x}{N-1} \right)^d dx \\ &\leq \frac{N-1}{4(d+1)} \left(\frac{q}{N-q} + \frac{4q}{N-1} \right)^{d+1}. \end{aligned}$$

In order to upper bound $\|\lambda_{\mathbf{s}} - \nu\|$, we fix $\mathbf{s} = (s^i)_{1 \leq i \leq q}$, and for $m = 0, \dots, q$, define probability distributions π'_m where for each $\mathbf{w} = (w^1, \dots, w^q) \in \Omega$,

$$\pi'_m(\mathbf{w}) = \Pr \left[(u^{m+1}, \dots, u^q) \stackrel{\$}{\leftarrow} (I_{2n} \setminus \{s^1, \dots, s^m\})^{*(q-m)}, \right.$$

$$\left. \Pi \stackrel{\$}{\leftarrow} \mathcal{P}_n^{l_2} : \psi^{l_2}[\Pi] \vdash (s^i, w^i)_{1 \leq i \leq m} \wedge \psi^{l_2}[\Pi] \vdash (u^i, w^i)_{m+1 \leq i \leq q} \right].$$

Since $\pi'_0 = \nu$ and $\pi'_q = \lambda_s$ we have

$$\|\lambda_s - \nu\| \leq \sum_{m=0}^{q-1} \|\pi'_{m+1} - \pi'_m\|. \quad (10)$$

In order to couple π'_{m+1} and π'_m , we define a random variable (T', V') on $\Omega \times \Omega$ by the sampling process described in Figure 3. We can check that T' and V' follow probability distributions π'_{m+1} and π'_m , respectively. We also have

$$\|\pi'_{m+1} - \pi'_m\| \leq \Pr [T' \neq V'] = \Pr [t[l_2] \neq v[l_2]] \quad (11)$$

and

$$\Pr [t[l_2] \neq v[l_2]] \leq \prod_{h=0}^{d-1} \Pr \left[t[3h+3] \neq v[3h+3] \mid t[3h] \neq v[3h] \right]. \quad (12)$$

If **flag** $[3h+2]$ is not true, then we have $t[3h+2]_L = v[3h+2]_L$. Similarly, if **flag** $[3h+3]$ is not true, then we have $t[3h+3]_L = v[3h+3]_L$, and subject to the condition $t[3h+2]_L = v[3h+2]_L$,

$$\begin{aligned} t[3h+3]_R &= t[3h+2]_L \oplus t[3h+3]_L \\ &= v[3h+2]_L \oplus v[3h+3]_L = v[3h+3]_R. \end{aligned}$$

Therefore the probability that $t[3h+3] \neq v[3h+3]$ is upper bounded by

$$\Pr [\mathbf{flag}[3h+2]] + \Pr [\mathbf{flag}[3h+3]]. \quad (13)$$

Similar to the analysis of the probability of **flag** $_1[4h+3]$ being true in the sampling process of (T, V) , we have

$$\Pr [\mathbf{flag}[3h+2]] \leq \frac{2m}{N-1}, \quad (14)$$

$$\Pr [\mathbf{flag}[3h+3]] \leq \frac{2m}{N-1}. \quad (15)$$

Therefore by (10), (11), (12), (13), (14), (15), we obtain

$$\begin{aligned} \|\lambda_s - \nu\| &\leq \sum_{m=0}^{q-1} \left(\frac{4m}{N-1} \right)^d \\ &\leq \int_0^q \left(\frac{4x}{N-1} \right)^d dx \\ &\leq \frac{N-1}{4(d+1)} \left(\frac{4q}{N-1} \right)^{d+1}. \end{aligned}$$

References

1. ETSI. Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms. Document 2: Kasumi algorithm specification (3GPP TS 35.202 version 3.1.2 Release 1999).
2. V. T. Hoang, B. Morris and P. Rogaway. An Enciphering Scheme Based on a Card Shuffle. CRYPTO 2012, LNCS 7417, pp. 7–13, Springer-Verlag, 2012.

```

1: for  $j \leftarrow 1$  to  $l_1$  do
2:    $D[j] \leftarrow \emptyset$ 
3:    $R[j] \leftarrow \emptyset$ 
4:    $p[j, x] \leftarrow \perp$  for every  $x \in I_n$ 
5:   for  $i \leftarrow 1$  to  $m$  do
6:      $w^i[0] \leftarrow s^i$ 
7:     for  $j \leftarrow 1$  to  $l_1$  do
8:        $w^i[j] \leftarrow w^i[j-1]_R || (\mathfrak{p}(j, w^i[j-1]_L) \oplus w^i[j-1]_R)$ 
9:    $t[0] \leftarrow s^{m+1}$ 
10:   $v[0] \stackrel{\$}{\leftarrow} I_{2n} \setminus \{s^1, \dots, s^m\}$ 
11:  for  $j \leftarrow 1$  to  $l_1$  do
12:    if  $t[j-1]_L \notin D[j]$  and  $v[j-1]_L \notin D[j]$  then
13:       $y \stackrel{\$}{\leftarrow} I_n \setminus R[j]$ 
14:       $\Delta \leftarrow t[j-1]_R \oplus v[j-1]_R$ 
15:      if  $j \equiv 3 \pmod{4}$  and  $y \oplus \Delta \notin R[j]$  then
16:         $y' \leftarrow y \oplus \Delta$ 
17:      else
18:         $\text{flag}_1[j] \leftarrow \text{true}$ 
19:         $y' \leftarrow y$ 
20:      else if  $t[j-1]_L \in D[j]$  or  $v[j-1]_L \in D[j]$  then
21:         $\text{flag}_2[j] \leftarrow \text{true}$ 
22:         $y \leftarrow \mathfrak{p}(j, t[j-1]_L)$ 
23:         $y' \leftarrow \mathfrak{p}(j, v[j-1]_L)$ 
24:         $t[j] \leftarrow t[j-1]_R || (y \oplus t[j-1]_R)$ 
25:         $v[j] \leftarrow v[j-1]_R || (y' \oplus v[j-1]_R)$ 
26:      if  $t[l_1] = v[l_1]$  then
27:         $(v^{m+2}, \dots, v^q) \stackrel{\$}{\leftarrow} (I_{2n} \setminus \{w^1[l_1], \dots, w^m[l_1], v[l_1]\})^{*(q-m-1)}$ 
28:         $(t^{m+2}, \dots, t^q) \leftarrow (v^{m+2}, \dots, v^q)$ 
29:      else
30:         $(v^{m+2}, \dots, v^q) \stackrel{\$}{\leftarrow} (I_{2n} \setminus \{w^1[l_1], \dots, w^m[l_1], v[l_1]\})^{*(q-m-1)}$ 
31:         $(t^{m+2}, \dots, t^q) \stackrel{\$}{\leftarrow} (I_{2n} \setminus \{w^1[l_1], \dots, w^m[l_1], t[l_1]\})^{*(q-m-1)}$ 
32:       $T \leftarrow (w^1[l_1], \dots, w^m[l_1], t[l_1], t^{m+2}, \dots, t^q)$ 
33:       $V \leftarrow (w^1[l_1], \dots, w^m[l_1], v[l_1], v^{m+2}, \dots, v^q)$ 
34:      return  $(T, V)$ 

Procedure  $\mathfrak{p}(j, x)$ 
35: if  $p[j, x] = \perp$  then
36:    $p[j, x] \stackrel{\$}{\leftarrow} I_n \setminus R[j]$ 
37:    $D[j] \leftarrow D[j] \cup \{x\}$ 
38:    $R[j] \leftarrow R[j] \cup \{p[j, x]\}$ 
39: return  $p[j, x]$ 

```

Fig. 2. Sampling process for random variable (T, V) that couples π_{m+1} and π_m

```

1: for  $j \leftarrow 1$  to  $l_2$  do
2:    $D[j] \leftarrow \emptyset$ 
3:    $R[j] \leftarrow \emptyset$ 
4:    $p[j, x] \leftarrow \perp$  for every  $x \in I_n$ 
5:   for  $i \leftarrow 1$  to  $m$  do
6:      $w^i[0] \leftarrow s^i$ 
7:     for  $j \leftarrow 1$  to  $l_2$  do
8:        $w^i[j] \leftarrow \mathfrak{p}(j, w^i[j-1]_R) || (\mathfrak{p}(j, w^i[j-1]_R) \oplus w^i[j-1]_L)$ 
9:    $t[0] \leftarrow s^{m+1}$ 
10:   $v[0] \stackrel{\mathfrak{S}}{\leftarrow} I_{2n} \setminus \{s^1, \dots, s^m\}$ 
11:  for  $j \leftarrow 1$  to  $l_2$  do
12:    if  $t[j-1]_R \notin D[j]$  and  $v[j-1]_R \notin D[j]$  then
13:       $y \stackrel{\mathfrak{S}}{\leftarrow} I_n \setminus R[j]$ 
14:       $y' \leftarrow y$ 
15:    else if  $t[j-1]_R \in D[j]$  or  $v[j-1]_R \in D[j]$  then
16:      flag $[j] \leftarrow \mathbf{true}$ 
17:       $y \leftarrow \mathfrak{p}(j, t[j-1]_R)$ 
18:       $y' \leftarrow \mathfrak{p}(j, v[j-1]_R)$ 
19:       $t[j] \leftarrow y || (y \oplus t[j-1]_L)$ 
20:       $v[j] \leftarrow y' || (y' \oplus v[j-1]_L)$ 
21:    if  $t[l_2] = v[l_2]$  then
22:       $(v^{m+2}, \dots, v^q) \stackrel{\mathfrak{S}}{\leftarrow} (I_{2n} \setminus \{w^1[l_2], \dots, w^m[l_2], v[l_2]\})^{*(q-m-1)}$ 
23:       $(t^{m+2}, \dots, t^q) \leftarrow (v^{m+2}, \dots, v^q)$ 
24:    else
25:       $(v^{m+2}, \dots, v^q) \stackrel{\mathfrak{S}}{\leftarrow} (I_{2n} \setminus \{w^1[l_2], \dots, w^m[l_2], v[l_2]\})^{*(q-m-1)}$ 
26:       $(t^{m+2}, \dots, t^q) \stackrel{\mathfrak{S}}{\leftarrow} (I_{2n} \setminus \{w^1[l_2], \dots, w^m[l_2], t[l_2]\})^{*(q-m-1)}$ 
27:     $T' \leftarrow (w^1[l_2], \dots, w^m[l_2], t[l_2], t^{m+2}, \dots, t^q)$ 
28:     $V' \leftarrow (w^1[l_2], \dots, w^m[l_2], v[l_2], v^{m+2}, \dots, v^q)$ 
29:    return  $(T', V')$ 

Procedure  $\mathfrak{p}(j, x)$ 
30: if  $p[j, x] = \perp$  then
31:    $p[j, x] \stackrel{\mathfrak{S}}{\leftarrow} I_n \setminus R[j]$ 
32:    $D[j] \leftarrow D[j] \cup \{x\}$ 
33:    $R[j] \leftarrow R[j] \cup \{p[j, x]\}$ 
34: return  $p[j, x]$ 

```

Fig. 3. Sampling process for random variable (T', V') that couples π'_{m+1} and π'_m

3. V. T. Hoang and P. Rogaway. On Generalized Feistel Networks. CRYPTO 2010. LNCS, vol. 6223, pp. 613–630, Springer-Verlag, 2010.
4. T. Iwata, T. Yoshino and K. Kurosawa. Non-cryptographic primitive for pseudorandom permutation. FSE 2002, LNCS 2365, pp. 149–163, Springer-Verlag, 2002.
5. T. Iwata, T. Yoshino, T. Yuasa and K. Kurosawa. Round security and super-pseudorandomness of MISTY type structure. FSE 2001, LNCS 2355, pp. 233–247, Springer-Verlag, 2001.
6. R. Lampe, J. Patarin and Y. Seurin. An asymptotically tight security analysis of the iterated Even-Mansour cipher. Asiacrypt 2012, LNCS 7658, pp. 278–295, Springer-Verlag, 2012.
7. J. Lee. Towards key-length extension with optimal security: cascade encryption and xor-cascade encryption. Eurocrypt 2013, LNCS 7881, pp. 405–425, Springer-Verlag, 2013.
8. J. Lee and B. Koo. Security of the Misty structure using involutions as round functions. IEICE Trans. Fundamentals, E93-A(9), 2010.
9. M. Matsui. New block encryption algorithm MISTY. FSE 1997, LNCS 1267, pp. 54–68, Springer-Verlag, 1997.
10. U. Maurer, K. Pietrzak and R. Renner: Indistinguishability Amplification. CRYPTO 2007, LNCS 4622, pp. 130–149. Springer, Heidelberg (2007)
11. M. Minier and H. Gilbert. New results on the pseudorandomness of some block cipher constructions. FSE 2001, LNCS 2355, pp. 248–266, Springer-Verlag, 2001.
12. B. Morris, P. Rogaway and T. Stegers. How to Encipher Messages on a Small Domain: Deterministic Encryption and the Thorp Shuffle. CRYPTO 2009. LNCS 5677, pp. 286–302, Springer-Verlag, 2009.
13. J. Patarin. About Feistel schemes with six (or more) rounds. FSE 1998. LNCS 1372, pp. 103–121, Springer-Verlag, 1998.
14. J. Patarin. Generic attacks on Feistel schemes. Asiacrypt 2001. LNCS 2248, pp. 222–238, Springer-Verlag, 2001.
15. J. Patarin. Luby-Rackoff: 7 rounds are enough for $2^{n-\epsilon}$ security. Crypto 2003. LNCS 2729, pp. 513–529, Springer-Verlag, 2003.
16. J. Patarin. New results on pseudorandom permutation generators based on the DES scheme. Crypto 1991. LNCS 576, pp. 301–312, Springer-Verlag, 1992.
17. J. Patarin. Security of random Feistel schemes with 5 or more rounds. Crypto 2004. LNCS 3152, pp. 106–122, Springer-Verlag, 2004.
18. G. Piret and J. Quisquater. Security of the MISTY structure in the Luby-Rackoff Model: improved results. SAC 2004, LNCS 3357, pp. 100–113, Springer-Verlag, 2004.
19. K. Sakurai and Y. Zheng. On non-pseudorandomness from block ciphers with provable immunity against linear cryptanalysis. IEICE Trans. Fundamentals, E80-A(1), 1997.

A Proof of Lemma 1 and Lemma 2

PROOF OF LEMMA 1. Let λ be a coupling of μ and ν and let $(X, Y) \sim \lambda$. By definition, for any $z \in \Omega$, $\lambda(z, z) \leq \min\{\mu(z), \nu(z)\}$. Since $\Pr[X = Y] = \sum_{z \in \Omega} \lambda(z, z)$, we have

$$\Pr[X = Y] \leq \sum_{z \in \Omega} \min\{\mu(z), \nu(z)\}.$$

Therefore we have

$$\begin{aligned} \Pr[X \neq Y] &\geq 1 - \sum_{z \in \Omega} \min\{\mu(z), \nu(z)\} \\ &= \sum_{z \in \Omega} (\mu(z) - \min\{\mu(z), \nu(z)\}) \\ &= \sum_{\substack{z \in \Omega \\ \mu(z) \geq \nu(z)}} (\mu(z) - \nu(z)) \\ &= \max_{S \subset \Omega} \{\mu(S) - \nu(S)\} = \|\mu - \nu\|. \end{aligned}$$

PROOF OF LEMMA 2. Let $S = \{x \in \Omega : \mu(x) \geq (1 - \sqrt{\epsilon})\nu(x)\}$. By definition, any element of S satisfies the second condition. Contrary to the first condition, suppose that $|S| < (1 - \sqrt{\epsilon})|\Omega|$. This implies $\nu(\Omega \setminus S) = 1 - |S|/|\Omega| > \sqrt{\epsilon}$, and hence

$$\nu(\Omega \setminus S) - \mu(\Omega \setminus S) \geq \nu(\Omega \setminus S) - (1 - \sqrt{\epsilon})\nu(\Omega \setminus S) = \sqrt{\epsilon}\nu(\Omega \setminus S) > (\sqrt{\epsilon})^2 = \epsilon.$$

This is a contradiction to $\|\mu - \nu\| \leq \epsilon$.