SCIS96 The 1996 Symposium on
Cryptography and Information Security
Komuro, Japan, January 29-31, 1996
The Institute of Electronics,
Information and Communication Engineers

**SCIS96-11C**

# On Pseudo Randomness from Block Ciphers

## — MISTY versus DES in cryptographic security—

*Kouichi SAKURAI*

Department of Computer Science
and Communication Engineering,
Kyushu University,
Hakozaki, Higashi-ku, Fukuoka 812-81, Japan
sakurai@csce.kyushu-u.ac.jp

*Yuliang ZHENG*

School of Comp & Info Tech
Monash University
McMahons Road, Frankston
Melbourne, VIC 3199,AUSTRALIA
yzheng@fcit.monash.edu.au

**Abstract:** MISTY is a data encryption algorithm recently proposed by M. Matsui from Mitsubishi. An important property of MISTY is that, in terms of theoretically provable resistance against linear cryptanalysis which along with differential cryptanalysis is the most powerful cryptanalytic attack known to date, it is twice as secure as the Data Encryption Standard or DES. This property can be attributed to the application of a new type of transformations in MISTY. These transformation are the main focus of this paper. Our research reveals that the transformations employed by MISTY, though superior in terms of strength against linear attacks, are inferior to Feistel-type transformations employed by DES when used to construct pseudorandom permutations. Another contribution of this paper is to show that MISTY has an algebraic property which may open a door for various cryptanalytic attacks. These results clearly indicate that the security of MISTY will remain open until a close examination of its resistance against other cryptanalytic attacks than linear or differential attacks.

# 1 Introduction

The Data Encryption Standard (DES) [NBS77] is the most widely used cipher over the world. The basic design of DES was accomplished in the 1970's. Due to rapid advances in cryptanalysis as well as computing technology over the past 20 years, especially the recent discovery of differential cryptanalysis by Biham and Shamir [BS93] and linear cryptanalysis by Matsui [Ma94], the security of DES is being questioned by an increasing number of researchers. Structurally DES can be viewed as being obtained by the iteration of a basic type of transformations. Both differential and linear cryptanalysis make use of statistical information on the basic transformations. In general this information becomes less and less useful to an attacker as the number of iterations increases.

Not all the design criteria for DES have been made public by its designer. Recent work by a number of researchers, however, shows that based on the iteration of the basic transformations employed by DES, it is possible to construct a block cipher that is provably secure against differential cryptanalysis. Notable work in this area includes the paper of Nyberg and Knudson [NK95]. Moreover, in [Nyb94] it has been shown that their earlier work can be generalized to resistance against linear cryptanalysis. Their work shows that in a theoretical framework, if the basic transformations used in DES are constructed to be strong against linear or differential cryptanalysis, 3 or more iterations of the transformations would result in a cipher that is immune to the cryptanalysis. An implication of this is that one reason for an iterative encryption algorithm, such as FEAL developed by NTT [Miy90], to be breakable by linear or differential cryptanalysis may lie in possible defects in basic transformations used by the encryption algorithm or a lack of an adequate number of iterations. It also suggests that by replacing the transformations with stronger ones, we may design an encryption algorithm that is more secure against linear of differential cryptanalysis.

Based on these observations, Matsui has proposed a new encryption algorithm called MISTY [Ma95a] that is provably twice as secure as DES against linear or differential cryptanalysis. It should be noted that an encryption algorithm secure against linear and differential cryptanalysis may be not secure against other types of cryptanalysis. One example of such an algorithm can be found in [Nyb93]. For this reason MISTY deserves special attention, simply because MISTY employs a new type of transformations which are different from that used in DES. One would expect that a cryptanalytic attack not applicable to DES may be used to break MISTY, which is precisely a major motivation of this research.

The soundness of the basic transformations used in DES has been theoretically studied by Luby and Rackoff [LR86]. In particular they proved that the concatenation of three basic transformations used in DES is in fact a pseudorandom permutation. In proving the result they assumed that truly random functions are used in the basic transformations. As the functions used in the basic transformations in DES are far from being random, their result does not form a proof for the security of DES.

It is important to note that Luby and Rackoff [LR86] also proved that the concatenation of two basic transformations used in DES never gives a pseudorandom permutation, as the resulting permutation is breakable by a chosen plaintext attack when it is regarded as an encryption algorithm. From this result can say that the approach taken by Luby and Rackoff is of fundamental importance to any basic transformation used in a cryptographic algorithm. This is best shown by recent studies on the security of an ISO authentication code [BKR94], one-way hashing functions [BGR94], and Kerberos-based key distribution [BR95].

In the Matsui's paper [Ma95a], soundness of the transformations used in MISTY has not been examined using Luby and Rackoff's approach. Hence, the focus of this paper is on the construction of pseudorandom permutations from the basic transformations used in MISTY, with the aim of comparing them against the basic transformations used in DES. We show that 3 iterations of the basic transformations in MISTY does not yield a pseudorandom permutation.

This should be contrasted to the basic transformations used in DES: as mentioned earlier, 3 iterations of them does result in a pseudorandom permutation. This contrast also shows that pseudorandom and resistance against linear or differential cryptanalysis are incomparable, hence provides an answer to the second open problem at the last section of [SP92].

More importantly we show that an concrete example of MISTY [Ma96b], which is based on a recursive application of the basic transformations, has an algebraic invariance property. This algebraic property could be potentially critical to the survivability of MISTY, as it would open a large door for various cryptanalytic attacks. These facts together clearly show that the basic transformation in MISTY are inferior to those in DES.

We have been examining on what conditions the basic transformations used in MISTY would yield a pseudorandom permutations. In particular we have considered cases where similar iterations of the transformations in DES would result in pseudorandom permutations. Our research so far in this direction shows that, in every case we considered, MISTY fails to produce pseudorandom permutations. To put in another way, in all these cases the basic transformations used in DES are superior to those used in MISTY.

# 2 Preliminary

## 2.1 Basic Notation

The set of positive integer is denoted by $\mathsf{N}$. For each $n \in \mathsf{N}$, let $I_n$ be the set of all $2^n$ binary strings of length $n$, i.e., $\{0,1\}^n$. For $s_1, s_2 \in I_n$, $s_1 \oplus s_2$ stands for the bit-wise XOR of $s_1$ and $s_2$, and $s_1 \bullet s_2$ denotes the XOR of the bit-wise products of $s_1$ and $s_2$.

Denote by $H_n$ the set of all functions from $I_n$ to $I_n$, which consists of $2^{n2^n}$ in total. The composition of two functions $f$ and $g$ in $H_n$, denoted by $f \circ g$, is defined by $f \circ g(x) = f(g(x))$, where $x \in I_n$. And in particular, $f \circ f$ is denoted by $f^2$, $f \circ f \circ f$ is denoted by $f^3$, and so on.

## 2.2 DES-like Transformation

Associate with each $f \in H_n$ a function $\delta_{2n,f}(L,R) = (R \oplus (L), L)$ for all $L, R \in I_n$. Note that $\delta_{2n,f}$ is a permutation in $H_{2n}$, and called the DES-like or Fiestel-type transformation associated with $f$ [NBS77]. Furthermore, for $f_1, f_2, \ldots, f_s \in H_n$, define $D(f_s, \ldots, f_2, f_1) = \delta_{2n,f_s} \circ \cdots \circ \delta_{2n,f_2} \circ \delta_{2n,f_1}$. We say that $D(f_s, \ldots, f_2, f_1)$ consists of $s$ rounds of DES-like transformations.

## 2.3 Notion of Pseudorandomness

Let $n \in \mathsf{N}$. An oracle circuit $T_n$ is an acyclic circuit which contains, in addition to ordinary AND, OR, NOT and constant gates, also a particular kind of gates – oracle gates. Each oracle gate has an $n$-bit output, and it is evaluated using some function from $H_n$. The output of $T_n$, a single bit, is denoted by $T_n[f]$ when a function $f \in H_n$ is used to evaluate the oracle gates. The size of $T_n$ is the total number of connections in it. Note that we can regard an oracle circuit as a circuit without any input or as a circuit with inputs to which constants are assigned.

A family of circuits $T = \{T_n | n \in \mathsf{N}\}$ is called statistical test for functions if each $T_n$ is an oracle whose size is bounded by some polynomial in $n$.

Assume that $S_n$ is a consisting of functions of $H_n$. Let $S = \{S_n | n \in \mathsf{N}\}$ and $H = \{H_n | n \in \mathsf{N}\}$. We say that $T$ is a distinguisher for $S$ if for some polynomial $P$ and for infinitely many $n$, we have

$$|Pr[T_n[s] = 1 - Pr[T_n[h] = 1]]| \leq 1/P(n),$$

where $s \in_R S_n$ and $h \in_R H_n$. We say hat $S$ is pseudorandom if there is no distinguisher for it. (See also [GGM86, LR86]).

# 3 Previous results

This section summarizes some of the currently known results on pseudorandomness of DES-like transformations. Note that only (some of) those directly related to this research have been shown below.

**Theorem 3.1** [LR86]: *$D(f, g)$ is not a PRG.*

**Theorem 3.2** [LR86]: *$D(f, g, h)$ is a PRG.*

**Theorem 3.3** [Pie90]: *$D(f, f, f, f^2)$ is PRG.*

We note that in the above theorems, $f$, $g$ and $h$ are functions drawn from $H_n$ independently at random.

# 4 A new block cipher: MISTY

The MISTY block encryption algorithm employs a type of transformations different from DES-like transformations. This section reviews the definition of the new transformations and relevant results on these transformations.

## 4.1 MISTY-like Transformation

Associate with $f \in H_n$, a function $\mu_{2n,f}(L, R) = (R, f(L) \oplus R)$ for all $L, R \in I_n$. $\mu_{2n,f}$ called the MISTY-like transformation associated with $f$ [Ma95a]. It is important to note that, unlike DES-like transformations, $\mu_{2n,f}$ forms a permutation over $I_{2n}$ only when $f \in H_n$ is also a permutation over $I_n$.

Furthermore, for $f_1, f_2, \ldots, f_s \in H_n$, define $M(f_s, \ldots, f_2, f_1) = \mu_{2n,f_s} \circ \cdots \circ \mu_{2n,f_2} \circ \mu_{2n,f_1}$. We say that $M(\mu_s, \ldots, \mu_2, \mu_1)$ consists of $s$ rounds of MISTY-like transformations.

## 4.2 Immunity against differential/linear cryptanalysis

Nyberg and Knudsen [NK95] introduced a measure of the security of block ciphers against differential cryptanalysis and showed that DES-like transformations gives block ciphers with provably security against the differential attack. Furthermore, Nyberg [Nyb94] extends the argument into the case of linear cryptanalysis.

The following measures are formulated in [Ma95a].

**Definition 4.1** [Ma95a]: *For given $f \in H_n, \Delta x, \Gamma x \in I_n$ and $\Delta y, \Gamma y \in I_n$*

$$DP(f) = \underset{\Delta x \neq 0, \Delta y}{MAX} \frac{\#\{x \in X | S(x) \oplus S(x \oplus \Delta x) = \Delta y)\}}{2^n},$$

$$LP(f) = \underset{\Gamma x, \Gamma y \neq 0}{MAX} (\frac{\#\{x \in X | x \bullet \Gamma x = S(x) \bullet \Gamma y)\}}{2^{n-1}} - 1)^2.$$

**Theorem 4.2** [NK95, Nyb94]: *For the s-round ($s \leq$) DES-like transformation $D(f_s, \ldots, f_2, f_1)$, assume that each function $f_i$ is a permutation and $DP(f_i) \leq p (resp. LP(f_i) \leq p)$. Then,*

$$DP(D(f_s, \ldots, f_2, f_1)) \leq 2p^2 \quad (resp.\ LP(D(f_s, \ldots, f_2, f_1)) \leq 2p^2).$$

**Remark 4.3:** Nyberg [Nyb93] showed that the DES-like transformation based on functions $f(x, k) = (x \oplus k)^{-1}$ in GF($2^n$) achieves highly resistant against differential attacks. Note, however, we can easily attack such an encryption scheme by solving low degree polynomial equations derived from known plaintext/ciphertext pairs. Thus, the measures in Definition4.2 is not enough for security criteria of block ciphers. Some recent works [Lai94, Knu94] give more refined measure of resistance against differential attacks.

By showing the following, Matsui [Ma95a] gives evidence that MISTY-like transformations do have an advantage over DES-like transformations, in terms of resistance against differential and linear cryptanalysis.

**Theorem 4.4** [Ma95a, Ma96b]: *For the s-round ($s \leq$) MISTY-like transformation $M(f_s, \ldots, f_2, f_1)$, assume that each function $f_i$ is a permutation and $DP(f_i) \leq p (resp. LP(f_i) \leq p)$. Then,*

$$DP(M(f_s, \ldots, f_2, f_1)) \leq p^2 \quad (resp. LP(M(f_s, \ldots, f_2, f_1)) \leq p^2).$$

In [Ma95a] Matsui also shows that 3-round MISTY-like transformations can be computed in (partially) parallel, whereas 3-round DES-like transformations cannot. This result was used by Matsui as further evidence to support the notion that MISTY-like transformations are better than their counterparts associated with DES.

# 5 Our results

We now investigate (non-)randomness of block ciphers obtained from MISTY-like transformations with aim to compare the security of MISTY with that of DES.

## 5.1 Non-randomness of MISTY

The following are results we have obtained so far regarding conditions under which MISTY-like transformations do not generate pseudorandom permutations. Note that each condition shown below gives pseudorandomness for DES-like transformation.

**Theorem 5.1:** *$M(f, g, h)$ is not a PRG.*

**Proof:** Let $S_3$ denote the 3-round concatenation. Then we have $S_3(L, R) = (R + f(L) + g(R), *)$, where $L$ and $R$ are arbitrary vectors from $I_n$ and $*$ denotes a string we don't care. Now we further assume that neither $L$ nor $R$ is 0. Then we have the following:

$$\begin{aligned} S_3(0,0) &= (f(0) + g(0), *) \\ S_3(L,0) &= (f(L) + g(0), *) \\ S_3(0,R) &= (f(0) + g(R) + R, *) \\ S_3(L,R) &= (f(L) + g(R) + R, *) \end{aligned}$$

Now adding together the left halves of the right-hand sides of the above four equations must give us 0. These observations indicates that we can construct an oracle circuit for $M(f, g, h)$ which uses only four (4) oracle gates. When $S_3$ is used in the oracle circuit for function evaluation, the oracle circuit always outputs a bit 1. On the other hand, when a random function is used in the oracle circuit, the probability for the oracle circuit to outputs a bit 1 is $1/2^n$. This proves that $M(f, g, h)$ is not a PRG. □

To interpret Theorem 5.1 in our plain language, the concatenation of three MISTY-like transformations, even if chosen independently at random, does not result in a PRG.

**Remark 5.2:** Ohnishi [Ohn88] gave a more general theorem on non-randomness related to Theorem 5.1: the family of functions with at most depth one (e.g. $f(L) \oplus g(R) \oplus h(L \oplus R)$) is not a PRG. Thus, for pseudorandom generation, functions must be at least depth two (e.g. $f(g(R))$).

For the concatenation of four MISTY-like transformations, we have the following two results.

**Theorem 5.3:** *$M(f^i, f^i, f^j, f^{i+j})$ is not a PRG, where $i$ and $j$ are integers larger than 0.*

A proof for this theorem can be easily obtained by noting the fact that a member in $M(f^i, f^i, f^j, f^{i+j})$ always translates $(0, 0)$ into $(*, 0)$, where $*$ as before means "don't care".

**Theorem 5.4:** *$M(f^i, f^i, f^j, f^i)$ is not a PRG, where $i$ and $j$ are integers larger than 0.*

**Proof:** To prove this theorem, we construct a oracle circuit for $M(f^i, f^i, f^j, f^i)$ that uses two oracle gates. The detailed arrangement of the two oracles is obtained through the following two observations:

1. A member of $M(f^i, f^i, f^j, f^i)$ always translates $(0, 0)$ into $(f^{i+j}(0), f^{i+j}(0) + f^i(0))$. Adding up the two halves gives us $f^i(0)$.

2. Now we have $(0, f^i(0))$, which will be translated by the same member function in $M(f^i, f^i, f^j, f^i)$ into $(f^{2i}(0) + f^j(0), f^{2i}(0) + f^j(0) + f^i(0))$. Interestingly, adding up the two halves, again we have $f^i(0)$.

The oracle circuit based on the above observations outputs a bit 1 with certainty when its oracles are evaluated using a member of $M(f^i, f^i, f^j, f^i)$, but with a probability of $1/2^n$ when using a truly random function. □

Finally we show a result on the concatenation of five (5) MISTY-like transformations.

**Theorem 5.5:** *$M(f^i, f^i, f^j, f^{i+j}, g)$ is not a PRG, where $i$ and $j$ are integers larger than 0.*

The proof for Theorem 5.5 is surprisingly simple: a member of $M(f^i, f^i, f^j, f^{i+j}, g)$ translates $(0, 0)$ into $(0, *)$, even if $f$ and $g$ are chosen independently at random.

It remains an interesting topic to see whether the above techniques can be generalized to other cases, including $MISTY(f, f, f, g)$, $MISTY(f, f, g, f)$, $MISTY(f, f, f, f, g)$, etc.

### 5.2 Practical consequences of non-randomness

Though the argument of non-randomness in the previous section is theoretical, the algorithm of the distinguisher could suggest potential attacks on MISTY and related block ciphers.

Consider 3-round MISTY-like transformations. As we have shown in Theorem 5.1, 3-round MISTY-like transformations is not a PRG. Set $T(L, R)$ be the left 32-bits of output of $S_3(L, R)$. Then, the following relation holds in 3-round MISTY-like transformations.

$$T(L, R) = T(0, 0) + T(L, 0) + T(0, R).$$

This implies that $T$ has an algebraic structure and $T(L, R)$ is computed from three ciphertexts, $T(0, 0), T(L, 0), and T(0, R)$. Even more importantly, the following general relation

$$T(L, R) = T(A, B) + T(L, B) + T(A, R),$$

holds for any 32-bit data $A$ and $B$. This implies that a known-plaintext attack may be applicable to the the left 32-bits of output of 3-round MISTY-like transformations.

For a cipher to be secure, the above algebraic relations must be avoided. To see this point, we note that by using Luby and Rackoff's argument for Theorem 3.1, an encryption algorithm placed in the public domain [Sch95] which was based on 2-round DES-like transformations, is not secure against a similar known-plaintext attack as described above.

Though such an algebraic structure could disappear in higher-round MISTY-like transformations. the biggest F-function of MISTY is recursively constructed from 3-round small MISTY-like transformations. Hence, the biggest F-function has the algebraic structure explained above.

We believe that this could be used by a cryptanalyst and hence cast very serious doubts on the security of MISTY. Indeed MISTY may be immune against the differential or linear attack, however, the fact that MISTY adopts 3-round small MISTY-like transformations in its big F-functions could render the cipher vulnerable to other (chosen plaintext) attacks.

**Remark 5.6:** In a private communication [Ma96pc], Matsui indicated that he realized the algebraic structure above in the biggest F-functions in the process of designing MISTY, and cautions have been taken to protect against attacks based on such an algebraic structure of F-functions. We believe, however, these methods are only heuristic and lack firm theoretical supports.

## 6 Concluding remarks

We have shown conditions that transformations used in MISTY do not yield a pseudorandom permutations. Remarking similar iterations of the transformations in DES would result in pseudorandom permutations, these cases all show that the basic transformations in DES are superior to those in MISTY.

Future research topics are to find conditions on transformations used in MISTY yield a pseudorandom permutations, and to compare MISTY with DES in other security criteria. A concrete problem which remain open is that:

> Is 4-round MISTY-like transformation $M(f, g, h, i)$ a pseudorandom permutation generator ?

## References

[BS93] Bihim, E. and Shamir, A., "Differential cryptanalysis of the Data Encryption Standard," Springer-Verlag, New York, (1993).

[BGR94] Bellare, M., Guérin, R., and Rogaway, P., "XOR MACs: New methods for message authentication using finite pseudorandom functions," in Advances in Cryptology – Crypto'95, Lecture Notes in Computer Science 963, pp.14-28, *Springer-Verlag*, Berlin (1995).

[BKR94] Bellare, M., Kilian, J., and Rogaway, P., "The security of cipher block chaining," in Advances in Cryptology – Crypto'94, Lecture Notes in Computer Science 839, pp.341-358, *Springer-Verlag*, Berlin (1994).

[BR93] Bellare, M. and Rogaway, P., "Entity authentication and key distribution," in Advances in Cryptology – Crypto'93, Lecture Notes in Computer Science 773, pp.232-249, *Springer-Verlag*, Berlin (1994).

[BR94] Bellare, M. and Rogaway, P., "Optimal Asymmetric Encryption," in Advances in Cryptology – EUROCRYPT'94, Lecture Notes in Computer Science 950, pp.92-111, *Springer-Verlag*, Berlin (1995).

[BR95] Bellare, M. and Rogaway, P., "Provably secure session key distribution — The three party case," Proc. of STOC'95.

[GGM86] Goldreich, O., Goldwasser, S., and Micali, S., "How to construct random functions," in JACM, Vol.33, No.4, pp.792-807 (1986).

[Knu94] Knudsen, L., "Truncated and higher order differentials," Proc. of 2nd Fast Software Encryption, LNCS 1008, pp.197-211, *Springer-Verlag*, Berlin (1995).

[Lai94] Lai, X., "Higher order derivatives and differential cryptanalysis," Proc. of Comm. Coding and Cryptography, (Feb.1994).

[LR86] Luby, M. and C. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions," STOC'86 (also in SIAM-COMP.1988).

[Ma94] Matsui, M., "Linear cryptanalysis method for DES cipher," in Advances in Cryptology – EUROCRYPT'93, LNCS 756, pp.386-397, *Springer-Verlag*, Berlin (1994).

[Ma95a] Matsui, M., "On probably security of block ciphers against differential and linear cryptanalysis," Proc. of SITA'95 (1995).

[Ma96b] Matsui, M., "New structure of block cipher with probable security against differential and linear cryptanalysis," To appear in 3rd Fast Software Encryption (1996) (also in these proceedings).

[Ma96pc] Personal communication via email with M.Matsui (Dec. 1996).

[Mau92] Maurer, U.K.. "A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators," in Advances in Cryptology – EUROCRYPT'92, Lecture Notes in Computer Science 658, pp.239-255, *Springer-Verlag*, Berlin (1995).

[Miy90] Miyagichi,S., "The FEAL cipher family," in Advances in Cryptology – CRYPTO'90, LNCS 573, pp.627-638, *Springer-Verlag*, Berlin (1991).

[NBS77] National Bureau of Standards, NBS FIPS PUB 46, "Data Encryption Standard," U.S.Department of Commerce (Jan. 1977).

[NK95] Nyberg, K. and Knudsen, L.R., "Provable security against a differential attacks ," J. Cryptology, Vol.8, pp.27-37 (1995).

[Nyb93] Nyberg, K. "Differentially uniform mappings for cryptography," in Advances in Cryptology – EUROCRYPT'93, LNCS 765, pp.55-64, *Springer-Verlag*, Berlin (1994).

[Nyb94] Nyberg, K. "Linear approximation of block ciphers," in Advances in Cryptology – EUROCRYPT'94, Lecture Notes in Computer Science 950, pp.439-444, *Springer-Verlag*, Berlin (1995).

[Ohn88] Ohnishi, Y. "A study on data security," Master Thesis (in Japanese), *Tohoku University*, Japan (March, 1988).

[Pat92] Patarin, J. "How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function," in Advances in Cryptology – EUROCRYPT'92, Lecture Notes in Computer Science 658, pp.256-266, *Springer-Verlag*, Berlin (1995).

[Pie90] Pieprzyk, J. "How to construct pseudorandom permutations from single pseudorandom functions," in Advances in Cryptology – EUROCRYPT'90, Lecture Notes in Computer Science 473, pp.140-150, *Springer-Verlag*, Berlin (1995).

[Sch95] Schneier, B. "Applied Cryptography (2nd Edition)," *John Wiley & Sons, Inc.*, (1995).

[SP92] Sadeghiyan,B., and Pieprzyk, J. "A construction for pseudorandom permutations from a single pseudorandom function," in Advances in Cryptology – EUROCRYPT'92, Lecture Notes in Computer Science 658, pp.267-284, *Springer-Verlag*, Berlin (1995).

[ZMI89] Zheng, Y., Matsumoto, T. and Imai, H. "Impossibility and optimality results on constructing pseudorandom permutations," in Advances in Cryptology – EUROCRYPT'89, Lecture Notes in Computer Science 434, pp.412-422, *Springer-Verlag*, Berlin (1990).

[ZMI89] Zheng, Y., Matsumoto, T. and Imai, H. "On the construction of block ciphers provably secure and not relying on any unproven hypotheses," in Advances in Cryptology – CRYPTO'89, Lecture Notes in Computer Science 435, pp.461-480, *Springer-Verlag*, Berlin (1990).

[Zhe90] Zheng, Y. "Principles for designing secure block ciphers and one-way hash functions," Ph.D Thesis, *Yokohama National University*, Japan (Dec. 1990).