PAPER Special Section on Cryptography and Information Security

On Non-Pseudorandomness from Block Ciphers with Provable Immunity Against Linear Cryptanalysis

Kouichi SAKURAI†, *Member and* Yuliang ZHENG††, *Nonmember*

SUMMARY Weakness of a block cipher, which has provable immunity against linear cryptanalysis, is investigated. To this end, the round transformation used in MISTY, which is a data encryption algorithm recently proposed by M. Matsui from Mitsubishi Electric Corporation, is compared to the round transformation of DES from the point of view of pseudorandom generation. An important property of the MISTY cipher is that, in terms of *theoretically provable resistance against linear and differential cryptanalysis*, which are the most powerful cryptanalytic attacks known to date, it is more robust than the Data Encryption Standard or DES. This property can be attributed to the application of a new round transform in the MISTY cipher, which is obtained by changing the location of the basic round-function in a transform used in DES. Cryptographic roles of the transform used in the MISTY cipher are the main focus of this paper. Our research reveals that when used for constructing pseudorandom permutations, the transform employed by the MISTY cipher is inferior to the transform in DES, though the former is superior to the latter in terms of strength against linear and differential attacks. More specifically, we show that a 3-round (4-round, respectively) concatenation of transforms used in the MISTY cipher is *not* a pseudorandom (super pseudorandom, respectively) permutation. For comparison, we note that with three (four, respectively) rounds, transforms used in DES yield a pseudorandom (super pseudorandom, respectively) permutation. Another contribution of this paper is to show that a 3-round concatenation of transforms used in (the preliminary version of) the MISTY cipher has an algebraic property, which may open a door for various cryptanalytic attacks. These results clearly indicate that provable immunity against linear and differential cryptanalysis is not sufficient for designing a secure block cipher, and the security of the MISTY cipher will remain open until a close examination of its resistance is conducted against other cryptanalytic attacks than the linear or differential attack.

key words: *block cipher, cryptography, Data Encryption Standard, differential cryptanalysis, linear cryptanalysis, pseudorandom permutation, security, secret-key block cipher*

1. Introduction

The Data Encryption Standard (DES) [17] is the most widely used cipher over the world. It has been nearly a quarter of a century since DES was published 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 [2] and linear cryptanalysis by Matsui [14], the cryptographic strength of DES is being questioned by an increasing number of researchers as well as practitioners. Structurally DES can be viewed as being obtained by the iteration of a basic transform which was first proposed by Feistel [8], [9] and will be called a DES-like transform in this paper. Both differential and linear cryptanalysis take advantage of statistical information on the transform. 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 designers. Recent work by some researchers, however, shows that based on the iteration of DES-like transforms, it is possible to construct a block cipher that is provably secure against differential cryptanalysis. Notable works in this area include that by Nyberg and Knudsen [18] which, since its initial publication at CRYPTO '92, has been further generalized to resistance against linear cryptanalysis in [20]. These results show that in a theoretical framework, if a DES-like transform is constructed to be strong against linear or differential cryptanalysis, the iterations of three or more rounds of the transform would result in a cipher that is immune to the cryptanalysis.

Based on these observations, Matsui has proposed a new block cipher (encryption algorithm) called MISTY [16]. A preliminary version of the MISTY cipher appears in [16], where it is shown that the MISTY cipher is provably more robust than DES in terms of its resistance against linear or differential cryptanalysis. In studying the security of a cipher, however, we should bear in mind that there is in general no inclusive relationship in the power of cryptanalytic attacks. In particular, a cipher secure against linear and differential cryptanalysis may be insecure against other (seemingly weaker) types of cryptanalysis. One example of such an algorithm can be found in [19]. In this context the MISTY cipher deserves special attention, as it employs a new transform that is different from a DES-like one. It is quite natural for one to expect that a cryptanalytic attack not applicable to DES may be used for breaking the MISTY cipher, which is precisely the major motivation of this research.

The cryptographic soundness of DES-like transforms has been theoretically studied by Luby and Rack-

Manuscript received March 15, 1996.
Manuscript revised July 10, 1996.

†The author is with the Department of Computer Science and Communication Engineering, Kyushu University, Fukuoka-shi, 812-81 Japan.

††The author is with the School of Comp & Info Tech, Monash University, Melbourne, VIC 3199, Australia.

off[13]. In particular they proved that a 3-round concatenation of DES-like transforms yields a pseudorandom permutation. In proving the result they assumed that truly random and independent functions were used in the three round transforms. As the function used in a DES-like transform is 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[13] also proved that a 2-round concatenation of DES-like transforms never gives a pseudorandom permutation, as the resulting permutation is breakable by a chosen plaintext attack when the permutation is regarded as a cipher. From this result one can say that the approach taken by Luby and Rackoff is of fundamental importance to any basic transform used in a cryptographic algorithm. This can be further demonstrated by recent studies on the security of message authentication codes[3],[4], and Kerberos-like key distribution[7].

When the preliminary version of the MISTY cipher was published in [16], the soundness of a transform used in the MISTY cipher, which will be called a MISTY-like transform hereafter, was not examined in the context of Luby and Rackoff's approach. Hence, the focus of this paper is on the construction of pseudorandom permutations from MISTY-like transforms, with the aim of comparing a MISTY-like transform against a DES-like one. We show that a 3-round concatenation of MISTY-like transforms does not yield a pseudorandom permutation. This should be compared with DES-like transforms: as mentioned earlier, a concatenation of the same number of DES-like transforms does result in a pseudorandom permutation. This contrast also shows that pseudorandomness and resistance against linear or differential cryptanalysis are incomparable. Hence it provides an answer to the second open problem in the last section of[24].

More importantly we show that a 3-round concatenation of MISTY-like transforms proposed in [16], has an algebraic invariance property. As 3-round concatenations are recursively used as basic building blocks for each round in a preliminary version of the MISTY cipher, this algebraic property would open a large door for various cryptanalytic attacks, and hence could be a potentially critical weakness of a preliminary version of the MISTY cipher. These facts clearly show that MISTY-like transforms are inferior to DES-like ones.

We have also examined under which conditions MISTY-like transforms would yield a pseudorandom permutation. In particular we have considered cases where similar concatenations of DES-like transforms would result in pseudorandom permutations. Our research in this direction shows that, in every case we considered, MISTY-like transforms fail to produce pseudorandom permutations. To put it in another way, in all these cases DES-like transforms are superior to MISTY-like ones.

2. Preliminary

2.1 Basic Notation

The set of positive integers is denoted by 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 exclusive-or of s_1 and s_2, and $s_1 \bullet s_2$ denotes the bit-wise product 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, $f \circ f \circ f$ by f^3, and so on.

By $x \in_R X$ we mean that x is drawn randomly and uniformly from a set X.

2.2 DES-Like Transforms

Associate with each $f \in H_n$ a function

$$\delta_{2n,f}(L,R) = (R \oplus f(L), L)$$

for all $L, R \in I_n$. In cryptography, the function f used in $\delta_{2n,f}$ is commonly referred to as *the F-function* of $\delta_{2n,f}$. Note that $\delta_{2n,f}$ is a permutation in H_{2n}, and it is commonly called a DES-like transform associated with f[8],[9],[17]. Furthermore, for $f_1, f_2, \ldots, f_s \in H_n$, define $D(f_s, \ldots, f_2, f_1) = \delta_{2n,f_s} \circ \cdots \circ \delta_{2n,f_2} \circ \delta_{2n,f_1}$ as an s-round concatenation of DES-like transforms.

Various generalizations of DES-like transforms, together with their cryptographic applications, were studied in [25]–[27].

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 a 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 all the oracle gates in T_n. 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 oracle circuits $T = \{T_n | n \in \mathsf{N}\}$ is called a statistical test for functions if there is a polynomial $Q(n)$ such that the size of each T_n is not larger than $Q(n)$.

Assume that S_n is a set composed of functions from 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 there is a polynomial $P(n)$ such that for infinitely many n, we have

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

where $s \in_R S_n$ and $h \in_R H_n$. We say that S is pseudorandom if there is no distinguisher for it. (See also [10], [13]).

3. Previous Results

This section summarizes some of the currently known results on pseudorandomness of DES-like transforms. We note that only those directly related to this research have been shown below.

Theorem 3.1 [13]: $\{D(g,f)|g,f \in H_n, n \in \mathsf{N}\}$ is not a pseudorandom permutation generator.

Theorem 3.2 [13]: $\{D(h,g,f)|h,g,f \in H_n, n \in \mathsf{N}\}$ is a pseudorandom permutation generator.

Theorem 3.3 [22]: $\{D(f^2,f,f,f)|f \in H_n, n \in \mathsf{N}\}$ is a pseudorandom permutation generator.

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

4. Some Facts on MISTY-Like Transforms

The MISTY cipher employs a transform different from a DES-like one. This section reviews the definition of the new transform, as well as relevant results on it.

4.1 Definition of MISTY-Like Transforms

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 a MISTY-like transform associated with f [16]. Similarly to a DES-like transform $\delta_{2n,f}(L,R) = (R \oplus f(L), L)$, we call the function f used in $\mu_{2n,f}$ the F-function of $\mu_{2n,f}$. Comparing $\mu_{2n,f}$ with $\delta_{2n,f}$, two differences between them are apparent: the first is the position where the F-function is placed, and the second is that unlike $\delta_{2n,f}$, $\mu_{2n,f}$ forms a permutation over I_{2n} only when f is also a permutation over I_n.

In addition, for $f_1, f_2, \ldots, f_s \in H_n$, we define $M(f_s, \ldots, f_2, f_1) = \mu_{2n,f_s} \circ \cdots \circ \mu_{2n,f_2} \circ \mu_{2n,f_1}$ as an s-round concatenation of MISTY-like transforms.

In [16] Matsui observes that unlike DES-like transforms, a 3-round concatenation of MISTY-like transforms allows partial parallel computation. This suggests that a cipher based on MISTY-like transforms would be more suitable for hardware implementation than those based on DES-like transforms. In the next section we turn to a more important issue, that is the resistance of a MISTY-like transform to cryptanalytic attacks, especially linear and differential attacks.

4.2 Immunity Against Differential and Linear Cryptanalysis

Nyberg and Knudsen [18] introduced a measure of security of block ciphers against differential cryptanalysis and showed that DES-like transforms yield block ciphers with provably security against differential attacks. Furthermore, Nyberg [20] extends the argument into the case of linear cryptanalysis.

The following measures are formulated in [16].

Definition 4.1 [16]: For $f \in H_n, \Delta x, \Gamma x \in I_n$ and $\Delta y, \Gamma y \in I_n$, define

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

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

Using this definition, a result in [18], [20] can now be stated as follows:

Theorem 4.2 [18], [20]: For an s-round concatenation ($s \geq 3$) of DES-like transforms $D(f_s, \ldots, f_2, f_1)$, assuming that $DP(f_i) \leqq p$, we have

$$DP(D(f_s, \ldots, f_2, f_1)) \leqq 2p^2.$$

Similarly, assuming that $LP(f_i) \leqq p$, we have

$$LP(D(f_s, \ldots, f_2, f_1)) \leqq 2p^2.$$

Remark 4.3: Nyberg [19] showed that a DES-like transform based on a function $f(x,k) = (x \oplus k)^{-1}$ on GF(2^n) achieves high resistance against differential attacks. Note, however, we can easily crack such a cipher by solving a set of low degree polynomial equations derived from known plaintext/ciphertext pairs. Thus, the measures introduced in Definition 4.1 are not sufficient for the security of a block cipher. This conclusion is further supported by extended differential attacks proposed in [11], [12]. In particular, the higher order differential cryptanalysis discussed in [11] breaks a 6-round version of an example cipher proposed in [18], despite of the fact that this example cipher has been proven to be resistant against ordinary differential attacks. These successfully extended attacks could be helpful in refining the security measures in Definition 4.1.

A key result in [16] is the following which was served as evidence that MISTY-like transforms would have an advantage over DES-like transforms, in terms of resistance against differential and linear cryptanalysis.

Theorem 4.4 [16]: For an s-round concatenation ($s \geq 3$) of MISTY-like transforms $M(f_s, \ldots, f_2, f_1)$, where each f_i is a permutation, assuming that $DP(f_i) \leqq p$, we have

$$DP(M(f_s, \ldots, f_2, f_1)) \leqq p^2.$$

Similarly, assuming that $LP(f_i) \leqq p$, we have

$$LP(M(f_s, \ldots, f_2, f_1)) \leqq p^2.$$

Remark 4.5: Recently, Aoki and Ohta [1] reported that the inequalities in Theorem 4.2 can be improved to the following:

$$DP(D(f_s, \ldots, f_2, f_1)) \leqq p^2$$
$$(LP(D(f_s, \ldots, f_2, f_1)) \leqq p^2, \text{respectively})$$

under the assumption that each function f_i is a permutation. This result disproves Matsui's conjecture on the advantages of MISTY-like transforms over DES-like transforms with respect to immunity against differential and linear cryptanalysis.

5. Our Results

We now investigate (non-) randomness of permutations obtained from MISTY-like transforms in order to compare the security of the MISTY cipher with that of DES.

5.1 Non-Randomness of MISTY-Like Transforms

The following are results we have obtained so far regarding conditions under which MISTY-like transforms do not generate pseudorandom permutations. For all conditions shown in Theorems 5.1 – 5.5, except that in Theorem 5.3 which is currently being investigated by the authors, it is known that DES-like transforms give pseudorandomness permutations.

Theorem 5.1: $\{M(h,g,f)|h,g,f \in H_n, n \in \mathsf{N}\}$ is not a pseudorandom permutation generator.

Proof: Let $M_3 = M(h,g,f)$. Then we have $M_3(L,R) = (R \oplus f(L) \oplus g(R), *)$, where L and R are arbitrary vectors from I_n and $*$ denotes a string we do not care. Now we further assume that neither L nor R is 0. Then we have the following:

$$M_3(0,0) = (f(0) \oplus g(0), *),$$
$$M_3(L,0) = (f(L) \oplus g(0), *),$$
$$M_3(0,R) = (f(0) \oplus g(R) \oplus R, *),$$
$$M_3(L,R) = (f(L) \oplus g(R) \oplus R, *).$$

Adding together the left halves of the right-hand sides of the above four equations must give us 0. These observations indicate that we can construct an oracle circuit for $\{M(h,g,f)|h,g,f \in H_n\}$. The oracle circuit uses only four (4) oracle gates. When M_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 from H_{2n} is used in the oracle circuit, the probability for the oracle circuit to produce a bit 1 is $1/2^n$. This completes the proof. □

In our plain language, Theorem 5.1 states that a 3-round concatenation of MISTY-like transforms is not a pseudorandom permutation, even if the F-function in each round is chosen independently at random from H_n.

Remark 5.2: Theorem 5.1 is also implied by a more general result by Ohnishi [21] which states that the family of functions with a depth of at most one (e.g. $f(L) \oplus g(R) \oplus h(L \oplus R)$) is not a pseudorandom function generator. Thus, for pseudorandom function generation, functions must have a depth of at least two (e.g. $f(g(R))$).

For a 4-round concatenation of MISTY-like transforms, we have the following two results.

Theorem 5.3: $\{M(f,f^2,f,f)|h,g,f \in H_n, n \in \mathsf{N}\}$ is not a pseudorandom permutation generator.

Proof: To prove this theorem, we construct a oracle circuit for $\{M(f,f^2,f,f)|f \in H_n\}$ that uses two oracle gates. The detailed arrangement of the two oracles is obtained through the following two observations:

1. $M(f,f^2,f,f)$ always translates $(0,0)$ into $(f^3(0), f^3(0) \oplus f(0))$. Adding up the two halves gives us $f(0)$.
2. Now we have $(0, f(0))$, which will be translated by $M(f,f^2,f,f)$ into $(0,*)$.

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

Theorem 5.4: $\{M(f^{i+j},f^j,f^i,f^i)|f \in H_n, n \in \mathsf{N}\}$ is not a pseudorandom permutation generator, where i and j are integers larger than 0.

A proof for this theorem can be easily obtained by noting the fact that $M(f^{i+j},f^j,f^i,f^i)$ always translates $(0,0)$ into $(*,0)$, where $*$ as before means a string we do not care.

Based on Theorem 5.4, the following result on a 5-round concatenation of MISTY-like transforms can be obtained:

Theorem 5.5: $\{M(g,f^{i+j},f^j,f^i,f^i)|g,f \in H_n, n \in \mathsf{N}\}$ is not a pseudorandom permutation generator, where i and j are integers larger than 0.

The proof for Theorem 5.5 is surprisingly simple: $M(g,f^{i+j},f^j,f^i,f^i)$ always 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 $M(g,f,f,f)$, $M(f,g,f,f)$, $M(g,f,f,f,f)$, etc.

Finally we study the super pseudorandomness of MISTY-like transforms. Super pseudorandomness is a slightly stronger notion than that of pseudorandomness. It is defined by allowing an oracle circuit to contain also gates that computes the inverse of a permutation. The reader is directed to [13] for the precise definition of super pseudorandomness.

In the case of DES-like transforms, Luby and Rackoff showed the following result.

Theorem 5.6 [13]: $\{D(f_4,f_3,f_2,f_1)|f_4,f_3,f_2,f_1 \in H_n, n \in \mathsf{N}\}$ is a super pseudorandom permutation generator.

Our following result shows that, in the case of MISTY-like transforms, a 4-round concatenation is not adequate for achieving super pseudorandomness, although whether it yields a pseudorandom permutation generator still remains open,

Theorem 5.7: $\{M(f_4,f_3,f_2,f_1)|f_4,f_3,f_2,f_1 \in H_n, n \in \mathsf{N}\}$ is not a super pseudorandom permutation generator.

Proof: Let $M_4 = M(f_4,f_3,f_2,f_1)$ and M_4^{-1} the converse of M_4, namely, $M_4^{-1}(M_4(A,B)) = (A,B)$ for

all vectors $A, B \in I_n$. Given two vectors A and B, first compute $(X, Y) = M_4(A, B)$, then set $(C, D) = M_4^{-1}(X \oplus Z, Y \oplus Z)$ for an arbitrary $Z \in I_n$. Next compute $(U, V) = M_4(A, D)$ and $(S, T) = M_4(C, B)$. It is easy to check that the relation $U \oplus V = S \oplus T$ holds. This proves the theorem. □

5.2 Practical Consequences of Non-Randomness

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

Consider a 3-round concatenation of MISTY-like transforms $M(h, g, f)$. As we have shown in Theorem 5.1, it is not a pseudorandom permutation. Set $t(L, R)$ be the left half of output of $S_3(L, R)$. Then, the following relation holds:

$$t(L, R) = t(0, 0) \oplus t(L, 0) \oplus t(0, R).$$

More importantly, the following general relation holds:

$$t(L, R) = t(A, B) \oplus t(L, B) \oplus t(A, R).$$

This implies that the left half t has an algebraic structure which allows $t(L, R)$ to be computed from three encrypted data items $t(A, B), t(L, B)$ and $t(A, R)$ for any $A, B, L, R \in I_n$. Based on this property, one may launch a known-plaintext attack against a 3-round concatenation of MISTY-like transforms.

For a cipher to be secure, the above algebraic relation must be avoided. To see this point, we note that by using Luby and Rackoff's argument for Theorem 3.1, a cipher placed in the public domain which was based on 2-round DES-like transforms, has been shown to be insecure against a known-plaintext attack similar to the one described above. (For details see Pages 351-352 of [23].)

Though such an algebraic structure could disappear in the concatenation of four or more MISTY-like transforms, the F-function of a round (which is a MISTY-like transform) in the preliminary version of the MISTY cipher is defined as the concatenation of three smaller MISTY-like transforms. In other words, an "outer" F-function in the MISTY cipher is recursively constructed from three smaller MISTY-like transforms. Hence, the "outer" F-function has the algebraic structure explained above.

This structure could be used by a cryptanalyst and hence cast very serious doubts on the security of the MISTY cipher. Indeed the MISTY cipher may be immune against the differential or linear attack, however, the fact that the MISTY cipher adopts the concatenation of three smaller MISTY-like transforms in its "outer" F-functions could render the cipher vulnerable to other (chosen plaintext) attacks.

6. Concluding Remarks

Based on our studies, the following observations can be made:

1. In a number of cases, MISTY-like transforms do not yield a pseudorandom permutation, although similar iterations of DES-like transforms would result in pseudorandom permutations. Hence in all these cases DES-like transforms are superior to MISTY-like ones.
2. From the way a MISTY-like transform is defined, it is clear that for a cipher based on the transform to be efficiently decipherable, the F-function of a MISTY-like transform must be an efficiently invertible permutation. This in effect says that a F-functions of a MISTY-like transform must be a "smaller" cipher as well. Compared with DES-like transforms whose F-functions need not to be invertible, MISTY-like transforms obviously impose more stringent conditions on the design of their F-functions.

Future research topics include (1) to identify under what conditions MISTY-like transforms would yield a pseudorandom permutation, and (2) to compare the MISTY cipher with DES from the perspectives of other security criteria. In particular, concerning the first topic the following two concrete questions remain to be tackled:

(Q1) Is a 4-round concatenation of MISTY-like transforms $M(f_4, f_3, f_2, f_1)$ a pseudorandom permutation ?

(Q2) Is a 5-round concatenation of MISTY-like transforms $M(f_5, f_4, f_3, f_2, f_1)$ a super pseudorandom permutation ?

Concerning on the second topic, an interesting question is if there are any security criteria which would indicate the advantage of a MISTY-like transform over a DES-like transform.

A final remark is that a detailed description of the original algorithm in the preliminary version of the MISTY cipher [16] uses a 8-round concatenation of MISTY-like transforms, though no design criteria on this decision have been disclosed.

Acknowledgment

The authors would like to thank Toshiya Itoh who pointed out an error in an early version of Theorem 5.3. Thanks also go to the anonymous referees whose comments have improved the presentation of this paper.

References

[1] K. Aoki and K. Ohta, "Stricter evaluation for the maximum average of differential probability and the maximum average of linear probability," Proc. of the 1996 SCIS '96, Japan, 1996.

[2] E. Biham and A. Shamir, "Differential cryptanalysis of the Data Encryption Standard," Springer-Verlag, New York, 1993.

[3] M. Bellare, R. Guérin, and P. Rogaway, "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.

[4] M. Bellare, J. Kilian, and P. Rogaway, "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.

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

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

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

[8] H. Feistel, "Cryptography and computer privacy," in Scientific American, vol.228, pp.15–23, 1973.

[9] H. Feistel, W.A. Notz, and J.L. Smith, "Some cryptographic techniques for machine-to-machine data communications," Proc. IEEE, vol.63, no.11, pp.1545–1554, 1975.

[10] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," JACM, vol.33, no.4, pp.792–807, 1986.

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

[12] X. Lai, "Higher order derivatives and differential cryptanalysis," Proc. Commun. Coding and Cryptography, Feb. 1994.

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

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

[15] M. Matsui, "On provably security of block ciphers against differential and linear cryptanalysis," Proc. of SITA '95, 1995.

[16] M. Matsui, "New structure of block cipher with provable security against differential and linear cryptanalysis," in 3rd Fast Software Encryption, Cambridge, U.K., Lecture Notes in Computer Science 1039, pp.205–218, Springer-Verlag, Berlin, 1996.

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

[18] K. Nyberg and L.R. Knudsen, "Provable security against a differential attacks," J. Cryptology, vol.8, pp.27–37, 1995.

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

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

[21] Y. Ohnishi, "A study on data security," Master Thesis, Tohoku University, Japan, March 1988.

[22] J. Pieprzyk, "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.

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

[24] B. Sadeghiyan and J. Pieprzyk, "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.

[25] Y. Zheng, T. Matsumoto, and H. Imai, "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.

[26] Y. Zheng, T. Matsumoto, and H. Imai, "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.

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

Kouichi Sakurai was born in Fukuoka, Japan on July 31, 1963. He received the B.S. degree in mathematics from Faculty of Science, Kyushu University and the M.S. degree in applied since from Faculty of Engineering, Kyushu University in 1986 and 1988, respectively. He had been engaged in the research and development on cryptography and information security at Computer & Information Systems Laboratory at Mitsubishi Electric Corporation from 1988 to 1994. He received the Dr. degree in engineering from Faculty of Engineering, Kyushu University in 1993. Since 1994, he has been working for department of computer science of Kyushu University as an associate professor. His current research interests are cryptography and computational complexity. Dr. Sakurai is a member of the Information Processing Society of Japan, the Mathematical Society of Japan and the International Association for Cryptologic Research.

Eaddress: sakurai@csce.kyushu-u.ac.jp

Yuliang Zheng received his B.Sc. degree in computer science from Southeast University (formerly Nanjing Institute of Technology), Nanjing, China, in 1982, and the M.E. and Ph.D. degrees, both in electrical and computer engineering, from Yokohama National University, Yokohama, Japan, in 1988 and 1991 respectively. From 1982 to 1984 he was with the Guangzhou Research Institute for Communications, Guangzhou (Canton), China, and from February 1991 to January 1992 he was a Post-Doctoral Fellow at the Computer Science Department, University College, University of New South Wales, in Canberra, Australia. From February 1992 to January 1995 he was a Lecturer of the Computer Science Department, University of Wollongong. Since February 1995 he has been a Senior Lecturer at the Peninsula School of Computing and Information Technology, Monash University, in Melbourne. His current research interests include information security, cryptography, computational complexity theory and information theory. Dr. Zheng is a member of IACR, ACM and IEEE. He has a homepage at http://pscit-www.fcit.monash.edu.au:/ yuliang/.