Pseudorandomness of Basic Structures in the Block Cipher KASUMI

Ju-Sung Kang, Bart Preneel, Heuisu Ryu, Kyo Il Chung, and Chee Hang Park

The notion of pseudorandomness is the theoretical foundation on which to consider the soundness of a basic structure used in some block ciphers. We examine the pseudorandomness of the block cipher KASUMI, which will be used in the next-generation cellular phones. First, we prove that the four-round unbalanced MISTY-type transformation is pseudorandom in order to illustrate the pseudorandomness of the inside round function *FI* of KASUMI under an adaptive distinguisher model. Second, we show that the three-round KASUMI-like structure is not pseudorandom but the four-round KASUMI-like structure is pseudorandom under a non-adaptive distinguisher model.

I. INTRODUCTION

A block cipher is a family of permutations on a message space indexed by a secret key. Luby and Rackoff [1] introduced a theoretical model for the security of block ciphers by using the notion of pseudorandom and super-pseudorandom permutations. A pseudorandom permutation can be interpreted as a block cipher that cannot be distinguished from a truly random permutation regardless of how many polynomial encryption queries an attacker makes. A super-pseudorandom permutation can be interpreted as a block cipher that cannot be distinguished from a truly random permutation regardless of how many polynomial encryption and decryption queries an attacker makes.

Luby and Rackoff used a Feistel-type transformation defined by the typical two-block structure of the block cipher DES in order to construct pseudorandom and super-pseudorandom permutations from pseudorandom functions [1]. They showed that the Feistel-type transformation with three rounds yields a $2n$-bit pseudorandom permutation and with four rounds it yields a $2n$-bit super-pseudorandom permutation under the assumption that each round function is an n-bit pseudorandom function. Patarin [2] proved that one could obtain similar results by using only a single pseudorandom function. Naor and Reingold [3] revisited the revised constructions of Luby and Rackoff and simplified their proofs of security.

There were also some noticeable results for the pseudorandomness of a MISTY-type transformation defined by another typical two-block structure of the block cipher MISTY [4], [5] different from the Feistel-type. Sakurai and Zheng [6] showed that the three-round MISTY-type transformation does not give a pseudorandom permutation and the four-round does not give a super-pseudorandom

Manuscript received Mar. 22, 2002; revised Feb. 3, 2003.

Ju-Sung Kang (phone: +82 42 860 5326, e-mail: jskang@etri.re.kr), Heuisu Ryu (e-mail: hsryu@etri.re.kr), Kyo Il Chung (e-mail: kyoil@etri.re.kr), and Chee Hang Park (e-mail: chpark@etri.re.kr) are with Information Security Technology Division, ETRI, Daejeon, Korea.

Bart Preneel (e-mail: Bart.Preneel@esat.kuleuven.ac.be) is with the Electrical Engineering Department, Kathorieke Universitat Leuven, Belgium.

permutation. Gilbert and Minier [7] and Kang et al. [8] showed independently that the four-round MISTY-type transformation yields a pseudorandom permutation. Iwata et al. [9] and Gilbert and Minier [7] also independently proved that the five-round MISTY-type yields a super-pseudorandom permutation. Recently, Iwata et al. [10] provided an improved result on the super-pseudorandomness of the MISTY-type transformation by proving that the second round permutation in the five-round MISTY-type transformation did not need to be cryptographic at all.

The overall structure of KASUMI [11] is of a Feistel-type, but its round function *FO* is composed of a three-round MISTY-type transformation; this is not a pseudorandom function according to the result in [6]. Thus, we cannot straightforwardly apply the Luby-Rackoff result to KASUMI. The *FO* function within KASUMI has the *FI* function as its component function; it consists of a four-round unbalanced MISTY-type transformation. We show that the structure of the *FI* function is a pseudorandom permutation. Based on the pseudorandomness of the *FI* function, we prove that the three-round KASUMI-like structure is not a pseudorandom permutation, but a four-round KASUMI-like structure is a pseudorandom permutation.

A KASUMI-like structure is a mixed structure, while Feistel-type and MISTY-type transformations are compounded. In this paper, we define a KASUMI-like structure as a simplified $4n$-bit block structure with its round functions being n-bit permutations. In order to investigate the properties of the round function, we consider a security model for adaptive distinguishers similar to that in the approach of Naor and Reingold [3]. This provides more detail than previous results such as [7] and [8]. However we consider the non-adaptive distinguisher model to examine the pseudorandomness of the overall KASUMI-like structure, since under the adaptive distinguisher model there are so many factors involved in controlling a $4n$-bit block structure. We found some flaws in the proof of Theorem 1 of [12] and revise them in this paper.

Within the security architecture of the 3rd Generation Partnership Project (3GPP) system [11], there are two standardized functions, the confidentiality function $f8$ and the integrity function $f9$. These two functions are based on the block cipher KASUMI [11]. Thus, the pseudorandomness of KASUMI is the main assumption on which to examine the provable security of $f8$ and $f9$ [13], [14]. The results of this paper provide support for this assumption.

An analysis of pseudorandomness does not directly lead to an attack or a proof of security for the block cipher itself, since the security is asymptotically evaluated in terms of its block size, and the attacker's information is limited to a number of queries and computational time that is polynomial in its block size. The pseudorandomness criteria can be used in the theoretical study of the soundness of a basic structure used in some block ciphers.

On the other hand, Knudsen [15] proved that any Feistel cipher with a bijective round function has the impossible characteristics of five rounds, which allows us to distinguish the five-round cipher from a randomly chosen permutation. Recently, Patarin [16] also discussed a generic distinguishing attack on five-round Feistel-type permutations. This distinguishing attack can be applied to KASUMI since the round functions *FO* and *FL* are permutations. Patarin's attack requires $O(2^{3n/2})$ chosen plaintext/ciphertext pairs and $O(2^{3n/2})$ computations to distinguish a five-round $2n$-bit Feistel-type permutation from a $2n$-bit random permutation. The mixed $4n$-bit block KASUMI-like structure, which is studied in this paper, is different from the $2n$-bit block Feistel-type structure, so the structures of Patarin's attack and our analysis are different from each other. Note that the number of queries in the practical distinguishing attack is exponential in its block size. This point is different from an analysis of pseudorandomness.

II. THE BLOCK CIPHER KASUMI

The block cipher KASUMI [11] produces a 64-bit output from a 64-bit input under the control of a 128-bit key. KASUMI is a modified version of the block cipher MISTY1 [5], and we can classify the structure of KASUMI into the following three stages:

- The overall structure of KASUMI is a 64-bit permutation composed of eight rounds of a Feistel-type permutation. The round function consists of a non-linear mixing function *FO* and a linear mixing function *FL*.
- The *FO* function is a 32-bit permutation composed of three rounds of a MISTY-type transformation with round permutation *FI*.
- The *FI* function is a 16-bit permutation which is composed of a four-round unbalanced MISTY-type transformation obtained from the 7-bit S-box *S*7 and the 9-bit S-box *S*9.

The structure of KASUMI is depicted in Fig. 1.

A security evaluation of KASUMI was primarily performed by the 3GPP Security Algorithms Group of Experts (SAGE) [17]. The general conclusion of [17] was that KASUMI is based on sound design principles and no practical attacks were found. We believe that the notion of pseudorandomness is theoretical evidence of the soundness of the basic structure of a block cipher. However there was no mention in [17] about the pseudorandomness criteria. This provided the motivation of our study, in which we examine the pseudorandomness of the block structures used in KASUMI.

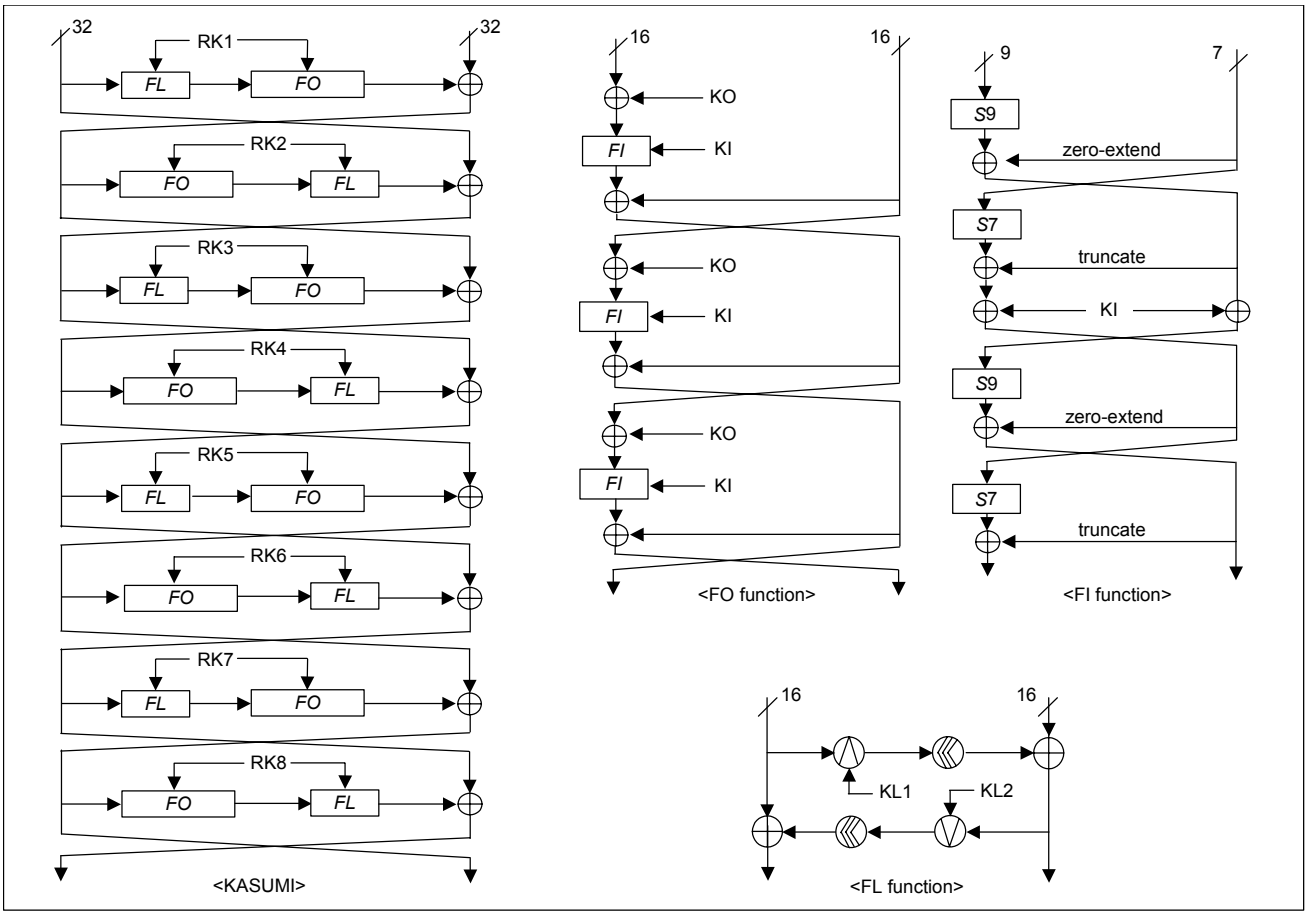

Fig. 1. Structure of KASUMI.

Kühn [18] showed that KASUMI with six rounds can be breakable by impossible differential attack with complexity of 2^{55} data and 2^{100} times, which is less than an exhaustive search. Kühn's attack shows that KASUMI with six rounds is not practically secure, whereas we theoretically show that the simplified KASUMI with four rounds is pseudorandom where the number of queries is polynomially bounded.

III. PRELIMINARIES FOR PSEUDORANDOMNESS

Let I_n denote the set of all *n*-bit strings and Ω_n be the set of all permutations from I_n to itself where n is a positive integer, that is, $\Omega_n = \{\pi : I_n \to I_n \mid \pi \text{ is a bijection}\}$. We define an *n*-bit perfect random permutation as a uniformly drawn element of Ω_n.

Definition 1. Ω_n is called the uniform permutation ensemble (UPE) if all permutations in Ω_n are uniformly distributed, that is, for any permutation $\pi \in \Omega_n$, $\Pr(\pi) = 1/(2^n!)$.

We consider the following security model. Let D be a computationally unbounded distinguisher with an oracle O. The oracle O chooses randomly a permutation π from the UPE Ω_n or from a permutation ensemble $\Lambda_n \subset \Omega_n$. For an n-bit block cipher, Λ_n is the multiset of permutations determined by all the secret keys. Since two or more different keys may define the same permutation, here we use the term multiset in which some elements can be found two or more times. The purpose of the distinguisher D is to distinguish whether the oracle O implements the UPE Ω_n or Λ_n.

Definition 2. Let D be a distinguisher, Ω_n be the UPE, and Λ_n be a permutation ensemble obtained from a block cipher. Then the advantage ADV_D of D is defined by

$$ADV_D = \left| \Pr(D \text{ outputs } 1 \mid O \leftarrow \Omega_n) - \Pr(D \text{ outputs } 1 \mid O \leftarrow \Lambda_n) \right|,$$

where $O \leftarrow \Omega_n$ and $O \leftarrow \Lambda_n$ denote that O implements Ω_n and Λ_n, respectively.

Assume that the distinguisher D is restricted to make at most $poly(n)$ queries to the oracle O, where $poly(n)$ is

some polynomial in n. We call D a pseudorandom distinguisher if it queries x and the oracle answers $y = \pi(x)$, where π is a randomly chosen permutation by O. We say that D is a super-pseudorandom distinguisher if it is a pseudorandom distinguisher and it also can make a query y and receives $x = \pi^{-1}(y)$ from the oracle O.

Definition 3. A function $h : N \to \Re$ is called negligible if for any constant $c > 0$ and all sufficiently large $n \in N$, $h(n) < 1/n^c$.

Definition 4. Let Λ_n be an efficiently computable permutation ensemble. Then Λ_n is called a pseudorandom permutation ensemble (PPE) if ADV_D is negligible for any pseudorandom distinguisher D.

Definition 5. Let Λ_n be an efficiently computable permutation ensemble. Then we call Λ_n a super-pseudorandom permutation ensemble (SPPE) if ADV_D is negligible for any super-pseudorandom distinguisher D.

In Definition 4 and 5, a permutation ensemble is efficiently computable if all permutations in the ensemble can be computed efficiently. See [3] for a rigorous definition of this. It is reasonable to assume that Λ_n is an efficiently computable permutation ensemble if it is obtained from an n-bit block cipher. Hence we assume that any permutation ensemble obtained from a block cipher is efficiently computable. Now we define a family of permutations to be (q, a)-secure in order to make a clear description of our results.

Definition 6. Let Λ_n be an efficiently computable permutation ensemble. Then Λ_n is a (q, a)-secure PPE, if the distinguisher D asks at most q queries, which are restricted to $ADV_D \le a$.

We define two transformations, Feistel-type and MISTY-type, which are obtained from two representative structures of current block ciphers. Let Ψ_n denote the set of all functions from I_n to itself. We say f is an n-bit function (resp. permutation) where $f \in \Psi_n$ (resp. $f \in \Omega_n$).

Definition 7. For any n-bit function $f \in \Psi_n$, the $2n$-bit Feistel-type permutation $F_f \in \Omega_{2n}$ is defined by

$$F_f(L, R) = (R, L \oplus f(R)),$$

where $L, R \in I_n$.

Definition 8. For any n-bit function $f \in \Omega_n$, the $2n$-bit MISTY-type permutation $M_f \in \Omega_{2n}$ is defined by

$$M_f(L, R) = (R, f(L) \oplus R),$$

where $L, R \in I_n$.

Now we can formally describe several important results on the pseudorandomness of Feistel-type and MISTY-type transformations. Note that a pseudorandom function ensemble (PFE) can be similarly defined as in Definition 4 by considering a function space instead of a permutation space.

- $F_{f_2} \circ F_{f_1}$ is not a $2n$-bit PPE and $F_{f_3} \circ F_{f_2} \circ F_{f_1}$ is not a $2n$-bit SPPE, even if all f_i's ($i = 1,2,3$) are independently chosen from an n-bit PFE [1].
- $F_{f_3} \circ F_{f_2} \circ F_{f_1}$ is a $2n$-bit PPE and $F_{f_4} \circ F_{f_3} \circ F_{f_2} \circ F_{f_1}$ is a $2n$-bit SPPE if all f_i's ($i = 1,2,3,4$) are independently chosen from an n-bit PFE [1].
- $M_{f_3} \circ M_{f_2} \circ M_{f_1}$ is not a $2n$-bit PPE and $M_{f_4} \circ M_{f_3} \circ M_{f_2} \circ M_{f_1}$ is not a $2n$-bit SPPE, even if each f_i ($i = 1,2,3,4$) is chosen independently from an n-bit PPE [6], [7].
- $M_{f_4} \circ M_{f_3} \circ M_{f_2} \circ M_{f_1}$ is a $2n$-bit PPE and $M_{f_5} \circ M_{f_4} \circ M_{f_3} \circ M_{f_2} \circ M_{f_1}$ is a $2n$-bit SPPE, where all f_i's ($i = 1,2,3,4,5$) are independently chosen from an n-bit PPE [7]-[9].

We first show that the structure of the *FI* function of KASUMI is a PPE by examining the pseudorandomness of an unbalanced MISTY-type transformation. Second, on the basis of the first result, we prove that a three-round KASUMI-like structure is not a PPE but a four-round KASUMI-like structure is a PPE. Note that the structure of the *FO* function of KASUMI is not a PPE, so it seems that unlike the Luby-Rackoff cipher, the three-round Feistel-type permutation of a KASUMI-like structure is not a PPE. Since the *FL* function is used to mix in the round key, we consider in this paper a simplified version of KASUMI without the *FL* function.

IV. PSEUDORANDOMNESS OF THE UNBALANCED MISTY-TYPE TRANSFORMATION

We describe two simple but useful lemmas, the proofs of which are given in [8].

Lemma 1. Let π be a permutation chosen from the UPE Ω_n. Then for any $x_1 \ne x_2$, $y \in I_n$,

$$\Pr(\pi(x_1) \oplus \pi(x_2) = y) = \begin{cases} 1/(2^n - 1) & \text{if } y \ne 0, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 2. Let π_1 and π_2 be two permutations independently chosen from the UPE Ω_n. Then for any a, b, c, d, $y \in I_n$,

$$\Pr(\pi_1(a) \oplus \pi_1(b) \oplus \pi_2(c) \oplus \pi_2(d) = y) < \frac{1}{2^{n-1}},$$

for $n \ge 2$.

Now we define two unbalanced MISTY-type transformations in order to examine accurately the pseudorandomness of the *FI* function.

Definition 9. Let n and m be two positive integers such that $m \le n$. Then for any n-bit permutation f and m-bit permutation g, two $(n+m)$-bit unbalanced MISTY-type transformations $\overline{M}_f \in \Omega_{n+m}$ and $\hat{M}_g \in \Omega_{n+m}$ are defined for any $(L,R) \in I_n \times I_m$,

$$\text{by} \quad \overline{M}_f(L,R) = (R, f(L) \oplus \overline{R}) \in I_m \times I_n,$$

and for any $(L,R) \in I_m \times I_n$,

$$\text{by} \quad \hat{M}_g(L,R) = (R, g(L) \oplus \hat{R}) \in I_n \times I_m$$

where for any n-bit vector x, $\hat{x}$ denotes the m-bit value obtained by discarding the n-m leftmost bits and for any m-bit vector y, $\overline{y}$ denotes the n-bit value obtained by adding n-m zero bits to the left.

Note that the *FI* function of KASUMI can be represented as a 16-bit permutation $\hat{M}_{f_4} \circ \overline{M}_{f_3} \circ \hat{M}_{f_2} \circ \overline{M}_{f_1}$, where f_1, f_3 are 9-bit permutations and f_2, f_4 are 7-bit permutations. We define the permutation ensemble based on the *FI* function as follows.

Definition 10. Λ_{n+m} is the $(n+m)$-bit permutation ensemble obtained from the four-round unbalanced MISTY-type transformation $\hat{M}_{f_4} \circ \overline{M}_{f_3} \circ \hat{M}_{f_2} \circ \overline{M}_{f_1}$, where $f_1, f_3 \in \Omega_n$ and $f_2, f_4 \in \Omega_m$ are independently chosen from the n-bit and m-bit UPEs, respectively.

The pseudorandomness of the *FI* function is guaranteed by the following theorem.

Theorem 1. Let for any positive integers n and m with $2 \le m \le n$, $f_1, f_3 \in \Omega_n$, and $f_2, f_4 \in \Omega_m$ be independently chosen from two n-bit and m-bit PPEs, respectively. Then the four-round unbalanced MISTY-type transformation $\hat{M}_{f_4} \circ \overline{M}_{f_3} \circ \hat{M}_{f_2} \circ \overline{M}_{f_1}$ is a (q,a)-secure PPE, where

$$a = \frac{q^2 - q}{2}\left(\frac{3}{2^{n-1}} + \frac{12}{2^m - 1}\right).$$

Recall that a pseudorandom distinguisher D can make a query x and the oracle O answers $y = \pi(x)$, where π is a randomly chosen permutation by O. Now we assume that D makes exactly q queries and refer to the sequence $\{(x^{(1)}, y^{(1)}), \ldots, (x^{(q)}, y^{(q)})\}$ of all query-answer pairs as the D-transcript, where $q = poly(n)$. We consider the following adaptive pseudorandom distinguisher.

Definition 11. D is called an adaptive pseudorandom distinguisher if it has a transcript $\{(x^{(1)}, y^{(1)}), \ldots, (x^{(q)}, y^{(q)})\}$ and a function C_D of the D-transcript such that for every $2 \le i \le q$,

$$x^{(i)} = C_D(\{(x^{(1)}, y^{(1)}), \ldots, (x^{(i-1)}, y^{(i-1)})\})$$

and the output of $D = C_D(\{(x^{(1)}, y^{(1)}), \ldots, (x^{(q)}, y^{(q)})\})$.

Under the adaptive distinguisher model, the *i*-th query of *D* is determined by the first *i*–1 query-answer pairs and *D*'s output is a function of its transcript. Throughout this paper we assume that all queries are distinct.

For the proof of Theorem 1, we consider an $(n+m)$-bit ensemble B_{n+m} on the *i*-th query $x^{(i)} \in I_{n+m}$ of D, when the oracle O implements B_{n+m}, its corresponding answer $y^{(i)} = (y_L^{(i)}, y_R^{(i)}) \in I_n \times I_m$ is as follows:

1. $y^{(i)}$ is the uniformly chosen $(n+m)$-bit vector under the condition that $y^{(i)} \ne y^{(j)}$ for all $1 \le j < i$.
2. $y_L^{(i)} \ne y_L^{(j)}$, $y_L^{(i)} \ne y_L^{(j)}$, and $\hat{y}_L^{(i)} \oplus y_R^{(i)} \ne \hat{y}_L^{(j)} \oplus y_R^{(j)}$ for all $1 \le j < i$.

Definition 12. Let $\sigma = \{(x^{(1)}, y^{(1)}), \ldots, (x^{(q)}, y^{(q)})\}$ be a D-transcript.

(i) σ is called separately distinct if $y_L^{(i)} \ne y_L^{(j)}$ and $y_L^{(i)} \ne y_L^{(j)}$ for all $1 \le i \ne j \le q$.
(ii) σ is called XOR-distinct if $\hat{y}_L^{(i)} \oplus y_R^{(i)} \ne \hat{y}_L^{(j)} \oplus y_R^{(j)}$ for all $1 \le i \ne j \le q$.

Note that the UPE Ω_{n+m} can provide answers that are not separately distinct or not XOR-distinct, but B_{n+m} always provides answers that are separately distinct and XOR-distinct.

We first prove that the advantage of D in distinguishing between the process UPE Ω_{n+m} and the process B_{n+m} is negligible. The next step of the proof will be an estimation for the advantage of D in distinguishing between the process B_{n+m} and the process Λ_{n+m}. Now we consider the different distributions on the transcript of D induced by different ensembles which are implemented by the oracle O.

Definition 13. $T_{\Omega_{n+m}}$, $T_{B_{n+m}}$, and $T_{\Lambda_{n+m}}$ are defined by the following random variables: $T_{\Omega_{n+m}}$ is the D-transcript when the oracle O implements the UPE Ω_{n+m}, $T_{B_{n+m}}$ is the D-transcript when the oracle O implements B_{n+m}, and $T_{B_{n+m}}$ is the D-transcript when the oracle O implements Λ_{n+m}, respectively.

The following lemma confirms that the advantage of D in distinguishing between the process UPE Ω_{n+m} and the

process B_{n+m} is small enough.

Lemma 3.

$$|\Pr(C_D(T_{\Omega_{n+m}})=1)-\Pr(C_D(T_{B_{n+m}})=1)| < \frac{q^2-q}{2}\left(\frac{1}{2^n-1}+\frac{2}{2^m-1}\right).$$

Proof. Let $G(T_{\Omega_{n+m}})$ be the event of $T_{\Omega_{n+m}}$ being separately distinct and XOR-distinct. Then for any separately distinct and XOR-distinct D-transcript σ,

$$\Pr(T_{\Omega_{n+m}}=\sigma \mid G(T_{\Omega_{n+m}})) = \frac{(2^{n+m}-q)!}{2^{n+m}!}$$

and

$$\Pr(T_{B_{n+m}}=\sigma) = \frac{1}{2^{n+m}(2^{n+m}-1)\cdots(2^{n+m}-q+1)}.$$

Hence the distribution of $T_{\Omega_{n+m}}$ conditioned on $T_{\Omega_{n+m}}$ being separately distinct and XOR-distinct is exactly the distribution of $T_{B_{n+m}}$. Furthermore, we can estimate the probability of the event $G(T_{\Omega_{n+m}})^c$, the complement of $G(T_{\Omega_{n+m}})$, as follows:

$$\begin{aligned}
&\Pr(G(T_{\Omega_{n+m}})^c)\\
&= \Pr\Big(y_L^{(i)}=y_L^{(j)} \text{ or } y_R^{(i)}=y_R^{(j)} \text{ or }\\
&\qquad \hat{y}_L^{(i)}\oplus y_R^{(i)}=\hat{y}_L^{(j)}\oplus y_R^{(j)} \text{ for some } 1\le i\ne j\le q\Big)\\
&\le \sum_{i\ne j}\Big\{\Pr(y_L^{(i)}=y_L^{(j)})+\Pr(y_R^{(i)}=y_R^{(j)})\\
&\qquad +\Pr(\hat{y}_L^{(i)}\oplus y_R^{(i)}=\hat{y}_L^{(j)}\oplus y_R^{(j)})\Big\}\\
&= \binom{q}{2}\left(\frac{2^m-1}{2^{n+m}-1}+\frac{2^n-1}{2^{n+m}-1}+\frac{2^n-1}{2^{n+m}-1}\right)\\
&< \frac{q^2-q}{2}\left(\frac{1}{2^n-1}+\frac{2}{2^m-1}\right).
\end{aligned}$$

Therefore the assertion follows by

$$\begin{aligned}
&|\Pr(C_D(T_{\Omega_{n+m}})=1)-\Pr(C_D(T_{B_{n+m}})=1)|\\
&\le \Pr(G(T_{\Omega_{n+m}}))\\
&\quad\cdot\left|\Pr(C_D(T_{\Omega_{n+m}})=1\middle|G(T_{\Omega_{n+m}}))-\Pr(C_D(T_{B_{n+m}})=1)\right|\\
&\quad+\Pr(G(T_{\Omega_{n+m}})^c)\\
&\qquad\cdot\left|\Pr(C_D(T_{\Omega_{n+m}})=1\middle|G(T_{\Omega_{n+m}})^c)-\Pr(C_D(T_{B_{n+m}})=1)\right|\\
&\le \Pr(G(T_{\Omega_{n+m}})^c)\\
&< \frac{q^2-q}{2}\left(\frac{1}{2^n-1}+\frac{2}{2^m-1}\right).
\end{aligned}$$

□

We now have to show that the advantage of D in distinguishing between B_{n+m} and Λ_{n+m} is also small enough. To prove this fact, we first formally define a bad event and estimate its probability.

Definition 14. For any n-bit permutation f_1 and m-bit permutation f_2, $BAD(f_1,f_2)$ is defined as the set of all D-transcripts $\sigma=\{(x^{(1)},y^{(1)}),\ldots,(x^{(q)},y^{(q)})\}$ satisfying, for some $1\le i\ne j\le q$,

$$f_1(x_L^{(i)})\oplus\bar{x}_R^{(i)}=f_1(x_L^{(j)})\oplus\bar{x}_R^{(j)}$$

or

$$f_2(x_R^{(i)})\oplus\hat{f}_1(x_L^{(i)})\oplus x_R^{(i)}=f_2(x_R^{(j)})\oplus\hat{f}_1(x_L^{(j)})\oplus x_R^{(j)}$$

or

$$\begin{aligned}
&y_L^{(i)}\oplus\bar{f}_2(x_R^{(i)})\oplus f_1(x_L^{(i)})\oplus\bar{x}_R^{(i)}\\
&=y_L^{(j)}\oplus\bar{f}_2(x_R^{(j)})\oplus f_1(x_L^{(j)})\oplus\bar{x}_R^{(j)},
\end{aligned}$$

where $x^{(i)}=(x_L^{(i)},x_R^{(i)})\in I_n\times I_m$ for all $1\le i\le q$.

Lemma 4. Let f_1 and f_2 be chosen independently from UPE Ω_n and UPE Ω_m, respectively. Then for any D-transcript $\sigma=\{(x^{(1)},y^{(1)}),\ldots,(x^{(q)},y^{(q)})\}$ and $n\ge m\ge 2$,

$$\Pr(\sigma\in BAD(f_1,f_2)) < (q^2-q)\left(\frac{1}{2^n}+\frac{1}{2^{m-1}}\right).$$

Proof. By definition, $\sigma\in BAD(f_1,f_2)$ if there exists $1\le i\ne j\le q$ such that

$$f_1(x_L^{(i)})\oplus\bar{x}_R^{(i)}=f_1(x_L^{(j)})\oplus\bar{x}_R^{(j)}$$

or

$$f_2(x_R^{(i)})\oplus\hat{f}_1(x_L^{(i)})\oplus x_R^{(i)}=f_2(x_R^{(j)})\oplus\hat{f}_1(x_L^{(j)})\oplus x_R^{(j)}$$

or

$$\begin{aligned}
&y_L^{(i)}\oplus\bar{f}_2(x_R^{(i)})\oplus f_1(x_L^{(i)})\oplus\bar{x}_R^{(i)}\\
&=y_L^{(j)}\oplus\bar{f}_2(x_R^{(j)})\oplus f_1(x_L^{(j)})\oplus\bar{x}_R^{(j)}.
\end{aligned}$$

For any fixed $i\ne j$, we estimate probabilities of these three events. We have the following three cases.

Case 1: $x_L^{(i)}\ne x_L^{(j)}$ and $x_R^{(i)}=x_R^{(j)}$. Since f_1 is a permutation,

$$\begin{aligned}
&\Pr\left(f_1(x_L^{(i)})\oplus\bar{x}_R^{(i)}=f_1(x_L^{(j)})\oplus\bar{x}_R^{(j)}\right)\\
&\quad=\Pr\left(f_1(x_L^{(i)})=f_1(x_L^{(j)})\right)=0.
\end{aligned}$$

Observe that, by a similar result to Lemma 1,

$$\Pr\Big(f_2(x_R^{(i)}) \oplus \hat{f}_1(x_L^{(i)}) \oplus x_R^{(i)} = f_2(x_R^{(j)}) \oplus \hat{f}_1(x_L^{(j)}) \oplus x_R^{(j)}\Big)$$
$$= \Pr\big(\hat{f}_1(x_L^{(i)}) = \hat{f}_1(x_L^{(i)})\big) = 2^n \cdot \frac{2^{n-m}\cdot(2^n-2)!}{2^n!} = \frac{2^{n-m}}{2^n-1}.$$

If $y_L^{(i)} = y_L^{(j)}$, then

$$\Pr\Big(y_L^{(i)} \oplus \bar{f}_2(x_R^{(i)}) \oplus f_1(x_L^{(i)}) \oplus \bar{x}_R^{(i)} = y_L^{(j)} \oplus \bar{f}_2(x_R^{(j)}) \oplus f_1(x_L^{(j)}) \oplus \bar{x}_R^{(j)}\Big)$$
$$= \Pr\big(f_1(x_L^{(i)}) = f_1(x_L^{(j)})\big) = 0.$$

Otherwise, that is, if $y_L^{(i)} \neq y_L^{(j)}$, by Lemma 1,

$$\Pr\Big(y_L^{(i)} \oplus \bar{f}_2(x_R^{(i)}) \oplus f_1(x_L^{(i)}) \oplus \bar{x}_R^{(i)} = y_L^{(j)} \oplus \bar{f}_2(x_R^{(j)}) \oplus f_1(x_L^{(j)}) \oplus \bar{x}_R^{(j)}\Big)$$
$$= \Pr\Big(f_1(x_L^{(i)}) \oplus f_1(x_L^{(j)}) = y_L^{(i)} \oplus y_L^{(j)}\Big) = \frac{1}{2^n-1}.$$

Case 2: $x_L^{(i)} = x_L^{(j)}$ and $x_R^{(i)} \neq x_R^{(j)}$. In this case the probability of the first event is equal to $\Pr\big(x_R^{(i)} = x_R^{(j)}\big) = 0$. By Lemma 1, the probability of the second event is estimated as

$$\Pr\Big(f_2(x_R^{(i)}) \oplus f_2(x_R^{(j)}) = x_R^{(i)} \oplus x_R^{(j)}\Big) = \frac{1}{2^m-1}.$$

If $y_L^{(i)} = y_L^{(j)}$, the probability of the third event is also equal to

$$\Pr\Big(f_2(x_R^{(i)}) \oplus f_2(x_R^{(j)}) = x_R^{(i)} \oplus x_R^{(j)}\Big) = \frac{1}{2^m-1}.$$

Otherwise, the probability of the third event is equal to

$$\Pr\Big(\bar{f}_2(x_R^{(i)}) \oplus \bar{f}_2(x_R^{(j)}) = \bar{x}_R^{(i)} \oplus \bar{x}_R^{(j)} \oplus y_L^{(i)} \oplus y_L^{(j)}\Big) = \frac{1}{2^m-1}\cdot\frac{1}{2^{n-m}}.$$

Case 3: $x_L^{(i)} \neq x_L^{(j)}$ and $x_R^{(i)} \neq x_R^{(j)}$. By Lemma 1, the probability of the first event is estimated as

$$\Pr\Big(f_1(x_L^{(i)}) \oplus f_1(x_L^{(j)}) = x_L^{(i)} \oplus x_L^{(j)}\Big) = \frac{1}{2^n-1}.$$

Similarly, by Lemma 2, the probability of the second event is also estimated as

$$\Pr\Big(\hat{f}_1(x_L^{(i)}) \oplus \hat{f}_1(x_L^{(j)}) \oplus f_2(x_R^{(i)}) \oplus f_2(x_R^{(j)}) = x_R^{(i)} \oplus x_R^{(j)}\Big) < \frac{1}{2^{m-1}},$$

since $n \geq m \geq 2$. If $y_L^{(i)} = y_L^{(j)}$, by Lemma 2, the probability of the third event is estimated as

$$\Pr\Big(f_1(x_L^{(i)}) \oplus f_1(x_L^{(j)}) \oplus \bar{f}_2(x_R^{(i)}) \oplus \bar{f}_2(x_R^{(j)}) = \bar{x}_R^{(i)} \oplus \bar{x}_R^{(j)}\Big) < \frac{1}{2^{m-1}}.$$

If $y_L^{(i)} \neq y_L^{(j)}$, the probability of the third event is also bounded above by $1/2^{m-1}$.

Therefore, for any case, we obtain that

$$\Pr\Big(f_1(x_L^{(i)}) \oplus \bar{x}_R^{(i)} = f_1(x_L^{(j)}) \oplus \bar{x}_R^{(j)}\Big) < \frac{1}{2^{n-1}},$$

$$\Pr\Big(f_2(x_R^{(i)}) \oplus \hat{f}_1(x_L^{(i)}) \oplus x_R^{(i)} = f_2(x_R^{(j)}) \oplus \hat{f}_1(x_L^{(j)}) \oplus x_R^{(j)}\Big) < \frac{1}{2^{m-1}},$$

and

$$\Pr\Big(y_L^{(i)} \oplus \bar{f}_2(x_R^{(i)}) \oplus f_1(x_L^{(i)}) \oplus \bar{x}_R^{(i)} = y_L^{(j)} \oplus \bar{f}_2(x_R^{(j)}) \oplus f_1(x_L^{(j)}) \oplus \bar{x}_R^{(j)}\Big) < \frac{1}{2^{m-1}}.$$

Hence

$$\Pr(\sigma \in BAD(f_1, f_2)) < \binom{q}{2}\left(\frac{1}{2^{n-1}} + \frac{2}{2^{m-1}}\right) = (q^2-q)\left(\frac{1}{2^n} + \frac{1}{2^{m-1}}\right).$$

□

Throughout this section we assume that $n \geq m \geq 2$ for the sake of freely using Lemma 4.

Lemma 5. For any XOR-distinct *D*-transcript $\sigma = \{(x^{(1)}, y^{(1)}), \ldots, (x^{(q)}, y^{(q)})\}$,

$$\Pr\big(T_{\Lambda_{n+m}} = \sigma \mid \sigma \notin BAD(f_1, f_2)\big) = \Pr\big(T_{B_{n+m}} = \sigma\big).$$

Proof. For any XOR-distinct *D*-transcript σ, we obtain that

$$\Pr(T_{B_{n+m}} = \sigma) = \frac{1}{2^n(2^n-1)\cdots(2^n-q+1)} \cdot \frac{1}{2^m(2^m-1)\cdots(2^m-q+1)}.$$

Consider any specific *n*-bit permutation f_1 and *m*-bit permutation f_2 such that $\sigma \notin BAD(f_1, f_2)$. Note that $T_{\Lambda_{n+m}} = \sigma$ if and only if for all $1 \leq i \leq q$, $y^{(i)} = \Lambda_{n+m}(x^{(i)})$. Since

$$\Lambda_{n+m} = \hat{M}_{f_4} \circ \overline{M}_{f_3} \circ \hat{M}_{f_2} \circ \overline{M}_{f_1},$$
$$y^{(i)} = \Lambda_{n+m}(x^{(i)}) \Leftrightarrow f_3(L_2^{(i)}) = y_L^{(i)} \oplus R_2^{(i)} \in I_n \text{ and } f_4(R_2^{(i)}) = y_L^{(i)} \oplus y_R^{(i)} \in I_m,$$

where $(L_2^{(i)}, R_2^{(i)}) = \hat{M}_{f_2} \circ \overline{M}_{f_1}(x_L^{(i)}, x_R^{(i)})$. By definition of $BAD(f_1, f_2)$, if $\sigma \notin BAD(f_1, f_2)$, then $L_2^{(i)} \neq L_2^{(j)}$, $R_2^{(i)} \neq R_2^{(j)}$, and $y_L^{(i)} \oplus \overline{R}_2^{(i)} \neq y_L^{(j)} \oplus \overline{R}_2^{(j)}$, for all $1 \le i \neq j \le q$. Moreover, $\hat{y}_L^{(i)} \oplus y_R^{(i)} \neq \hat{y}_L^{(j)} \oplus y_R^{(j)}$ for all XOR-distinct σ. Therefore, for any XOR-distinct σ, we obtain that

$$\Pr\left(T_{\Lambda_{n+m}} = \sigma \mid \sigma \notin BAD(f_1, f_2)\right) = \frac{(2^n - q)!}{2^n!} \cdot \frac{(2^m - q)!}{2^m!},$$

which completes the assertion. □

The next lemma guarantees that the advantage of D in distinguishing between B_{n+m} and Λ_{n+m} is negligible.

Lemma 6.

$$\left|\Pr\left(C_D(T_{B_{n+m}}) = 1\right) - \Pr\left(C_D(T_{\Lambda_{n+m}}) = 1\right)\right| < (q^2 - q)\left(\frac{1}{2^{n-1}} + \frac{5}{2^m}\right).$$

Proof. Let Θ be the set of all XOR-distinct D-transcripts σ such that the output of D is $C_D(\sigma) = 1$. Then we obtain that

$$\left|\Pr\left(C_D(T_{B_{n+m}}) = 1\right) - \Pr\left(C_D(T_{\Lambda_{n+m}}) = 1\right)\right| \le \left|\sum_{\sigma \in \Theta}\left\{\Pr\left(T_{B_{n+m}} = \sigma\right) - \Pr\left(T_{\Lambda_{n+m}} = \sigma\right)\right\}\right| \quad (1)$$

$$+ \Pr(T_{\Lambda_{n+m}} \text{ is not XOR-distinct}). \quad (2)$$

We first estimate the term (2). Note that $T_{\Lambda_{n+m}}$ is not XOR-distinct if and only if for some $1 \le i \neq j \le q$, $\hat{y}_L^{(i)} \oplus y_R^{(i)} = \hat{y}_L^{(j)} \oplus y_R^{(j)}$, where

$$\Lambda_{n+m}(x^{(i)}) = y^{(i)} = (y_L^{(i)}, y_R^{(i)}) \in I_n \times I_m.$$

Now we can see that

$$\hat{y}_L^{(i)} \oplus y_R^{(i)} = \hat{y}_L^{(j)} \oplus y_R^{(j)} \Leftrightarrow f_4(R_2^{(i)}) = f_4(R_2^{(j)}) \Leftrightarrow R_2^{(i)} = R_2^{(j)}.$$

From the proof of Lemma 4, we know that

$$\Pr\left(R_2^{(i)} = R_2^{(j)}\right) = \frac{1}{2^{m-1}}.$$

Thus

$$\Pr(T_{\Lambda_{n+m}} \text{ is not XOR-distinct}) < (q^2 - q) \cdot \frac{1}{2^m}.$$

On the other hand, the term (1) is bounded above as follows:

$$\left|\sum_{\sigma \in \Theta}\left\{\Pr\left(T_{B_{n+m}} = \sigma\right) - \Pr\left(T_{\Lambda_{n+m}} = \sigma\right)\right\}\right| \le \sum_{\sigma \in \Theta} \Pr(\sigma \notin BAD(f_1, f_2)) \cdot \left|\Pr\left(T_{\Lambda_{n+m}} = \sigma \mid \sigma \notin BAD(f_1, f_2)\right) - \Pr\left(T_{B_{n+m}} = \sigma\right)\right| \quad (3)$$

$$+ \sum_{\sigma \in \Theta} \Pr\left(T_{\Lambda_{n+m}} = \sigma, \sigma \in BAD(f_1, f_2)\right) \quad (4)$$

$$+ \sum_{\sigma \in \Theta} \Pr(\sigma \in BAD(f_1, f_2)) \cdot \Pr\left(T_{B_{n+m}} = \sigma\right). \quad (5)$$

By Lemma 5, the term (3) is zero and by Lemma 4, the value of (5) is bounded by

$$\max_{\sigma \in \Theta} \Pr(\sigma \in BAD(f_1, f_2)) \cdot \Pr\left(\bigcup_{\sigma \in \Theta}\{T_{B_{n+m}} = \sigma\}\right) < (q^2 - q)\left(\frac{1}{2^n} + \frac{1}{2^{m-1}}\right).$$

By Lemma 4, the value of (4) is also estimated as

$$\sum_{\sigma \in \Theta} \Pr\left(T_{\Lambda_{n+m}} = \sigma, \sigma \in BAD(f_1, f_2)\right) = \sum_{\sigma \in \Theta} \Pr\left(T_{\Lambda_{n+m}} = \sigma\right) \cdot \Pr\left(\sigma \in BAD(f_1, f_2) \mid T_{\Lambda_{n+m}} = \sigma\right) < (q^2 - q)\left(\frac{1}{2^n} + \frac{1}{2^{m-1}}\right),$$

since we can easily check that under the condition that $T_{\Lambda_{n+m}} = \sigma$, the probability of event $\sigma \in BAD(f_1, f_2)$ has the same upper bound as Lemma 4. □

Proof of Theorem 1: By using Lemma 3 and 6, we complete the proof as follows:

$$\begin{aligned} ADV_D &= \left|\Pr\left(C_D(T_{\Lambda_{n+m}}) = 1\right) - \Pr\left(C_D(T_{\Omega_{n+m}}) = 1\right)\right| \\ &\le \left|\Pr\left(C_D(T_{\Lambda_{n+m}}) = 1\right) - \Pr\left(C_D(T_{B_{n+m}}) = 1\right)\right| \\ &\quad + \left|\Pr\left(C_D(T_{B_{n+m}}) = 1\right) - \Pr\left(C_D(T_{\Omega_{n+m}}) = 1\right)\right| \\ &< \frac{q^2 - q}{2}\left(\frac{3}{2^{n-1}} + \frac{12}{2^m - 1}\right). \end{aligned}$$

□

V. PSEUDORANDOMNESS OF THE SIMPLIFIED KASUMI

From Theorem 1, it is reasonable to assume that the *FI* function of KASUMI is a PPE. In order to investigate the pseudorandomness of KASUMI, we use a simplified figure of KASUMI. The four-round simplified KASUMI is illustrated in Fig. 2, where $\vec{x} = (x_1, x_2, x_3, x_4)$ denotes a 4*n*-bit input value,

$$\vec{y} = (y_1, y_2, y_3, y_4), \quad \vec{w} = (w_1, w_2, w_3, w_4),$$

and $\vec{z} = (z_1, z_2, z_3, z_4)$ denotes the corresponding output of

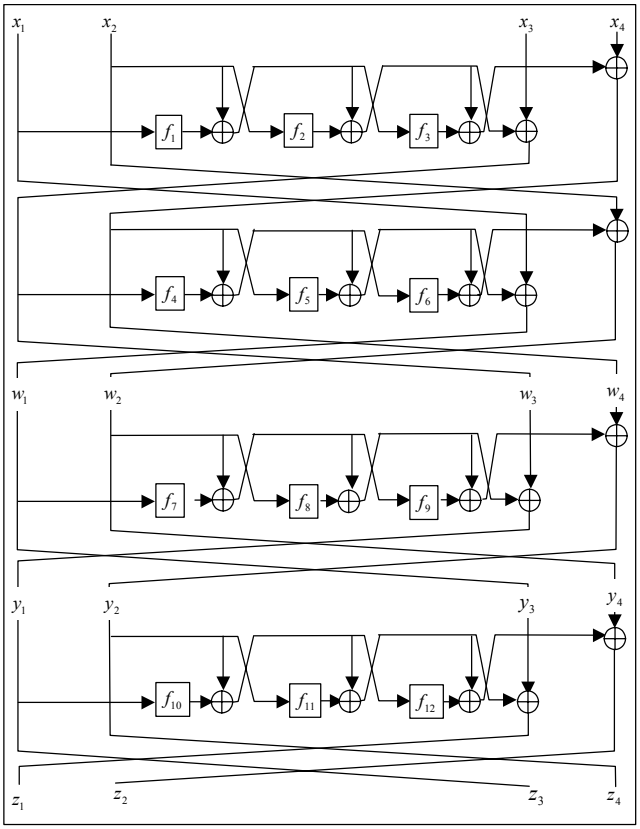

Fig. 2. Simplified four-round KASUMI.

the second, third, and fourth round of KASUMI, respectively. Each $x_i, w_i, y_i,$ and z_i is an n-bit value.

By the following theorem, we obtain the fact that three rounds of KASUMI is insufficient to be a PPE.

Theorem 2. The three-round simplified KASUMI is not a $4n$-bit PPE even if the f_i's $(i = 1,\ldots,9)$ of Fig. 2 are independently chosen from an n-bit PPE.

Proof. Let Λ_{4n} be the set of all permutations over I_{4n} obtained from the three-round simplified KASUMI. Consider a distinguisher D such as follows:

1. D chooses four $4n$-bit queries $\vec{x}^{(1)}, \vec{x}^{(2)}, \vec{x}^{(3)}$, and $\vec{x}^{(4)}$ such that

$$\vec{x}^{(1)} = (x_1, x_2, 0, 0), \quad \vec{x}^{(2)} = (x_1, x_2, x_3, 0),$$
$$\vec{x}^{(3)} = (x_1, x_2, 0, x_4), \quad \vec{x}^{(4)} = (x_1, x_2, x_3, x_4),$$

where x_1 and x_2 are two fixed n-bit values and $x_3 \neq 0 \neq x_4$.

2. D sends these four queries to the oracle O and receives the corresponding answers $\vec{y}^{(i)} = (y_1^{(i)}, y_2^{(i)}, y_3^{(i)}, y_4^{(i)})$ $(i = 1,2,3,4)$ from the oracle.

3. D outputs 1 if and only if

$$y_3^{(1)} \oplus y_3^{(2)} \oplus y_3^{(3)} \oplus y_3^{(4)} = 0.$$

If the oracle implements the UPE Ω_{4n}, then we obtain that

$$\begin{aligned} &\Pr(D \text{ outputs } 1 | O \leftarrow \Omega_{4n}) \\ &= \frac{2^{4n}(2^{4n}-1)(2^{4n}-2)2^{3n}(2^{4n}-4)!}{2^{4n}!} \\ &= \frac{2^{3n}}{2^{4n}-3} < \frac{1}{2^n - 1}. \end{aligned}$$

On the other hand, if O implements Λ_{4n}, then for the four queries $\vec{x}^{(1)}, \vec{x}^{(2)}, \vec{x}^{(3)}$, and $\vec{x}^{(4)}$, we can see from Fig. 2 that

$$\begin{aligned} y_3^{(1)} &= x_1 \oplus f_4(\alpha_1) \oplus f_5(\alpha_2) \oplus \alpha_2, \\ y_3^{(2)} &= x_1 \oplus f_4(\alpha_1 \oplus x_3) \oplus f_5(\alpha_2) \oplus \alpha_2, \\ y_3^{(3)} &= x_1 \oplus f_4(\alpha_1) \oplus f_5(\alpha_2 \oplus x_4) \oplus \alpha_2 \oplus x_4, \\ y_3^{(4)} &= x_1 \oplus f_4(\alpha_1 \oplus x_3) \oplus f_5(\alpha_2 \oplus x_4) \oplus \alpha_2 \oplus x_4, \end{aligned}$$

where (α_1, α_2) is the $2n$-bit output of the first-round function corresponding to the input (x_1, x_2). Hence we obtain by an argument similar to that of Sakurai and Zheng [6] that

$$y_3^{(1)} \oplus y_3^{(2)} \oplus y_3^{(3)} \oplus y_3^{(4)} = 0$$

with probability 1. Consequently we obtain that

$$\begin{aligned} ADV_D &= \left| \Pr(D \text{ outputs } 1 | O \leftarrow \Omega_{4n}) \right. \\ &\qquad \left. - \Pr(D \text{ outputs } 1 | O \leftarrow \Lambda_{4n}) \right| \\ &> 1 - \frac{1}{2^n - 1}, \end{aligned}$$

which is non-negligible. □

At this point, we consider the non-adaptive distinguisher security model, which is different from the one in section IV. The non-adaptive distinguisher sends all queries to the oracle at the same time, whereas the adaptive distinguisher determines the i-th query from the first i–1 query-answer pairs. We have experienced that under the adaptive distinguisher model, there are many factors involved in controlling a $4n$-bit block structure. The following theorem guarantees that KASUMI with four or more rounds is a pseudorandom permutation ensemble under the security model with a non-adaptive distinguisher.

Theorem 3. If f_i's $(i = 1,2,\ldots,12)$ in Fig. 2 are independently chosen from an n-bit PPE, then the four-round simplified KASUMI is a (q,a)-secure PPE, where $a = (q^2 - q)/2^n$.

Proof. Assume that f_i's are independently chosen from the UPE Ω_n. It suffices to prove the assertion under this assumption [1]. Let Λ_{4n} be the set of all permutations over

I_{4n} obtained from the simplified four-round KASUMI. Suppose that the distinguisher D makes q calls to the oracle O. In the i-th oracle call, D sends a $4n$-bit query $\vec{x}^{(i)} = (x_1^{(i)}, x_2^{(i)}, x_3^{(i)}, x_4^{(i)})$ to O and receives the corresponding output

$$\vec{z}^{(i)} = (z_1^{(i)}, z_2^{(i)}, z_3^{(i)}, z_4^{(i)}) = \pi(x_1^{(i)}, x_2^{(i)}, x_3^{(i)}, x_4^{(i)}),$$

where π is the randomly chosen permutation by O from Ω_{4n} or Λ_{4n}.

Let A_{w_j} denote the event that the j-th block of the output of two-round KASUMI $w_j^{(1)}, \ldots, w_j^{(q)}$ is all distinct for $j = 1,2,3,4$ (Fig. 2). If A_{w_1} occurs, then we can see that $z_4^{(1)}, \ldots, z_4^{(q)}$ are completely random since the output of f_7 and f_9 is completely random. Furthermore we also see that $z_1^{(1)}, \ldots, z_1^{(q)}$ are completely random because the output of f_{11} is also completely random. Similarly, if A_{w_2} occurs, then $z_3^{(1)}, \ldots, z_3^{(q)}$ and $z_2^{(1)}, \ldots, z_2^{(q)}$ are completely random due to f_8 and f_{10}, respectively. Therefore, if A_{w_1} and A_{w_2} occur, then ADV_D is bounded above as follows:

$$\begin{aligned} ADV_D &\le 1 - \Pr\left(A_{w_1} \cap A_{w_2}\right) \\ &\le \sum_{1 \le i < j \le q} \Pr\left(w_1^{(i)} = w_1^{(j)}\right) + \sum_{1 \le i < j \le q} \Pr\left(w_2^{(i)} = w_2^{(j)}\right). \end{aligned}$$

We estimate the summands $\Pr\left(w_1^{(i)} = w_1^{(i)}\right)$ and $\Pr\left(w_2^{(i)} = w_2^{(i)}\right)$ for any $1 \le i \ne j \le q$. Fix

$$\vec{x}^{(i)} = (x_1^{(i)}, x_2^{(i)}, x_3^{(i)}, x_4^{(i)})$$

and

$$\vec{x}^{(j)} = (x_1^{(j)}, x_2^{(j)}, x_3^{(j)}, x_4^{(j)})$$

arbitrarily. We separate the following four cases.

Case 1: $x_1^{(i)} \ne x_1^{(j)}$. In this case by considering the two paths

$$x_1 \to f_1 \to f_3 \to f_5 \to w_1$$

and

$$x_1 \to f_1 \to f_4 \to f_6 \to w_2,$$

we obtain that

$$\Pr\left(w_1^{(i)} = w_1^{(i)}\right) \le \frac{1}{2^n} \quad \text{and} \quad \Pr\left(w_2^{(i)} = w_2^{(i)}\right) \le \frac{1}{2^n},$$

since for any n-bit vector b, $\Pr(a_1 \oplus a_2 = b) = 1/2^n$, where a_1 and a_2 are randomly chosen n-bit vectors.

Case 2: $x_2^{(i)} \ne x_2^{(j)}$. Consider the path

$$x_2 \to f_2 \to f_4 \to f_6 \to w_2.$$

Then we can see that $w_2^{(i)}$ and $w_2^{(j)}$ are completely random. By considering the path $x_2 \to f_2 \to f_5 \to w_1$, we also know that $w_1^{(i)}$ and $w_1^{(j)}$ are completely random. Hence we obtain that

$$\Pr\left(w_1^{(i)} = w_1^{(i)}\right) \le \frac{1}{2^n} \quad \text{and} \quad \Pr\left(w_2^{(i)} = w_2^{(i)}\right) \le \frac{1}{2^n}.$$

Case 3: $x_3^{(i)} \ne x_3^{(j)}$. By considering the path

$$x_3 \to f_4 \to f_6 \to w_2,$$

we can see that $w_2^{(i)}$ and $w_2^{(j)}$ are completely random. And by considering the path $x_3 \to f_4 \to w_1$, we also obtain that $w_1^{(i)}$ and $w_1^{(j)}$ are completely random. Hence we obtain that

$$\Pr\left(w_1^{(i)} = w_1^{(i)}\right) \le \frac{1}{2^n} \quad \text{and} \quad \Pr\left(w_2^{(i)} = w_2^{(i)}\right) \le \frac{1}{2^n}.$$

Case 4: $x_4^{(i)} \ne x_4^{(j)}$. Consider the path $x_4 \to f_5 \to w_1$. Then $w_1^{(i)}$ and $w_1^{(j)}$ are completely random. Thus

$$\Pr\left(w_1^{(i)} = w_1^{(i)}\right) \le \frac{1}{2^n}$$

holds. Similarly we obtain that

$$\Pr\left(w_2^{(i)} = w_2^{(i)}\right) \le \frac{1}{2^n},$$

by considering the path $x_4 \to f_5 \to w_1$.

Therefore, for any case, we obtain that

$$\Pr\left(w_1^{(i)} = w_1^{(i)}\right) \le \frac{1}{2^n} \quad \text{and} \quad \Pr\left(w_2^{(i)} = w_2^{(i)}\right) \le \frac{1}{2^n}.$$

This implies that $ADV_D \le q(q-1)/2^n$. □

VI. CONCLUSION

In this work we examined the pseudorandomness of the 3GPP block cipher KASUMI. We have proved that the structure of the *FI* function within a KASUMI composed of a four-round unbalanced MISTY-type structure is a pseudorandom permutation under a security model with an adaptive distinguisher. We have shown that the simplified KASUMI with three rounds is not a pseudorandom permutation ensemble, but a four-round simplified KASUMI is a pseudorandom permutation ensemble under a non-adaptive distinguisher model. Under an adaptive distinguisher model it is necessary to consider many factors to control a $4n$-bit block structure. Thus, we set aside the pseudorandomness of the

KASUMI-like structure as an open problem.

The results of this paper disclose the soundness of the basic block structure of KASUMI from the viewpoint of pseudorandomness. Within the security architecture of the 3GPP system there are two standardized functions, the confidentiality function *f*8 and the integrity function *f*9. These two functions are based on the block cipher KASUMI. Thus the pseudorandomness of KASUMI is the main assumption on which to examine the provable security of *f*8 and *f*9. The results of this paper provide support for this assumption.

ACKNOWLEDGEMENTS

Thanks to Tetsu Iwata for pointing out some flaws in the proof of Theorem 1 of [12]. We also appreciate the anonymous referees' valuable comments.

REFERENCES

[1] M. Luby and C. Rackoff, "How to Construct Pseudorandom Permutations and Pseudorandom Functions," *SIAM J. Comput*., vol. 17, 1988, pp. 189-203.

[2] J. Patarin, "How to Construct Pseudorandom and Super Pseudorandom Permutations from one Single Pseudorandom Function," *Advances in Cryptology-Eurocrypt*'92, LNCS 658, Springer-Verlag, 1992, pp. 256-266.

[3] M. Naor and O. Reingold, "On the Construction of Pseurandom Permutations: Luby-Rackoff Revisited," *J. Cryptology*, vol. 12, 1999, pp. 29-66.

[4] M. Matsui, "New Permutation of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis," *Fast Software Encryption*, LNCS 1039, Springer-Verlag, 1996, pp. 205-218.

[5] M. Matsui, "New Block Encryption Algorithm MISTY," Fast Software Encryption'97, LNCS 1267, Springer-Verlag, 1997, pp. 54-68.

[6] K. Sakurai and Y. Zheng, "On Non-Pseudorandomness from Block Ciphers with Provable Immunity against Linear Cryptanalysis," *IEICE Trans. Fundamentals*, vol. E80-A, no. 1, 1997, pp. 19-24.

[7] H. Gilbert and M. Minier, "New Results on the Pseudorandomness of Some Block Cipher Constructions," *FSE* 2001, LNCS 2355, Springer-Verlag, 2002, pp. 248-266.

[8] J.S. Kang, O.Y. Yi, D.W. Hong, and H.S. Cho, "Pseudorandomness of MISTY-Type Transformations and the Block Cipher KASUMI," *ACISP*2001, LNCS 2119, Springer-Verlag, 2001, pp. 60-73.

[9] T. Iwata, T. Yoshino, T. Yuasa, and K. Kurosawa, "Round Security and Super-Pseudorandomness of MISTY Type Structure," *FSE*2001, LNCS 2355, Springer-Verlag, 2002, pp. 233-247.

[10] T. Iwata, T. Yoshino, and K. Kurosawa, "Non-Cryptographic Primitive for Pseudorandom Permutation," *FSE* 2002, LNCS 2365, Springer-Verlag, 2002, pp. 149-163.

[11] 3G TS 35.201, *Specification of the 3GPP Confidentiality and Integrity Algorithm; Document 1: f8 and f9 specifications*, available at http://www.3gpp.org.

[12] J.S. Kang, S.U. Shin, D.W. Hong, and O.Y. Yi, "Provable Security of KASUMI and 3GPP Encryption mode f8," *ASIACRYPT* 2001, LNCS 2248, Springer-Verlag, 2001, pp. 255-271.

[13] M. Bellare, J. Kilian, and P. Rogaway, "The Security of Cipher Block Chaining Message Authentication Codes," *Advances in Cryptology-Crypto*'94, LNCS 839, Springer-Verlag, 1994, pp. 341-358.

[14] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation," 38*th Symp. on Foundations of Computer Science* (FOCS), *IEEE Computer Society*, 1997, pp. 394-403.

[15] L.R. Knudsen, *DEAL-A 128-Bit Block Cipher*, Technical report 151, Univ. of Bergen, February 1998, available at http://www.ii.uib.no/\~larsr/newblock.html.

[16] J. Patarin, "Generic Attacks on Feistel Schemes," *ASIACRYPT* 2001, LNCS 2248, Springer-Verlag, 2001, pp. 222-238.

[17] 3GPP SAGE, *Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms*, SAGE version 2.0, 2001, available at http://www.3gpp.org.

[18] U. Kühn, "Cryptanalysis of Reduced-Round MISTY," *Advances in Cryptology-Eurocrypt* 2001, LNCS 2045, Springer-Verlag, 2001, pp. 325-339.

Ju-Sung Kang received the BS, MS, and PhD degrees in mathematics from Korea University, Seoul, Korea in 1989, 1991, and 1996. He joined ETRI in 1997, and he is currently with the Information Security Division of ETRI. In 2001-2002, he was a Visiting Researcher of the COSIC, Research Group of Katholieke Universiteit Leuven in Belgium. His current research interests include cryptographic algorithms and protocols.

Bart Preneel is a Professor in the Electrical Engineering Department of the Katholieke Universiteit Leuven in Belgium. He is also a Visiting Professor at the Ruhr-Universitaet Bochum in Germany and at the University of Ghent in Belgium. In 1993-1994 he was Research Fellow at the University of California at Berkeley. He heads the COSIC Research Group. He is the Vice President of the International Association of Cryptologic Research (IACR) and Chairman of L-SEC.

Heuisu Ryu received his MS and BS degrees in mathematics from Korea University in 1990 and 1992. He received his PhD in mathematics from Johns Hopkins University in the USA in 1999. He joined ETRI in 2000 and has been working on cryptography. Currently, he is the Team Leader of the Information Security Basic Research Team and Senior Engineering Staff. His research interests are elliptic curve cryptography, information security algorithms, information security protocols, and information security in mobile environments.

Kyo Il Chung received the PhD, MS, and BS degrees in electronic engineering from Hanyang University in 1997, 1983, and 1981. He joined ETRI in 1982 and has been involved with COMSEC systems. Currently, he is a Principal Member of Engineering Staff and the Director of the Information Security Basic Department. His research interests are IC cards, biometrics and information warfare.

Chee Hang Park received the BS degree in applied physics from Seoul National University, Korea, in 1974, the MS degree from Korea Advanced Institute of Science and Technology, Korea, in 1980, and the PhD degree in computer science from University of Paris 6, France, in 1987. During the last 10 years, he has been involved as Project Leader in several large projects such as Multimedia Computer System Development and High Speed Parallel Computer System Development. His research interests include multimedia systems, distributed systems, middleware, group-ware, network virtual computing, and mobile agent architecture. He is currently the Executive Director of the Information Security Technology Division at ETRI.