Research Article

Rüdiger Sparr and Ralph Wernsdorf

The round functions of KASUMI generate the alternating group

Abstract: We show that the round functions of the KASUMI block cipher for odd and even round type generate the alternating group on the message space. Moreover, under the assumption of independent round keys, we prove that also the KASUMI two-round functions and the KASUMI encryption functions generate the alternating group.

Keywords: KASUMI, block cipher, permutation groups

MSC 2010: 94A60, 20B35

Rüdiger Sparr, Ralph Wernsdorf: Rohde & Schwarz SIT GmbH, Am Studio 3, 12489 Berlin, Germany,
e-mail: ruediger.sparr@rohde-schwarz.com, ralph.wernsdorf@rohde-schwarz.com

Communicated by: Robert Gilman

1 Introduction

KASUMI is a 64-bit block cipher with 128-bit key size which is used for the confidentiality and integrity algorithms of the Third Generation Partnership Project (3GPP) for mobile communications [7]. KASUMI is based on the MISTY1 block cipher [15] and is carefully designed to resist conventional differential and linear cryptanalysis [1]. It has been shown that the four-round KASUMI-type permutation is pseudorandom and that the six-round KASUMI-type permutation is super-pseudorandom under an adaptive distinguisher model [11]. Furthermore, as shown in [6], KASUMI is susceptible to a related key attack using four related keys, which however is not a security threat for the use of KASUMI in GSM and UMTS applications. Recent further cryptanalysis results about KASUMI can be found in [12, 19].

In this paper we present several new results on group theoretic properties of the KASUMI round functions and component functions. For any block cipher, it is desirable to exclude possible structural defects for the group generated by the round functions, such as an insufficient diversity of occurring permutations or imprimitivity. Because of the widespread use for 3GPP mobile communications, the exclusion of such structural weaknesses appears particularly relevant for the KASUMI block cipher. As shown by Paterson [17], there are DES-like block ciphers which possess a certain resistance to linear and differential cryptanalysis, but can be easily broken since the round functions generate a group which acts imprimitively on the message space. A further purpose for the analysis of group theoretic properties of a block cipher stems from the fact that, if the round functions of the cipher generate the alternating group on the message space, then general security proofs for the cipher are possible with respect to the Markov cipher approach to classical differential cryptanalysis (cf. [2, 10, 16]). For the DES [4], AES [22], and other ciphers, several results on the cyclic and group theoretic structure of their components have already been found (see [3, 5, 8, 13, 21, 23, 24]).

The paper is organized as follows. In Section 2 we provide some notions and facts from the theory of permutation groups which are used in this paper. In Section 3 we give a description of the KASUMI block cipher. In Section 4 we investigate cyclic properties of the internal components of the KASUMI round functions and prove an unexpected property of the FO-functions of KASUMI. In Section 5 we show that the groups generated by the KASUMI round functions for odd and even round type are equal to the alternating group on the message space $\{0,1\}^{64}$. In Section 6 we show that also the KASUMI two-round functions as well as the KASUMI encryption functions generate the alternating group on the set $\{0,1\}^{64}$ under the assumption of independent round keys. In Section 7 we finish the paper with some concluding remarks.

2 Group theoretical facts

For any nonempty finite set X, the group of bijective mappings of X onto itself is denoted by S_X. If n is a natural number and $X = \{1, \dots, n\}$, we also write S_n instead of S_X. Every subgroup of S_X is called a *permutation group* on X. Let ℓ be a natural number with $0 < \ell \le |X|$. A permutation group $G \le S_X$ is called *ℓ-transitive* if, for any pair of ℓ-tuples $(a_1, \dots, a_\ell)$, $(b_1, \dots, b_\ell) \in X^\ell$ with $a_i \neq a_j, b_i \neq b_j$ for $i \neq j$, there is a permutation $g \in G$ with $g(a_i) = b_i$ for $i = 1, \dots, \ell$. A 1-transitive permutation group is simply called *transitive*. If G is a permutation group on a set X and $a \in X$, the subgroup of all $g \in G$ with $g(a) = a$ is denoted by G_a.

For multiple transitivity we have the following proposition (cf. [25]).

Proposition 2.1. *Let G be a transitive permutation group on a finite set X, ℓ a natural number with $0 < \ell < |X|$, and $a \in X$. Then G is $(\ell + 1)$-transitive on X if and only if G_a is ℓ-transitive on $X \setminus \{a\}$.*

Let $G \le S_X$ be a permutation group with $|X| = n$. A subset $B \subseteq X$ is called a *block* of G if $g(B) = B$ or $g(B) \cap B = \emptyset$ for every $g \in G$. A block $B \subseteq X$ is said to be *trivial* if $B \in \{X, \emptyset\}$ or $B = \{x\}$ where $x \in X$. A *complete nontrivial block system* for G is a partition $\{X_1, \dots, X_t\}$ of X into disjoint subsets X_i of equal size s with $1 < s < n$, such that for every permutation $g \in G$ and every block X_i there is a block X_j with $g(X_i) = X_j$ for $i, j \in \{1, \dots, t\}$. Let $G \le S_X$ be transitive. G is called *imprimitive* if there is a nontrivial block $B \subset X$ of G. Otherwise, G is said to be *primitive*. Every 2-transitive permutation group is primitive, but not conversely. A permutation $g \in S_X$ is a *transposition* if g interchanges two elements $x, y \in X$ and fixes all the other elements of X. A permutation g is called *even* (*odd*) if g can be represented as a product of an even (odd) number of transpositions. The set of all even permutations $g \in S_n$ forms a group which is called the *alternating group* on the set $\{1, \dots, n\}$ and which is denoted by A_n.

For any permutation on a finite set of even cardinality, the number of cycles of odd length in its disjoint cycle decomposition must be even. Since the cycles of even length are odd permutations, we have the following result.

Proposition 2.2. *A permutation on a finite set with even cardinality is even if and only if its cycle representation contains an even number of cycles (including the cycles of length 1).*

The *degree* of a permutation group G on a finite set X is defined as the number of elements of X that are moved by at least one permutation of G. The *degree of a permutation* is defined as the degree of the cyclic group generated by this permutation.

We need the subsequent results which provide sufficient conditions for a permutation group to be the alternating or symmetric group.

Theorem 2.3 (cf. [25, Theorem 13.10]). *Let p be a prime and G a primitive permutation group of degree $n = qp + k$, which contains an element of order p and degree qp, but which is neither the alternating nor symmetric group.*

(a) *If $q \le 7$ and $p \ge 11$, then $k \le 8$.*
(b) *If $q \ge 8$ and $p \ge 2q - 1$, then $k \le 4q - 4$.*

Proposition 2.4. *Let G be a primitive permutation group on the set $\{0, 1\}^{2n}$ with $n > 2$. Suppose there is an element $g \in G$ which contains in its cycle representation a cycle with a prime factor $p > 2^{n+1}$ and for $r = 2^{2n} \bmod p$ we have*

$$r > \max\bigl(8, 4 \cdot (2^{2n} - r)/p - 4\bigr).$$

Then G is the alternating or the symmetric group on $\{0, 1\}^{2n}$.

Proof. Suppose G is neither the alternating nor symmetric group. Using an appropriate exponentiation of g, we obtain a permutation with q cycles of length p, where $1 \le q < 2^{n-1}$. Hence G contains an element of order p and degree pq, where $pq \le 2^{2n} - r$. Then $p \ge \max(11, 2q - 1)$, but

$$2^{2n} - pq \ge r > \max\bigl(8, 4 \cdot (2^{2n} - r)/p - 4\bigr) \ge \max(8, 4q - 4)$$

which is a contradiction to Theorem 2.3. □

Remark 2.5. As an alternative to Theorem 2.3 and Proposition 2.4, it is also possible to use the theorems [18, Theorem A] or [14, Theorem 1.1] to derive similar sufficient conditions for a permutation group to be the alternating or symmetric group.

Theorem 2.6 (cf. [20, Corollary 10.2.2]). *Let G be a transitive permutation group on a finite set X with $|X| > 7$. If there is an element $g \in G$ which contains in its cycle representation a cycle of prime number length p with $|X|/2 < p < |X| - 2$, then G is the alternating or the symmetric group on X.*

3 Description of KASUMI

For every $x = (x_1, \dots, x_{2n}) \in \{0,1\}^{2n}$ we write x_L for $(x_1, \dots, x_n)$ and x_R for $(x_{n+1}, \dots, x_{2n})$. The all-zero bit-vector in the set $\{0,1\}^n$ is denoted by 0^n and elements of $(\{0,1\}^m)^n$ are identified with elements in $\{0,1\}^{mn}$ by concatenation. We write rot_k for the left rotation of 16-bit words by k bit positions and pr for the projection of 9-bit words w to the seven right-most bits of w. Let S7 and S9 denote the S-boxes of KASUMI, which are nonlinear permutations on $\{0,1\}^7$ and $\{0,1\}^9$, respectively [7]. Furthermore, let

$$\mu(v, w) = \big(\mathrm{S7}(v) \oplus v \oplus \mathrm{pr}(\mathrm{S9}(w)), (0^2, v) \oplus \mathrm{S9}(w)\big)$$

for every $(v, w) \in \{0,1\}^7 \times \{0,1\}^9$ and $\sigma_k(x) = x \oplus k$ for every $k \in \{0,1\}^{16}$ and $x \in \{0,1\}^{16}$. For every $z \in \{0,1\}^{16}$, the mapping FI_z is defined as

$$FI_z = \mu \circ \sigma_z \circ \mu \circ \mathrm{rot}_9\,.$$

Obviously, rot_9, μ, σ_z, and FI_z are permutations on $\{0,1\}^{16}$ for every $z \in \{0,1\}^{16}$. For all $z, z' \in \{0,1\}^{16}$ and $x \in \{0,1\}^{32}$, let $f_{z,z'}(x) = (x_R, FI_{z'}(x_L \oplus z) \oplus x_R)$. For every $k = (z_1, \dots, z_6) \in \{0,1\}^{96}$ with $z_1, \dots, z_6 \in \{0,1\}^{16}$, the nonlinear permutation FO_k on $\{0,1\}^{32}$ is defined as

$$FO_k = f_{z_3,z_6} \circ f_{z_2,z_5} \circ f_{z_1,z_4}.$$

Let f_{and} and f_{or} denote the Boolean AND-function and the Boolean OR-function on $\{0,1\}^{16}$, respectively. For every $l \in \{0,1\}^{32}$, the linear mixing permutation FL_l on $\{0,1\}^{32}$ is defined as

$$FL_l(x) = \big(x_L \oplus \mathrm{rot}_1(f_{\mathrm{or}}(a, l_R)), a\big)$$

for every $x \in \{0,1\}^{32}$, where $a = x_R \oplus \mathrm{rot}_1(f_{\mathrm{and}}(x_L, l_L))$. For every $(k, l) \in \{0,1\}^{96} \times \{0,1\}^{32}$, let

$$F^{(1)}_{k,l} = FO_k \circ FL_l \quad \text{and} \quad F^{(2)}_{k,l} = FL_l \circ FO_k.$$

The round functions of KASUMI for odd resp. even round type are defined as

$$R^{(t)}_{k,l}(x) = \big(x_R \oplus F^{(t)}_{k,l}(x_L), x_L\big)$$

for every $x \in \{0,1\}^{64}$, $(k, l) \in \{0,1\}^{96} \times \{0,1\}^{32}$, and $t = 1$ resp. $t = 2$. Finally, the KASUMI encryption function f_{enc} is defined as

$$f_{\mathrm{enc}} = \big(R^{(2)}_{k_8,l_8} \circ R^{(1)}_{k_7,l_7}\big) \circ \cdots \circ \big(R^{(2)}_{k_2,l_2} \circ R^{(1)}_{k_1,l_1}\big)$$

for $(k_1, l_1), \dots, (k_8, l_8) \in \{0,1\}^{96} \times \{0,1\}^{32}$.

The key schedule of KASUMI is defined as follows. Firstly, the 128-bit key is divided into eight consecutive 16-bit values K_j, $j = 0, \dots, 7$. Secondly, an array of eight 16-bit values K'_j, $j = 0, \dots, 7$, is defined by

$$K'_j = K_j \oplus c_j, \quad j = 0, \dots, 7,$$

where

$$c_0 = \mathrm{0x0123}, \quad c_1 = \mathrm{0x4567}, \quad c_2 = \mathrm{0x89ab}, \quad c_3 = \mathrm{0xcdef},$$
$$c_4 = \mathrm{0xfedc}, \quad c_5 = \mathrm{0xba98}, \quad c_6 = \mathrm{0x7654}, \quad c_7 = \mathrm{0x3210}.$$

For $i = 1, \dots, 8$, let

$$\begin{aligned} &z_{i,1} = \mathrm{rot}_5(K_{i \bmod 8}), && z_{i,2} = \mathrm{rot}_8(K_{(i+4) \bmod 8}), && z_{i,3} = \mathrm{rot}_{13}(K_{(i+5) \bmod 8}), && z_{i,4} = K'_{(i+3) \bmod 8}, \\ &z_{i,5} = K'_{(i+2) \bmod 8}, && z_{i,6} = K'_{(i+6) \bmod 8}, && l_{i,1} = \mathrm{rot}_1(K_{i-1}), && l_{i,2} = K'_{(i+1) \bmod 8}. \end{aligned}$$

Finally, the round key $(k_i, l_i) \in \{0,1\}^{96} \times \{0,1\}^{32}$ for round i is defined as $k_i = (z_{i,1}, \dots, z_{i,6})$ and $l_i = (l_{i,1}, l_{i,2})$ for $i = 1, \dots, 8$.

Remark 3.1. For every $(k, l) \in \{0,1\}^{96} \times \{0,1\}^{32}$ and every $i \in \{1, \dots, 8\}$ there is a KASUMI round key $(k_i, l_i) \in \{0,1\}^{96} \times \{0,1\}^{32}$ such that $(k, l) = (k_i, l_i)$.

4 Properties of the round function components

For $t \in \{1, 2\}$, let $H^{(t)}$ denote the group generated by the set of permutations

$$\{F_{k,l}^{(t)} : k \in \{0,1\}^{96}, l \in \{0,1\}^{32}\}.$$

In this section we first prove several cyclic properties for the component functions of KASUMI and show that the groups $H^{(1)}$ and $H^{(2)}$ are equal to the alternating group on the set $\{0,1\}^{32}$. Furthermore, we prove an unexpected property for the family of FO-permutations.

Lemma 4.1. (a) *For every $x, y \in \{0,1\}^{16}$ there is an element $z \in \{0,1\}^{16}$ with $FI_z(x) = y$.*
(b) *For every $x, y \in \{0,1\}^{32}$ there is an element $k \in \{0,1\}^{96}$ with $FO_k(x) = y$.*

Proof. (a) For $x, y \in \{0,1\}^{16}$, define $z \in \{0,1\}^{16}$ as $z = \mu(\mathrm{rot}_9(x)) \oplus \mu^{-1}(y)$.

(b) Let $a, b \in \{0,1\}^{32}$ and $z_1, z_2 \in \{0,1\}^{16}$. We can choose elements $z'_1, z'_2 \in \{0,1\}^{16}$ such that $FI_{z'_1}(a_L \oplus z_1) = a_R \oplus b_L$ and $FI_{z'_2}(a_R \oplus z_2) = b_L \oplus b_R$. Then $f_{z_1,z'_1}(a) = (a_R, FI_{z'_1}(a_L \oplus z_1) \oplus a_R) = (a_R, b_L)$, hence

$$f_{z_2,z'_2}(f_{z_1,z'_1}(a)) = f_{z_2,z'_2}(a_R, b_L) = (b_L, FI_{z'_2}(a_R \oplus z_2) \oplus b_L) = b.$$

Thus, for any $x, y \in \{0,1\}^{32}$ and $z_1, z_2, z_3, z'_3 \in \{0,1\}^{16}$, there are $z'_1, z'_2 \in \{0,1\}^{16}$ such that

$$f_{z_3,z'_3}(f_{z_2,z'_2}(f_{z_1,z'_1}(x))) = y. \qquad \square$$

Corollary 4.2. *The groups $H^{(1)}$ and $H^{(2)}$ are transitive.*

Lemma 4.3. (a) *FO_k is an even permutation for every $k \in \{0,1\}^{96}$.*
(b) *FL_l is an even permutation for every $l \in \{0,1\}^{32}$.*

Proof. (a) Every FO-function is a three-fold composition of permutations of the form

$$f_{z,z'}(x) = (x_R, FI_{z'}(x_L \oplus z) \oplus x_R),$$

where $x \in \{0,1\}^{32}$ and $z, z' \in \{0,1\}^{16}$. For every $z, z' \in \{0,1\}^{16}$ we have

$$f_{z,z'} = \psi_4 \circ \psi_3 \circ \psi_2 \circ \psi_1,$$

where $\psi_1(x) = (x_R, x_L)$, $\psi_2(x) = (x_L, x_R \oplus z)$, $\psi_3(x) = (x_L, FI_{z'}(x_R))$, and $\psi_4(x) = (x_L, x_L \oplus x_R)$ for all $x \in \{0,1\}^{32}$. Then ψ_1 is an even permutation by [8, Lemma 1], and ψ_2 and ψ_4 are even by [8, Lemma 2]. Finally, ψ_3 is an even permutation by Proposition 2.2 because the number of cycles of ψ_3 is a multiple of 2^{16}.

(b) Every function FL_l, $l = \{0,1\}^{32}$, is a composition $FL_l = h_l \circ g_l$, where

$$g_l(x) = (x_L, x_R \oplus \mathrm{rot}_1(f_{\mathrm{and}}(x_L, l_L))) \quad \text{and} \quad h_l(x) = (x_L \oplus \mathrm{rot}_1(f_{\mathrm{or}}(x_R, l_R)), x_R)$$

for all $x \in \{0,1\}^{32}$. If $l \in \{0,1\}^{32}$ with $l_L = 0^{16}$, then $g_l = \mathrm{id}$. Otherwise, g_l has $2^{32-\mathrm{wt}(l_L)}$ fixed points and $(2^{32} - 2^{32-\mathrm{wt}(l_L)})/2$ cycles of length 2, where $\mathrm{wt}(l_L)$ denotes the Hamming weight of l_L. If $l \in \{0,1\}^{32}$ with $l_R \neq 0^{16}$, the mapping h_l has 2^{31} cycles of length 2. Otherwise, h_l has 2^{16} fixed points and $(2^{32} - 2^{16})/2$ cycles of length 2. Thus, g_l and h_l are even permutations for every $l \in \{0,1\}^{32}$ by Proposition 2.2. $\square$

Proposition 4.4. *$H^{(1)}$ and $H^{(2)}$ are equal to the alternating group on the set $\{0,1\}^{32}$.*

Proof. By Corollary 4.2, $H^{(1)}$ and $H^{(2)}$ are transitive groups. For

$$k = (\text{0xbbb0}, \text{0x12de}, \text{0xe1b1}, \text{0x84cd}, \text{0x6e33}, \text{0xbd61}) \quad \text{and} \quad l = (\text{0x2e2e}, \text{0x8fd1}),$$

the $F^{(1)}_{k,l}$-cycle starting at 0x5ac292d0 is of length $c = 3\,669\,513\,383$ (here, the round key and the cycle have been found by a random search). By definition, the cycle representation of $F^{(2)}_{k,l}$ must contain a cycle with the same length. Since c is a prime number with

$$2^{31} < c < 2^{32} - 2$$

and the groups $H^{(1)}, H^{(2)}$ contain only even permutations, the result follows by Theorem 2.6. □

For any subset $M \subseteq \{0,1\}^n$, let $\langle M \rangle$ denote the linear hull of M in the vector space $\mathbb{F}_2^n$.

In the following section we will prove that the groups generated by the KASUMI round functions of odd and even round type are 2-transitive. For the proof we need the following result that was verified by a computer search with $m = 64$ for $t = 1$ and $m = 62$ for $t = 2$.

Lemma 4.5. *Let $t \in \{1,2\}$. There are $m \geq 32$, $k_1, \dots, k_m \in \{0,1\}^{96}$, and $l_1, \dots, l_m \in \{0,1\}^{32}$ such that $F^{(t)}_{k_i,l_i}(0^{32}) = 0^{32}$ for $i = 1, \dots, m$, and $\langle F^{(t)}_{k_i,l_i}(x) : i = 1, \dots, m \rangle = \mathbb{F}_2^{32}$ for every $x \in \{0,1\}^{32} \setminus \{0^{32}\}$.*

Contrary to the preceding result, the mappings FO_k, $k \in \{0,1\}^{96}$, have the following unexpected property.

Proposition 4.6. *Let $a \in \{0,1\}^{32}$. For all $m \geq 32$ and $k_1, \dots, k_m \in \{0,1\}^{96}$ with $FO_{k_i}(0^{32}) = a$ for $i = 1, \dots, m$, we have $\langle FO_{k_i}(x) : i = 1, \dots, m \rangle \neq \mathbb{F}_2^{32}$ for every $x \in \{0^{25}\} \times \{0,1\}^7$.*

Proof. Let $k, k' \in \{0,1\}^{96}$ with $FO_k(0^{32}) = FO_{k'}(0^{32})$, $x \in \{0^{25}\} \times \{0,1\}^7$, and $\xi = FO_k(x) \oplus FO_{k'}(x)$. We will show that

$$\xi_L \oplus \xi_R \in \{0,1\}^7 \times \{0^2\} \times \{0,1\}^7.$$

Let $k = (z_1, \dots, z_6)$ with $z_1, \dots, z_6 \in \{0,1\}^{16}$, and $y = f_{z_2,z_5}(f_{z_1,z_4}(x))$, where

$$y_L = FI_{z_4}(x_L \oplus z_1) \oplus x_R \quad \text{and} \quad y_R = FI_{z_5}(x_R \oplus z_2) \oplus y_L.$$

Let further $u = f_{z_3,z_6}(y) = FO_k(x)$, where $u_L = y_R$ and $u_R = FI_{z_6}(y_L \oplus z_3) \oplus y_R$. Then

$$u_L \oplus u_R = FI_{z_6}(FI_{z_4}(x_L \oplus z_1) \oplus z_3 \oplus x_R).$$

Similarly, for $k' = (z'_1, \dots, z'_6)$ with $z'_1, \dots, z'_6 \in \{0,1\}^{16}$, and $u' = FO_{k'}(x)$, we obtain

$$u'_L \oplus u'_R = FI_{z'_6}(FI_{z'_4}(x_L \oplus z'_1) \oplus z'_3 \oplus x_R).$$

By assumption we have

$$FI_{z_6}(FI_{z_4}(x_L \oplus z_1) \oplus z_3) = FI_{z'_6}(FI_{z'_4}(x_L \oplus z'_1) \oplus z'_3).$$

Then, by Proposition A.3 in the Appendix, it follows that

$$\xi_L \oplus \xi_R = u_L \oplus u_R \oplus u'_L \oplus u'_R \in \{0,1\}^7 \times \{0^2\} \times \{0,1\}^7.$$ □

5 Group theoretic properties of the KASUMI round functions

In this section we show that the KASUMI round functions for odd and even rounds generate the alternating group on $\{0,1\}^{64}$.

Proposition 5.1. *Let $s, t \in \{1,2\}$. For every $x, y \in \{0,1\}^{64}$ there are $k, k' \in \{0,1\}^{96}$ and $l, l' \in \{0,1\}^{32}$ such that $(R^{(t)}_{k',l'} \circ R^{(s)}_{k,l})(x) = y$.*

Proof. Let $x, y \in \{0,1\}^{64}$. By Lemma 4.1 there are $k, k' \in \{0,1\}^{96}$ and $l, l' \in \{0,1\}^{32}$ such that

$$F^{(s)}_{k,l}(x_L) = x_R \oplus y_R \quad \text{and} \quad F^{(t)}_{k',l'}(y_R) = x_L \oplus y_L.$$

Then

$$R^{(t)}_{k',l'}(R^{(s)}_{k,l}(x_L, x_R)) = (x_L \oplus F^{(t)}_{k',l'}(x_R \oplus F^{(s)}_{k,l}(x_L)), x_R \oplus F^{(s)}_{k,l}(x_L)) = (x_L \oplus F^{(t)}_{k',l'}(y_R), y_R) = (y_L, y_R). \qquad \square$$

For $t \in \{1,2\}$, let $G^{(t)}$ denote the group generated by the set of functions

$$\{R^{(t)}_{k,l} : k \in \{0,1\}^{96},\ l \in \{0,1\}^{32}\}.$$

Proposition 5.2. *$G^{(1)}$ and $G^{(2)}$ are 2-transitive permutation groups.*

Proof. By Proposition 5.1, $G^{(1)}$ and $G^{(2)}$ are transitive permutation groups. Let $t \in \{1,2\}$ and $z = 0^{64}$. We have

$$\begin{aligned}
((R^{(t)}_{k_n,l_n})^{-1} \circ R^{(t)}_{k'_n,l'_n}) \circ \cdots \circ ((R^{(t)}_{k_1,l_1})^{-1} \circ R^{(t)}_{k'_1,l'_1})(a,b) &= (a, b \oplus F^{(t)}_{k_1,l_1}(a) \oplus F^{(t)}_{k'_1,l'_1}(a) \oplus \cdots \oplus F^{(t)}_{k_n,l_n}(a) \oplus F^{(t)}_{k'_n,l'_n}(a)),\\
(R^{(t)}_{k_n,l_n} \circ (R^{(t)}_{k'_n,l'_n})^{-1}) \circ \cdots \circ (R^{(t)}_{k_1,l_1} \circ (R^{(t)}_{k'_1,l'_1})^{-1})(a,b) &= (a \oplus F^{(t)}_{k_1,l_1}(b) \oplus F^{(t)}_{k'_1,l'_1}(b) \oplus \cdots \oplus F^{(t)}_{k_n,l_n}(b) \oplus F^{(t)}_{k'_n,l'_n}(b), b)
\end{aligned}$$

for all $n \geq 1$, $(k_1,l_1), (k'_1,l'_1), \ldots, (k_n,l_n), (k'_n,l'_n) \in \{0,1\}^{96} \times \{0,1\}^{32}$, and $a, b \in \{0,1\}^{32}$. Hence, by Lemma 4.5, for every $c, d, c', d' \in \{0,1\}^{32}$ there are functions $f, g \in G^{(1)}_z$ with

$$f(c,d) = (c,d') \quad \text{and} \quad g(c,d') = (c',d').$$

Thus, $G^{(1)}_z$ is transitive on $\{0,1\}^{64} \setminus \{z\}$ and, by the same arguments, also $G^{(2)}_z$ is transitive on $\{0,1\}^{64} \setminus \{z\}$. Then $G^{(1)}$ and $G^{(2)}$ are 2-transitive permutation groups by Proposition 2.1. □

A permutation $F : \{0,1\}^{2n} \to \{0,1\}^{2n}$, $n > 0$, is said to be of *Feistel-type* if there is a mapping $f : \{0,1\}^n \to \{0,1\}^n$ with $F(x,y) = (y, x \oplus f(y))$ for all $(x,y) \in \{0,1\}^n \times \{0,1\}^n$.

The average cycle length of a random permutation on the set $\{0,1\}^{2n}$ is approximately equal to $2^{2n}/\ln 2^{2n}$ (see [9, pp. 257–258]). It can be shown that for every Feistel-type permutation F on $\{0,1\}^{2n}$, $n \geq 4$, the cycle representation of F contains at least 2^{n-1} cycles (see [5, Lemma 3]). Since the KASUMI round functions are inverse Feistel-type permutations, the average cycle length for every KASUMI round function is not greater than 2^{33}. Thus, it is feasible to use Proposition 2.4 for the proof of the following result.

Theorem 5.3. *The groups generated by the KASUMI round functions of odd and even round type are equal to the alternating group on the set $\{0,1\}^{64}$.*

Proof. $G^{(1)}$ and $G^{(2)}$ are primitive by Proposition 5.2 and contain only even permutations by [8, Corollary 2]. The following two large cycles for the first resp. second KASUMI round function have been obtained by a random search.

For the first KASUMI round function defined by the cipher key

$$k = \text{0xe18d9e90077d5bff59c9c9f1d3e22403},$$

the cycle starting at 0x0211f74b7527ce8b is of length $c = 18\,375\,676\,469$.

For the second KASUMI round function defined by the cipher key

$$k' = \text{0x294635be4374a0fe1b3ae978e199ee18},$$

the cycle starting at 0x85346017c65edd91 is of length $c' = 13\,535\,443\,601$. Since c and c' are primes with $c, c' > 2^{33}$ satisfying the condition of Proposition 2.4, the groups $G^{(1)}$ and $G^{(2)}$ are both equal to the alternating group on the set $\{0,1\}^{64}$. □

Remark 5.4. Since the KASUMI key scheduling maps the set of possible keys onto the set of round keys, the actual KASUMI round functions both for odd and even rounds generate the alternating group on $\{0,1\}^{64}$.

6 The KASUMI two-round functions generate the alternating group

Let G^* denote the group generated by the set of KASUMI two-round functions

$$\{R^{(2)}_{k',l'} \circ R^{(1)}_{k,l} : k,k' \in \{0,1\}^{96},\ l,l' \in \{0,1\}^{32}\},$$

where independent round keys are assumed. In this section, we show that G^* is equal to the alternating group on the set $\{0,1\}^{64}$. Then it follows that also the KASUMI encryption functions with independent round keys generate the alternating group on the message space (cf. Theorem 6.7).

Proposition 6.1. *The group G^* is 2-transitive, hence primitive.*

Proof. The group G^* is transitive by Proposition 5.1, and we have

$$\begin{aligned}(R^{(1)}_{k_1,l_1})^{-1} \circ R^{(1)}_{k_2,l_2} &= (R^{(2)}_{k_3,l_3} \circ R^{(1)}_{k_1,l_1})^{-1} \circ (R^{(2)}_{k_3,l_3} \circ R^{(1)}_{k_2,l_2}),\\ R^{(2)}_{k_1,l_1} \circ (R^{(2)}_{k_2,l_2})^{-1} &= (R^{(2)}_{k_1,l_1} \circ R^{(1)}_{k_3,l_3}) \circ (R^{(2)}_{k_2,l_2} \circ R^{(1)}_{k_3,l_3})^{-1}\end{aligned}$$

for all $(k_1,l_1),(k_2,l_2),(k_3,l_3) \in \{0,1\}^{96} \times \{0,1\}^{32}$. Then, similar to the proof of Proposition 5.2, it follows that G^* is a 2-transitive group. □

Remark 6.2. Similar to the preceding proof we can show that the group G_{enc} generated by the KASUMI encryption functions f_{enc} with independent round keys is 2-transitive. Thus G_{enc} acts primitively on the message space.

We say a Feistel-type permutation F with $F(x,y) = (y, x \oplus f(y))$ for all $(x,y) \in \{0,1\}^n \times \{0,1\}^n$ is *proper* if $f^{-1}(0^n) \neq \emptyset$. We first provide a useful lower bound for the number of cycles of compositions consisting of a proper Feistel-type permutation on $\{0,1\}^{2n}$ and a more general type of permutation, which shows that the average cycle length of such compositions is not greater than 2^{n+1}. Since G^* is primitive, this opens up the possibility to use Proposition 2.4 for the proof that G^* equals the alternating group on the message space (cf. Theorem 6.6).

Theorem 6.3. *Let $n \geq 1$ and $\theta(x,y) = (y,x)$ for all $(x,y) \in \{0,1\}^n \times \{0,1\}^n$. Let further $\varphi : \{0,1\}^{2n} \to \{0,1\}^{2n}$ be a permutation with $\varphi \circ \theta = \theta \circ \varphi^{-1}$. Then for every proper Feistel-type permutation $F : \{0,1\}^{2n} \to \{0,1\}^{2n}$ the cycle representation of $\varphi \circ F$ contains at least 2^{n-1} cycles.*

Proof. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a mapping with $f^{-1}(0^n) \neq \emptyset$ and $F(x,y) = (y, x \oplus f(y))$ for all $(x,y) \in \{0,1\}^n \times \{0,1\}^n$. We show that every cycle of $\varphi \circ F$ contains no more than two elements from the set

$$S = \{(x,y) \in \{0,1\}^n \times \{0,1\}^n : f(y) = 0^n\}.$$

Let $(a,b) \in S$. Then $F(a,b) = \theta(a,b)$ and $\varphi(F(a,b)) = \theta(\varphi^{-1}(a,b)) = \theta(F((\varphi \circ F)^{-1}(a,b)))$. Induction yields

$$(\varphi \circ F)^i(a,b) = \theta(F((\varphi \circ F)^{-i}(a,b)))$$

for every integer $i > 0$. Let $i_0 > 0$ be the smallest integer such that $(\varphi \circ F)^{i_0}(a,b) \in S$ or $(\varphi \circ F)^{-i_0}(a,b) \in S$. In the first case

$$F((\varphi \circ F)^{i_0}(a,b)) = \theta((\varphi \circ F)^{i_0}(a,b)) = F((\varphi \circ F)^{-i_0}(a,b)).$$

In the second case we have

$$F((\varphi \circ F)^{-i_0}(a,b)) = \theta((\varphi \circ F)^{-i_0}(a,b)),$$

hence $(\varphi \circ F)^{-i_0}(a,b) = \theta(F((\varphi \circ F)^{-i_0}(a,b))) = (\varphi \circ F)^{i_0}(a,b)$. Thus, (a,b) and $(\varphi \circ F)^{i_0}(a,b)$ are the only elements of S occurring in the cycle starting from (a,b). Since $|S| \geq 2^n$, the cycle representation of $\varphi \circ F$ contains at least 2^{n-1} cycles. □

Corollary 6.4. *Let $F, F' : \{0,1\}^{2n} \to \{0,1\}^{2n}$ be two Feistel-type permutations, where F is proper. Then the cycle representation of $F' \circ F$ contains at least 2^{n-1} cycles.*

The average cycle length of a random permutation on the set $\{0,1\}^{64}$ is a number greater than 2^{58} (see [9, pp. 257–258]). Since the KASUMI round functions are the inverses of proper Feistel-type permutations, we have the following result.

Corollary 6.5. *The average cycle length for every KASUMI two-round function is not greater than* 2^{33}.

Theorem 6.6. *The group* G^* *generated by the KASUMI two-round functions with independent round keys is equal to the alternating group on the message space.*

Proof. The group G^* is primitive by Proposition 6.1 and contains only even permutations by [8, Corollary 2]. The KASUMI cipher key

$$k = \mathrm{0x6205b5d9ee63edf11f1acea14477d5a9}$$

with the following property has been obtained by random search. The composition of the first two KASUMI round functions defined by the cipher key k has the cycle

$$(\mathrm{0x445b1b948ce25f49} \cdots \mathrm{0x3e72cc3296b66829})$$

of length $c = 28\,737\,645\,371$, where c is a prime with $c > 2^{33}$ satisfying the condition of Proposition 2.4. Hence G^* is equal to the alternating group on the set $\{0,1\}^{64}$. □

Theorem 6.7. *The group generated by the KASUMI encryption functions with independent round keys is equal to the alternating group on the message space.*

Proof. The group generated by the KASUMI encryption functions with independent round keys is a normal subgroup of G^* (see [10]). Since the alternating group on $\{0,1\}^{64}$ is simple, the result follows from Theorem 6.6. □

7 Conclusions

Possible structural defects of the groups generated by the KASUMI round functions and two-round functions, such as imprimitivity or an insufficient diversity of occurring permutations, can be excluded by the results provided in the paper.

Furthermore, by Theorem 6.6, for all Markov ciphers corresponding to KASUMI two-round functions, the Markov chains of differences are irreducible and aperiodic [10]. If the hypothesis of stochastic equivalence holds for the Markov ciphers corresponding to KASUMI two-round functions, then these ciphers are secure against classical differential cryptanalysis after the application of sufficiently many two-round functions [10].

Finally, it appears that the methods used here to prove the main results cannot be employed to show that the KASUMI round functions without the linear mixing permutations generate the alternating group on the message space (cf. Proposition 4.6).

A Properties of the FI-permutations

We provide here some properties of the permutations $\mu(v,w) = (\mathrm{S7}(v) \oplus v \oplus \mathrm{pr}(\mathrm{S9}(w)), (0^2, v) \oplus \mathrm{S9}(w))$ for $(v,w) \in \{0,1\}^7 \times \{0,1\}^9$ and $FI_z = \mu \circ \sigma_z \circ \mu \circ \mathrm{rot}_9$ for $z \in \{0,1\}^{16}$. These properties are used for the proof of Proposition 4.6, but might also be of interest on their own.

For every mapping $f : \{0,1\}^n \to \{0,1\}^n$ and $a \in \{0,1\}^n$, let $D_a f : \{0,1\}^n \to \{0,1\}^n$ denote the derivative of f with respect to a defined by

$$D_a f(x) = f(x) \oplus f(x \oplus a)$$

for all $x \in \{0,1\}^n$. For the derivatives of the permutation μ with respect to elements of the form $a \in \{0,1\}^7 \times \{0^9\}$ we have the following two properties.

Proposition A.1. *$D_a\mu(v,w) \in \{0,1\}^7 \times \{0^2\} \times \{0,1\}^7$ for all $(v,w) \in \{0,1\}^7 \times \{0,1\}^9$ and $a \in \{0,1\}^7 \times \{0^9\}$.*

Proposition A.2. *$D_a\mu(v,w) \oplus D_a\mu(v',w') \in \{0,1\}^7 \times \{0^9\}$ for every (v,w), $(v',w') \in \{0,1\}^7 \times \{0,1\}^9$ and $a \in \{0,1\}^7 \times \{0^9\}$.*

Proof. Let (v,w), $(v',w') \in \{0,1\}^7 \times \{0,1\}^9$ and $a = (b,0^9) \in \{0,1\}^7 \times \{0^9\}$. Then

$$\mu(v' \oplus b, w') \oplus \mu(v', w') = \big(\mathrm{S7}(v' \oplus b) \oplus \mathrm{S7}(v') \oplus b, 0^2, b\big) = \mu(v \oplus b, w) \oplus \mu(v,w) \oplus (c, 0^9)$$

with $c = \mathrm{S7}(v' \oplus b) \oplus \mathrm{S7}(v') \oplus \mathrm{S7}(v \oplus b) \oplus \mathrm{S7}(v)$. □

Proposition A.3. *Let $y, y', z, z' \in \{0,1\}^{16}$ with $FI_z(y) = FI_{z'}(y')$. Then $FI_z(y \oplus x) \oplus FI_{z'}(y' \oplus x) \in \{0,1\}^7 \times \{0^2\} \times \{0,1\}^7$ for every $x \in \{0^9\} \times \{0,1\}^7$.*

Proof. Let $y = (w,v)$, $y' = (w',v')$ with $v, v' \in \{0,1\}^7$, $w, w' \in \{0,1\}^9$ and $x = (0^9, b)$ with $b \in \{0,1\}^7$. If $z, z' \in \{0,1\}^{16}$ with $FI_z(w,v) = FI_{z'}(w',v')$, we have $\sigma_z(\mu(v,w)) = \sigma_{z'}(\mu(v',w'))$. Let $a = (b, 0^9)$. By the preceding result we have

$$D_a\mu(v,w) \oplus D_a\mu(v',w') = (c, 0^9)$$

with $c \in \{0,1\}^7$. Then

$$\sigma_z\big(\mu(v \oplus b, w)\big) \oplus \sigma_{z'}\big(\mu(v' \oplus b, w')\big) = \sigma_z\big(\mu(v,w)\big) \oplus \sigma_{z'}\big(\mu(v',w')\big) \oplus (c, 0^9) = (c, 0^9).$$

Thus,

$$FI_z(y \oplus x) \oplus FI_{z'}(y' \oplus x) = \mu\big(\sigma_z\big(\mu(v \oplus b, w)\big)\big) \oplus \mu\big(\sigma_{z'}\big(\mu(v' \oplus b, w')\big)\big) \in \{0,1\}^7 \times \{0^2\} \times \{0,1\}^7.$$ □

Acknowledgement: We would like to thank Harry Reimann for valuable comments and discussions.

References

[1] 3GPP TR 33.908 V4.0.0 (2001-09), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms (Release 4), www.3gpp.org.

[2] T. Baignères and S. Vaudenay, Proving the security of AES substitution-permutation network, in: *Selected Areas in Cryptography* (SAC 2005), Lecture Notes in Comput. Sci. 3897, Springer, Berlin (2006), 65–81.

[3] A. Caranti, F. Dalla Volta and M. Sala, An application of the O'Nan-Scott theorem to the group generated by the round functions of an AES-like cipher, *Des. Codes Cryptography* **52** (2009), 293–301.

[4] Data Encryption Standard (DES), National Institute of Standards and Technology, FIPS Publication 46 (3), 1999.

[5] R. Dittmar, G. Hornauer and R. Wernsdorf, SAFER, DES and FEAL: Algebraic properties of the round functions, in: *Proceedings of PRAGOCRYPT'96*, part I, CTU Publishing House, Prague (1996), 55–66.

[6] O. Dunkelman, N. Keller and A. Shamir, A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony, in: *Advances in Cryptology* (CRYPTO 2010), Lecture Notes in Comput. Sci. 6223, Springer, Berlin (2010), 393–410.

[7] ETSI TS 135 202 V7.0.0 (2007-06), Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 2: KASUMI specification (3GPP TS 35.202 version 7.0.0 Release 7), www.etsi.org.

[8] S. Even and O. Goldreich, DES-like functions can generate the alternating group, *IEEE Trans. Inform. Theory* **29** (1983), 863–865.

[9] W. Feller, *An Introduction to Probability Theory and Its Applications*, vol. 1, 3rd ed., John Wiley & Sons, New York, 1968.

[10] G. Hornauer, W. Stephan and R. Wernsdorf, Markov ciphers and alternating groups, in: *Advances in Cryptology* (EUROCRYPT'93), Lecture Notes in Comput. Sci. 765, Springer, Berlin (1994), 453–460.

[11] T. Iwata, T. Yagi and K. Kurosawa, On the pseudorandomness of KASUMI type permutations, in: *Information Security and Privacy* (ACISP 2003), Lecture Notes in Comput. Sci. 2727, Springer, Berlin (2003), 130–141.

[12] K. Jia, L. Li, C. Rechberger, J. Chen and X. Wang, Improved cryptanalysis of the block cipher KASUMI, in: *Selected Areas in Cryptography* (SAC 2012), Lecture Notes in Comput. Sci. 7707, Springer, Berlin (2013), 222–233.

[13] T. V. Le, R. Sparr, R. Wernsdorf and Y. Desmedt, Complementation-like and cyclic properties of AES round functions, in: *Advanced Encryption Standard* (AES 2004), Lecture Notes in Comput. Sci. 3373, Springer, Berlin (2005), 128–141.

[14] M. W. Liebeck and J. Saxl, Primitive permutation groups containing an element of large prime order, *J. London Math. Soc. (2)* **31** (1985), 237–249.

[15] M. Matsui, New block encryption algorithm MISTY, in: *Fast Software Encryption* (FSE'97), Lecture Notes in Comput. Sci. 1267, Springer, Berlin (1997), 54–68.

[16] L. O'Connor and J. Golic, A unified Markov approach to differential and linear cryptanalysis, in: *Advances in Cryptology* (ASIACRYPT'94), Lecture Notes in Comput. Sci. 917, Springer, Berlin (1995), 387–397.

[17] K. G. Paterson, Imprimitive permutation groups and trapdoors in iterated block ciphers, in: *Fast Software Encryption* (FSE'99), Lecture Notes in Comput. Sci. 1636, Springer, Berlin (1999), 201–214.

[18] C. E. Praeger, On elements of prime order in primitive permutation groups, *J. Algebra* **60** (1979), 126–157.

[19] T. Saito, A single-key attack on 6-round KASUMI, preprint (2011), http://eprint.iacr.org/2011/584.

[20] A. Seress, *Permutation Group Algorithms*, Cambridge University Press, Cambridge, 2002.

[21] R. Sparr and R. Wernsdorf, Group theoretic properties of Rijndael-like ciphers, *Discr. Appl. Math.* **156** (2008), 3139–3149.

[22] Specification for the Advanced Encryption Standard (AES), National Institute of Standards and Technology, FIPS Publication 197, 2001.

[23] R. Wernsdorf, The one-round functions of the DES generate the alternating group, in: *Advances in Cryptology* (EUROCRYPT'92), Lecture Notes in Comput. Sci. 658, Springer, Berlin (1993), 99–112.

[24] R. Wernsdorf, The round functions of Rijndael generate the alternating group, in: *Fast Software Encryption* (FSE 2002), Lecture Notes in Comput. Sci. 2365, Springer, Berlin (2002), 143–148.

[25] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

Received August 6, 2013; revised July 28, 2014; accepted August 7, 2014.