Cryptanalysis of Reduced-Round MISTY

Ulrich Kühn

Dresdner Bank AG
Group Information Technology
RS Research
D-60301 Frankfurt
Germany
Ulrich.Kuehn@dresdner-bank.com

Abstract. The block ciphers MISTY1 and MISTY2 proposed by Matsui are based on the principle of provable security against differential and linear cryptanalysis. This paper presents attacks on reduced-round variants of both ciphers, without as well as with the key-dependent linear functions FL. The attacks employ collision-searching techniques and impossible differentials. KASUMI, a MISTY variant to be used in next generation cellular phones, can be attacked with the latter method faster than brute force when reduced to six sounds.

1 Introduction

The MISTY algorithms proposed by Matsui [8] are designed to be resistant against differential [3] and linear [7] cryptanalysis. One design criterion is that no single differential or linear characteristic with a usable probability does hold for the cipher. An additional feature is the use of key-dependent linear functions which were introduced to counter other than differential and linear attacks.

Previous attacks by Tanaka, Hisamatsu and Kaneko [12] on MISTY1 and by Sugita [10] on MISTY2 employ higher order differentials against 5-round variants without the linear FL functions. A cryptographic weakness of the round construction of MISTY2 was pointed out by Sakurai and Zheng [9].

In this paper we present attacks on reduced-round variants of MISTY1 and MISTY2, both without and with the key-dependent linear functions FL. The round function involves a huge amount of keying material, so it is one purpose of this paper to point out properties of the round function that allow to use divide-and-conquer techniques on the subkeys in order to improve basic attacks which make use of impossible differentials [2, 5] and collision-searching [1]; the latter technique is extended by using multiple permutations. Furthermore reduced-round KASUMI, a MISTY variant to be used in next generation cellular phones, is attacked with impossible differentials. Table 1 shows a summary of the attacks.

This paper is organised as follows. The MISTY algorithms are described in Section 2; properties of the key scheduling and the round function that are used here are explained in Section 3; the new attacks on MISTY1 resp. MISTY2 are described in Section 4 resp. 5. A comparison to KASUMI is made in Section 6. Conclusions are drawn in Section 7.

Cipher	FL functions	Rounds	Complexity [data]	[time]	Comments
MISTY1	–	5	11×2^7	2^{17}	[12] (previously known)
	–	5	2^6	2^{38}	[10, 11] (previously known)
	–	6	2^{39}	2^{106}	impossible differential (new)
	–	6	2^{54}	2^{61}	impossible differential (new)
	✓	4	2^{23}	$2^{90.4}$	impossible differential (new)
	✓	4	2^{38}	2^{62}	impossible differential (new)
	✓	4	2^{20}	2^{89}	collision-search (new)
	✓	4	2^{28}	2^{76}	collision-search (new)
MISTY2	–	5	2^7	2^{39}	[10, 11] (previously known)
	✓	5	2^{23}	2^{90}	impossible differential (new)
	✓	5	2^{38}	2^{62}	impossible differential (new)
	✓	5	2^{20}	2^{89}	collision-search (new)
	✓	5	2^{28}	2^{76}	collision-search (new)
KASUMI	✓	6	2^{55}	2^{100}	impossible differential (new)

Table 1. Summary of attacks on MISTY variants.

2 Description of MISTY

The MISTY algorithms [8] are symmetric block ciphers with a block size of 64 bits and a key size of 128 bits. There are two flavors called MISTY1 and MISTY2, which differ by their global structure (see Figure 1). MISTY1 is a Feistel network with additional key-dependent linear functions FL placed in the data path before every second round. MISTY2 has a different structure that allows parallel execution of round functions during encryption. The FL functions are applied in MISTY2 to both halfs of the data before every fourth round and also in every second round just before XORing the right to the left half of the data. In both ciphers the linear functions are also used as an output transformation.

MISTY has a recursive structure, that is, the round function consists of a network with a smaller block size using the function FI that itself is again a smaller network; the structure of both the round function FO and the function FI is that of MISTY2. Figure 2 shows FO, FI and FL in a representation that is equivalent to the original description [8]. This equivalent description[1] is the result moving the mixing of the leftmost seven bits of each KI_{ij} in each FI (as given in the specification [8]) out of FI and to the end of its superstructure FO; this is possible because these key bits do not affect any S-box inside the instance of FI where they are inserted. Due to the recursive structure a huge amount of keying material is involved in each round, i.e. 112 bits for FO in

[1] For another equivalent description of MISTY's round function see [12].

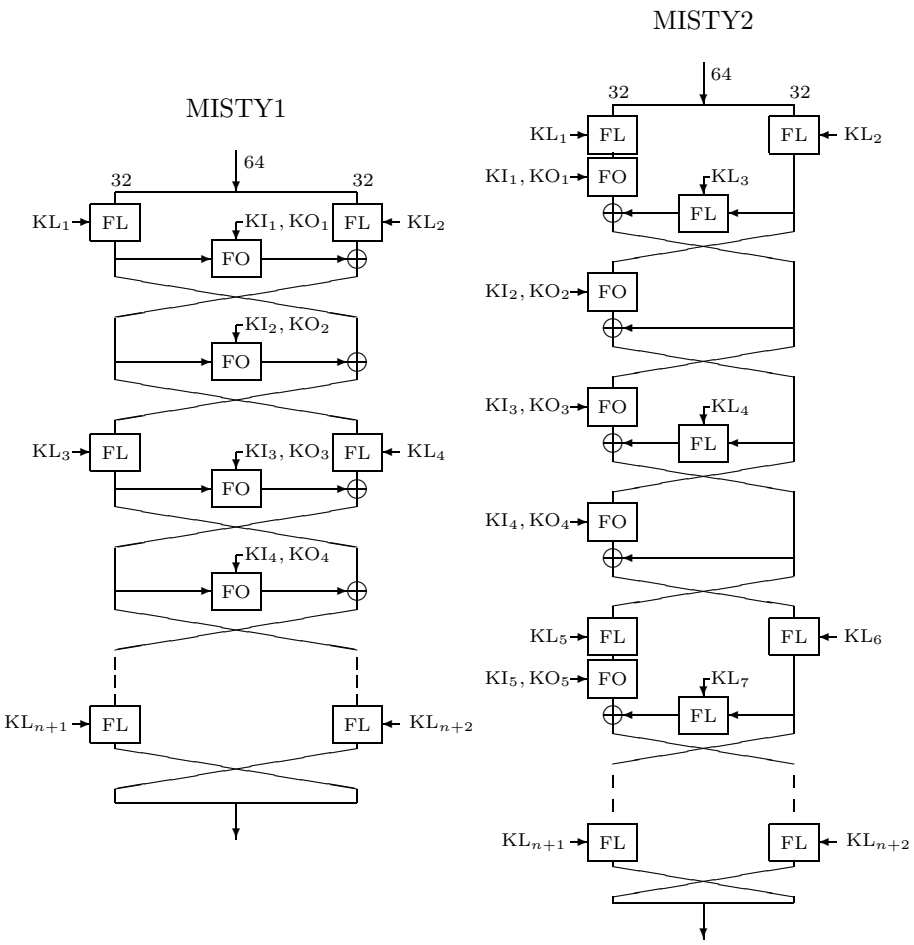

Fig. 1. Global structure of MISTY1 and MISTY2.

the original description; the equivalent description has a key size of 107 bits. Additional subkey bits are used if the round contains FL functions. The ciphers are proposed with 8 (MISTY1) resp. 12 (MISTY2) rounds.

The key scheduling takes as input a 128 bit key consisting of 16 bit values $K_1, \ldots, K_8$ and computes additional 16 bit values $K'_t = \mathrm{FI}_{K_{t+1}}(K_t)$, $1 \le t \le 8$ where $K_9 = K_1$. The subkeys of each round are (i is identified with $i - 8$ for $i > 8$):

Subkey	KO_{i1}	KO_{i2}	KO_{i3}	KO_{i4}	KI_{i1}	KI_{i2}	KI_{i3}	KL_i
Value	K_i	K_{i+2}	K_{i+7}	K_{i+4}	K'_{i+5}	K'_{i+1}	K'_{i+3}	$(K_{\frac{i+1}{2}} \| K'_{\frac{i+1}{2}+6})$ (odd i) $(K'_{\frac{i}{2}+2} \| K_{\frac{i}{2}+4})$ (even i)

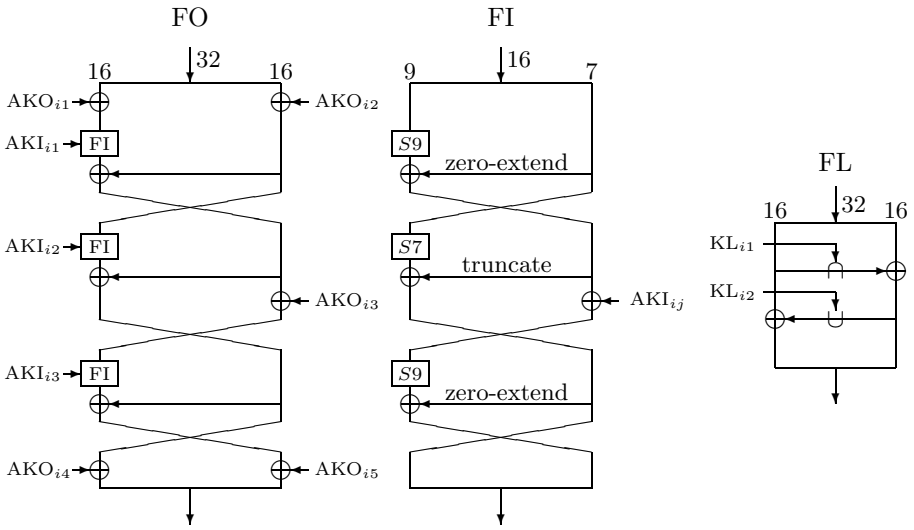

Fig. 2. The functions FO and FI in a form equivalent to the original specification which eliminates the left 7 bits of the key to FI. $S7$ and $S9$ are bijective 7×7 resp. 9×9 S-boxes; in FL the operators $\cap$ resp. $\cup$ denote the bitwise AND resp. OR.

Given $\mathrm{KO}_i = (\mathrm{KO}_{i1}, \ldots, \mathrm{KO}_{i4})$, $\mathrm{KI}_i = (\mathrm{KI}_{i1}, \ldots, \mathrm{KI}_{i3})$, then AKO_{ij} and AKI_{ij} of our equivalent description relate to the original subkeys as follows. Let $||$ denote the concatenation of bitstrings and $[x]_{i..j}$ the selection of the bits $i..j$ from x where bit 0 is the rightmost bit. Let KI'_{ij} denote the 16 bits $[\mathrm{KI}_{ij}]_{15..9}||00||[\mathrm{KI}_{ij}]_{15..9}$. Then the actual subkeys are

$$\begin{aligned}
\mathrm{AKO}_{ik} &= \mathrm{KO}_{ik}, \quad \text{with } 1 \le k \le 2 \\
\mathrm{AKO}_{i3} &= \mathrm{KO}_{i2} \oplus \mathrm{KO}_{i3} \oplus \mathrm{KI}'_{i1} \\
\mathrm{AKO}_{i4} &= \mathrm{KO}_{i2} \oplus \mathrm{KO}_{i4} \oplus \mathrm{KI}'_{i1} \oplus \mathrm{KI}'_{i2} \\
\mathrm{AKO}_{i5} &= \mathrm{KO}_{i2} \oplus \mathrm{KI}'_{i1} \oplus \mathrm{KI}'_{i2} \oplus \mathrm{KI}'_{i3} \\
\mathrm{AKI}_{ik} &= [\mathrm{KI}_{ik}]_{8..0}, \quad \text{with } 1 \le k \le 3
\end{aligned} \tag{1}$$

Notation. Throughout this paper all differences are taken as XOR of the appropriate values. Let L_i resp. R_i denote the left resp. right half of the input to round i, X_i the input to the round function FO, and Z_i its output; so L_1 resp. R_1 denotes the left resp. right half of the plaintext data. If round i uses FL in its data path (for example every odd round in MISTY1) let X_i resp. Y_i denote the left resp. right half of the data after the transformation through FL, and set $X_i = L_i$, $Y_i = R_i$ otherwise. For MISTY2 let $\tilde{Y}_i$ denote the possibly transformed value of Y_i that is XORed to Z_i to form the half of the round's output that becomes R_{i+1} after the swap.

3 Observations on the Key Scheduling and the Round Function

Key Scheduling. The key scheduling is designed such that every round is affected by all key bits. This causes major problems in terms of complexity when exhaustively guessing the subkey of one round with a distinguisher for the other rounds, but it also allows to recover the whole key with reasonable effort once a large part of one round subkey is known.

For example consider the first round's subkeys AKO_{11}, AKO_{12}, AKO_{13} and AKI_{11}, AKI_{12}, AKI_{13}. By equation 1 (and the key scheduling table in Section 2) the 16 bits of key words K_1 and K_3 are known. AKI_{12} resp. AKI_{13} provides a 9 bit condition for K_2 resp. K_4 and K_5. After guessing the 7 bits of KI'_{11} in AKO_{13} there is – knowing AKI_{11} – a 16 bit condition for K_6 and K_7; also the word K_8 is known from AKO_{13}. Using a factor of 2 for the 8 computations of FI in the key schedule the total complexity of exhaustive search is about $2 \cdot 2^{128-32} \cdot 2^{-9} \cdot 2^{-9} \cdot 2^{-32} = 2^{47}$ encryptions using two or three known plaintexts and corresponding ciphertexts.

Round function in differential and collision-searching attacks. The subkeys AKO_{i4} and AKO_{i5} are invisible in our attacks as they introduce fixed constants after all non-linearities when FO is applied in forward direction. The following properties of FO allow divide-and-conquer techniques for the other 75 subkey bits at the cost of increased chosen plaintext or ciphertext requirements.

Property 1. In forward direction, consider FO in round i having an output XOR of the form (β, β) where β is a nonzero 16 bit value. Then the input and output XOR of the third instance of FI must be zero, so $(\mathrm{AKO}_{i3}, \mathrm{AKI}_{i3})$ does not influence the output XOR. The input XOR to FO must be (α_l, α_r) such that α_r cancels the output XOR of the first FI under key $(\mathrm{AKO}_{i1}, \mathrm{AKI}_{i1})$ when the input XOR is α_l from the given input values. The value of β is solely influenced by $(\mathrm{AKO}_{i2}, \mathrm{AKI}_{i2})$.

Property 2. In forward direction, consider inputs to FO in round i of the form (a_i, b) where the a_i are all different (thus forming a permutation in the notation of [1]) and b is a constant. Then the output of the second FI is a constant that depends on AKO_{i2} and AKI_{i2}; the input of the third FI is a permutation, namely the XOR of the output of the first FI and $b \oplus \mathrm{AKO}_{i2} \oplus \mathrm{AKO}_{i3}$. As long as $\mathrm{AKO}_{i2} \oplus \mathrm{AKO}_{i3}$ has the same value as for the unknown key, and AKO_{i1}, AKI_{i1} and AKI_{i3} are also correct, the output of FO is the same as for the correct subkey, up to XORing with a constant. So one can set $\mathrm{AKO}_{i2} = 0$, $\mathrm{AKI}_{i2} = 0$ in a first step, making sure that $\mathrm{AKO}_{i2} \oplus \mathrm{AKO}_{i3}$ has the correct value.

Directional Asymmetry. Due to the Feistel network, FO is used in MISTY1 in forward direction both for encrypting and decrypting data. But for MISTY2 this is not the case. In forward direction the output of the second FI does not

affect the input of the third FI; this fact is inherently used in both properties explained above. In backward direction, the output of the first and second FI each affect the input of every subsequent FI, which makes analysis harder in this direction. This is the reason that for MISTY2 the attacks presented in this paper use the chosen ciphertext model of attack, as then FO in the first round can be used in forward direction.

4 Attacks on Reduced-Round MISTY1

In this section we present attacks on MISTY1; it is assumed that the final swap of MISTY is also present in the reduced variant. One attack finds the last round subkey of 6 rounds of MISTY1 without FL functions, other attacks find the last round subkey of MISTY1 reduced to 4 rounds with FL functions but without the final output transformation; these attacks break exactly half of the cipher.

4.1 Attacking MISTY1 without FL Functions

This attack is based on the generic 5-round impossible differential for Feistel networks with bijective round functions

$$(0,0,\alpha_l,\alpha_r) \overset{5R}{\not\to} (0,0,\alpha_l,\alpha_r), \quad (\alpha_l,\alpha_r) \neq (0,0),$$

discovered by Knudsen [5]. The attack looks for differences $(\beta_l,\beta_r,\alpha_l,\alpha_r)$ after 6 rounds (including the final swap) and rules out all subkeys that can yield $(\alpha_l,\alpha_r) \to (\beta_l,\beta_r)$ from the given outputs, as that is impossible.

The basic attack uses a structure of 2^{32} chosen plaintexts $P_i = (x, y, a_i, b_i)$ with some fixed values x, y and (a_i, b_i) running through all 2^{32} values. After obtaining the corresponding ciphertexts (c_i, d_i, e_i, f_i) by encryption under the unknown key set up a list of values $w_i = (a_i, b_i) \oplus (e_i, f_i)$. For a pair i, j such that $w_i = w_j$ the input difference is $(0, 0, \alpha_l, \alpha_r)$ with $(\alpha_l, \alpha_r) = (a_i \oplus a_j, b_i \oplus b_j)$; the output difference after six rounds and the final swap is $(\beta_l, \beta_r, \alpha_l, \alpha_r)$ with $(\beta_l, \beta_r) = (c_i \oplus c_j, d_i \oplus d_j)$. Now check for all 75 bit subkeys $k = (\mathrm{AKO}_{61}, \mathrm{AKI}_{61}, \ldots, \mathrm{AKO}_{63}, \mathrm{AKI}_{63})$ if $\mathrm{FO}_k((e_i, f_i)) \oplus \mathrm{FO}_k((e_j, f_j)) = (\beta_l, \beta_r)$. Such a subkey is wrong while a correct guess never yields this difference.

About $\binom{2^{32}}{2} \cdot 2^{-32} \approx 2^{31}$ pairs $w_i = w_j$ are expected in a structure. A wrong key has a probability of about 2^{-32} to cause a given output XOR, so a fraction of $(1 - 2^{-32})^{2^{31}} = \mathrm{e}^{-1/2}$ of the wrong subkeys are discarded. After repeating this basic step $75/\log_2(\mathrm{e}^{1/2}) \approx 104$ times only the correct subkey is expected to survive.

This attack takes about $104 \cdot 2^{32} \approx 2^{39}$ chosen plaintexts. The time complexity is $2 \cdot 2^{31}$ computations of FO per guessed key and per structure, so the total complexity is about $\left(\sum_{i=0}^{103} (\mathrm{e}^{-1/2})^i\right) \cdot 2^{75+32} \approx 2^{108.4}$ evaluations of FO which is equivalent to about 2^{106} encryptions of 6-round MISTY1 without FL functions; this is hardly a practical attack.

It is possible to reduce the amount of work at the cost of increased chosen plaintext requirements using Property 1 of FO (see Section 3). Using the above structure of plaintexts and their ciphertexts set up a list of (w_i, u_i) with $w_i = (a_i \oplus e_i, b_i \oplus f_i)$ and $u_i = c_i \oplus d_i$. Now only matches with $w_i = w_j$ and $u_i = u_j$ are of interest which yield $(c_i, d_i, e_i, f_i) \oplus (c_j, d_j, e_j, f_j) = (\beta, \beta, \alpha_l, \alpha_r)$. About $\binom{2^{32}}{2} \cdot 2^{-32} \cdot 2^{-16} \approx 2^{15}$ matches are expected with this form; these pairs are analysed. We determine subkeys that yield $(\alpha_l, \alpha_r) \rightarrow (\beta, \beta)$ via FO as follows (such a subkey cannot be the correct one). For each $(\mathrm{AKO}_{61}, \mathrm{AKI}_{61})$ we check if the first FI gives output XOR α_r from e_i, e_j. Then each guess of $(\mathrm{AKO}_{62}, \mathrm{AKI}_{62})$ is checked if it yields output XOR β by the second instance of FI. Each part results in about 2^9 candidates due to a 16 bit restriction.

Each structure is expected to discard about $2^{9+9} \cdot 2^{15} = 2^{33}$ 50 bit key candidates. Due to collisions a fraction of 1/e of the wrong keys is expected to remain after 2^{17} structures, but using in total $2^{17} \ln 2^{50} \approx 2^{17} \cdot 2^5$ structures, only the correct subkey remains. Thus about $2^{32} \cdot 2^{22} = 2^{54}$ chosen plaintexts with about $2^{15} \cdot 2^{22} = 2^{37}$ analysed pairs are needed. The time complexity of this part is $2 \cdot 2 \cdot 2^{25}$ evaluations of FI per analysed pair equivalent to about 2^{26} evaluations of FO. In total this is $2^{26} \cdot 2^{37} = 2^{63}$ evaluations of FO equivalent to about 2^{61} encryptions of 6-round MISTY1 without FL functions.

It remains to determine the 25 key bits $(\mathrm{AKO}_{63}, \mathrm{AKI}_{63})$ using the basic attack with $25/\log_2(\mathrm{e}^{1/2}) \approx 35$ structures requiring $2^{38.2}$ chosen plaintexts which can be reused from previous structures. The time complexity of this second part is about $\left(\sum_{i=0}^{34} (e^{-1/2})^i\right) \cdot 2^{25+32} \approx 2^{58.4}$ evaluations of FO equivalent to about 2^{56} encryptions, which is much less than for the first part.

In total this attack needs about 2^{54} chosen plaintexts and time comparable to 2^{61} encryptions; about 2^{37} pairs are analysed.

4.2 Attacking MISTY1 with FL Functions

Here we show two attacks on 4-round MISTY1 where FL functions are present with the exception of the final output transformation. One attack uses an impossible differential, the other uses the collision-searching technique of Biham's attack on Ladder-DES [1]; in order to use Property 2 we extend this technique by employing multiple permutations.

Differential-style attack. The impossible differential used to attack MISTY1 without the FL functions does not work here. The problem occurs because FL changes nonzero differences.

Lemma 1. *The generic 5-round impossible differential for Feistel networks does not work for MISTY1 with the keyed linear functions* FL.

Proof. Assume that the differential starts at an odd-numbered round, i.e. a round where the FL functions are applied in, w.l.o.g. at round 1. The difference in the R_i is changed by FL for $i \in \{1, 3, 5\}$. For the impossible differential to work the

differences in Y_3 and L_4 have to be the same, and thus the output XOR of the round function must be zero (which is impossible). But as the application of FL in general changes the differences, this cannot be assured. In the second case the differential starts at an even numbered round, i.e. a round where FL is not applied in; here the reasoning goes along the same lines. □

The following 3-round impossible differential does work since FL cannot change zero differences. An input difference $(0, 0, \alpha_l, \alpha_r)$ to round 1 with some nonzero values α_l, α_r cannot yield an output difference of $(0, 0, \delta_l, \delta_r)$ before the swap in round 3 for a nonzero values δ_l, δ_r. After round 1 the difference is $(\beta_l, \beta_r, 0, 0)$ for some nonzero β_l, β_r as FL is bijective. Going backwards from round 3, the output difference of round 2 (before the swap) must have been $(\gamma_l, \gamma_r, 0, 0)$ with nonzero γ_l, γ_r which is only possible if $(\gamma_l, \gamma_r) = (\beta_l, \beta_r)$ and if FO causes a zero output difference which is impossible. Basically the same argument works when the differential starts at round 2, where the nonzero part of the difference is changed in round 3.

The attack works along similar lines as in Section 4.1 but uses structures of 2^{16} plaintexts $P_i = (x, y, a_i, b_i)$ where x, y are constant and the (a_i, b_i) all different. Let (c_i, d_i, e_i, f_i) denote the ciphertexts. For each structure all about 2^{31} pairs can be used which rule out a fraction of about $\mathrm{e}^{-1/2}$ of the wrong keys. This attack requires about $75/\log_2(\mathrm{e}^{1/2}) \approx 104$ structures (2^{23} chosen plaintexts) and about $\left(\sum_{i=0}^{74}(\mathrm{e}^{-1/2})^i\right) \cdot 2^{75+16} \approx 2^{92.4}$ evaluations of FO comparable to $2^{90.4}$ encryptions.

We can improve this result by using Property 1. From the ciphertexts a list $u_i = c_i \oplus d_i$ is set up. So we can easily find those pairs which yield an output XOR $(\beta, \beta, \alpha_l, \alpha_r)$; their number is expected to be 2^{15} per structure. The analysis of the first part from the improved analysis in Section 4.1 can be used for finding AKO_{41},AKO_{42}, AKI_{41}, and AKI_{42} requiring about $2^{17} \cdot 2^5 = 2^{22}$ structures (2^{38} chosen plaintexts) and $2^{22} \cdot 2^{16} \cdot 2^{26} = 2^{64}$ computations of FO comparable to 2^{62} encryptions. The second part for recovering AKO_{43} and AKI_{43} needs another $\left(\sum_{i=0}^{24}(e^{-1/2})^i\right) \cdot 2^{25+16} \approx 2^{42.4}$ computations of FO where the needed plaintexts/ciphertexts are reused. In total this attack needs 2^{38} chosen plaintexts and work of about 2^{62} encryptions.

Attack using collisions. Biham's attack on Ladder-DES [1] is also applicable to 4 round MISTY1 with FL functions, as these are bijective and thus cannot produce collisions. Consider a collection of chosen plaintexts of the form (x, y, a_i, b_i) with $i \in I$ for some index set I where x, y are constants and (a_i, b_i) different random values. Using the notation from [1] this property of the collection of $\{(a_i, b_i)\}_{i \in I}$ is called a *permutation*, that is, there can be no collision.

By the FL functions X_1 is a constant (x', y'), and Y_1 is a permutation, say $\{(a'_i, b'_i)\}_{i \in I}$. Z_1 is another fixed constant (x'', y'') derived from (x', y') by FO, so $L_2 = X_2$ is the permutation $\{(a'_i \oplus x'', b'_i \oplus y'')\}_{i \in I}$ while $R_2 = Y_2$ is constant. Then Z_2 is yet another permutation, and so is L_3. X_3 is still a permutation after the FL in round 3, as is Z_3, but $Z_3 \oplus Y_3$ behaves like a pseudo-random function.

The attack proceeds as follows. Prepare 2^{20} plaintexts $P_i = (x, y, a_i, b_i)$ and get their encryptions $C_i = (c_i, d_i, e_i, f_i)$ under the unknown key. For all guesses $k = (\mathrm{AKO}_{41}, \mathrm{AKI}_{41}, \ldots, \mathrm{AKO}_{43}, \mathrm{AKI}_{43})$ of the last round's FO 75 bit key decrypt the ciphertexts one round

$$w_i = \mathrm{FO}_k((e_i, f_i)) \oplus (c_i, d_i).$$

If $w_i = w_j$ for some i, j then the key guess is wrong. The one-round decryption with a wrong key behaves like a pseudo-random function, so on average about 2^{16} decryptions are needed to eliminate a wrong guess; a correct guess never produces a collision. The attack needs 2^{20} chosen plaintexts and at most $2^{20} \cdot 2^{75} = 2^{95}$ evaluations of FO. But on average a wrong guess should be ruled out after about 2^{16} tries, so the workload is expected to be about $2^{16} \cdot 2^{75} = 2^{91}$ evaluations of FO equivalent to 2^{89} encryptions.

The probability of each wrong key guess to survive is the probability that all 2^{20} decrypted values are distinct. By the birthday paradox this probability is $\exp(-2^{20}(2^{20} - 1)/(2 \cdot 2^{32})) \approx \exp(-2^7) \approx 2^{-184}$, so for all keys the probability for a false guess to survive is 2^{-109}.

This attack can be improved using Property 2 at the cost of more chosen plaintexts. This version uses 2^{28} chosen plaintexts $P_i = (x, y, a_i, b_i)$ with constants x, y and all different (a_i, b_i). The ciphertexts $C_i = (c_i, d_i, e_i, f_i)$ are partitioned into sets B_t, $t \in \{0, \ldots, 2^{16} - 1\}$, such that $C_i \in B_t \Leftrightarrow f_i = t$. First, set $\mathrm{AKO}_{42} = 0$, $\mathrm{AKI}_{42} = 0$. For each guess $k = (\mathrm{AKO}_{41}, \mathrm{AKI}_{41}, k_{23}, \mathrm{AKI}_{43})$ of 50 bits with k_{23} in the role of AKO_{43} and each B_t, $0 \le t \le 2^{16} - 1$ decrypt all $C_i \in B_t$ one round yielding $w_i^t = \mathrm{FO}_{k_t}((e_i, f_i)) \oplus (c_i, d_i)$. If at one point $w_i^t = w_j^t$ then this key is discarded, and the procedure is started with the next guess. This takes at most $2^{50} \cdot 2^{28} = 2^{78}$ evaluations of FO comparable to 2^{76} encryptions to complete.

Once a correct k with $k_{23} = \mathrm{AKO}_{42} \oplus \mathrm{AKO}_{43}$ has been found the correct 25 bits $\mathrm{AKO}_{42}, \mathrm{AKI}_{42}$ with $\mathrm{AKO}_{43} = k_{23} \oplus \mathrm{AKO}_{42}$ have to be found. This time ciphertexts are used such that f_i varies. Here about 2^{20} ciphertexts from the collection of the 2^{28} should be sufficient to find the correct key. This requires work of at most $2^{20} \cdot 2^{25} = 2^{45}$ evaluations of FO equivalent to 2^{43} encryptions. The time and chosen plaintext requirements are dominated by the first part (2^{76} work and 2^{28} chosen plaintexts).

The first part uses several permutations, with the complication that the sum of the number of elements over all permutations is a constant. The probability of success can be estimated using methods from convexity theory [6]; we show that the case that all permutations are of equal size is the worst case. Let $m_t = |B_t|$ and $N = 2^{32}$. For each B_t a wrong key survives the test with probability $p_t = \exp(-\frac{m_t(m_t-1)}{2N})$ with $0 \le |m_t| \le 2^{28}$ and $\sum_{t=0}^{2^{16}-1} |m_t| = 2^{28}$. The product of all p_t is the probability of failure to eliminate the wrong key.

Lemma 2. *The function* $p(m_0, \ldots, m_{2^{16}-1}) = \prod p_t$ *with* $m_i \in \{0, \ldots, M\}$, $\sum_{i=0}^{2^{16}-1} m_i = M > 0$ *has its maximum for* $m_0 = \cdots = m_{2^{16}-1} = M/2^{16}$.

Proof. Consider the function $f(m) = \exp(-\frac{m(m-1)}{2N})$; it is clear that $\ln(f(m))$ is a concave function for $0 \leq m \leq M$. It follows from [6, Prop. E.1] that $p(m_0, \ldots, m_{2^{16}-1})$ is Schur-concave and thus has its maximum when all m_i are equal, as claimed. □

By Lemma 2 the maximum probability of each wrong key guess to survive is

$$\left(\exp(-\frac{2^{12}(2^{12}-1)}{2 \cdot 2^{32}})\right)^{2^{16}} \approx \left(\exp(-2^{-9})\right)^{2^{16}} = \exp(-2^7) \approx 2^{-184}.$$

It follows that also the probability is negligible that a single wrong key guess survives the first part. The probability that a wrong guess survives in the second part is, by the birthday paradox, about 2^{-184}, so for all 25 key bits this is about 2^{-159} which is also negligible.

5 Attacks on Reduced-Round MISTY2

While the attacks given in this section work for 5-round MISTY2 both with and without FL functions, the attacks on MISTY2 without FL functions have a much higher complexity than the one given in [10]; therefore we present here only the attacks on MISTY2 with FL functions; again we assume that the final swap but no output transformation is present.

Because of the asymmetry of the round function described in Section 3 it seems to help to attack MISTY2 in the chosen ciphertext model, as then the round function is used in the forward direction when testing a guessed value of a subkey.

Differential-style attack. This attack on 5-round MISTY2 makes use of the following impossible differential:

Proposition 1. *Given MISTY2 without* FL*, any input XOR* $(\alpha_l, \alpha_r, 0, 0)$ *with nonzero* (α_l, α_r) *to round* i *cannot yield a difference* $(\delta_1, \delta_2, \delta_1, \delta_2)$ *for any* (δ_1, δ_2) *in round* $i+3$*. Conversely, a difference* $(\delta_1, \delta_2, \delta_1, \delta_2)$*,* $(\delta_1, \delta_2) \neq (0, 0)$*, in round* $i+3$ *cannot decrypt to a difference* $(\alpha_l, \alpha_r, 0, 0)$ *before round* i*.*

For MISTY2 with FL *functions this differential is also impossible provided that* $\tilde{Y}_{i+3} = Y_{i+3}$*, i.e. round* $i+3$ *does not apply* FL *to the right half before it is XORed to the left half.*

Proof. This differential uses the miss-in-the-middle approach (see [2]) where two differentials with probability 1 are concatenated such that a contradiction arises. The 2-round differential used here has input difference $(\alpha_l, \alpha_r, 0, 0)$ and output difference $(\beta_1, \beta_2, \beta_1, \beta_2)$ which happens with probability 1. The input difference of $(\alpha_l, \alpha_r, 0, 0)$ causes a nonzero input difference for the first FO, which then becomes output difference $(\beta_1, \beta_2) \neq (0, 0)$ as FO is bijective. The XOR with the right hand side zero difference does not change this. So at the beginning of round 2 the difference is $(0, 0, \beta_1, \beta_2)$ which FO cannot change. After round 2

the difference is $(\beta_1, \beta_2, \beta_1, \beta_2)$. The same reasoning works for the backwards direction, where an output difference $(\delta_1, \delta_2, \delta_1, \delta_2) \neq (0, 0, 0, 0)$ decrypts always to $(\gamma_1, \gamma_2, 0, 0)$. Connecting two instances of this differential yields the contradiction.

When FL functions are present, the assumption on round $i + 3$ ensures that the output difference of FO in this round is zero. Application of FL in the first two rounds cannot yield a zero difference in the right half input to round $i + 2$, so the contradiction between rounds $i + 1$ and $i + 2$ still occurs. □

In oder to use this impossible differential the condition of a missing FL function in the last round must be met. From the specification of MISTY2 it is clear that if a group of 4 rounds does not employ FL functions in the fourth round the round preceeding this group also does not use FL, so no additional key material has to be guessed besides the subkey for FO. This holds for example for rounds 2 to 6.

The attack works as follows. Set up a structure of 2^{16} ciphertexts $C_i = (e_i, f_i, e_i \oplus x, f_i \oplus y)$ where x, y are constants and (e_i, f_i) are different values. Get the plaintexts $P_i = (a_i, b_i, c_i, d_i)$ by decryption under the unknown key. Every pair of ciphertexts fulfills the ciphertext condition of the impossible differential. For each pair P_i, P_j any key k to the first round that encrypts P_i and P_j to a difference $(\alpha_1, \alpha_2, 0, 0)$ must be a wrong guess, while a correct guess never yields such a contradiction. There are about 2^{31} such pairs, so that a fraction of $(1-2^{-32})^{2^{31}} = \mathrm{e}^{-1/2}$ of the wrong keys survives. Thus about $75/\log_2(\mathrm{e}^{1/2}) \approx 104$ structures (about 2^{23} chosen ciphertexts) are required to eliminate all wrong keys. The work complexity is $\left(\sum_{i=0}^{103}(\mathrm{e}^{-1/2})^i\right) \cdot 2^{75+16} \approx 2^{92.4}$ computations of FO roughly comparable to 2^{90} decryptions.

An improvement of the work factor can be reached using Property 1 in a similar way as for MISTY1 in sections 4.1 and 4.2. For the attack we use the same structures as above. From their decryptions $P_i = (a_i, b_i, c_i, d_i)$ we make a list $w_i = c_i \oplus d_i$. All matches $w_i = w_j$, $i \neq j$ yield a plaintext difference $P_i \oplus P_j = (\alpha_l, \alpha_r, \beta, \beta)$ for some value of β; these are the analysed pairs. With the input resp. output XOR (α_l, α_r) resp. (β, β) for FO in the first round we determine subkeys $(\mathrm{AKO}_{11}, \mathrm{AKI}_{11})$, $(\mathrm{AKO}_{12}, \mathrm{AKI}_{12})$ that yield this output difference from (a_i, b_i) and (a_j, b_j) as follows. For each $(\mathrm{AKO}_{11}, \mathrm{AKI}_{11})$ we check if the first FI gives output XOR α_r from a_i, a_j. Then each guess for $(\mathrm{AKO}_{12}, \mathrm{AKI}_{12})$ is checked if it yields output XOR β by the second FI. Each part is expected to result in about 2^9 candidates due to the 16 bit restriction. Each of the expected 2^{18} combinations is a wrong guess by the impossible differential.

In each structure there are about 2^{31} pairs, each of which has a chance of 2^{-16} to have a plaintext difference (β, β) in the right half. So about 2^{15} pairs are analysed, each of which excludes about 2^{18} not necessarily distinct subkey guesses. After about $2^{17} \cdot \ln(2^{50}) \approx 2^{17} \cdot 2^5$ structures (2^{38} chosen ciphertexts, 2^{37} analysed pairs) there is only a single remaining key expected. The time complexity per pair is $2 \cdot 2^{25}$ evaluations each for the first and the second FI, which is about 2^{26} evaluations of FO. In total this is about $2^{26} \cdot 2^{38} = 2^{64}$ evaluations of FO equivalent to about 2^{62} encryptions.

Determining the last 25 subkey bits AKO_{13} and AKI_{13} can be done with the basic attack and $25/\log_2(\mathrm{e}^{1/2}) \approx 35$ structures with about $2^{21.2}$ chosen ciphertexts reused from previous structures. The work requirements are about $\left(\sum_{i=0}^{34}(\mathrm{e}^{-1/2})^i\right) \cdot 2^{25+16} \approx 2^{42.4}$ evaluations of FO which is approximately 2^{40} encryptions, much less than for the first part.

In total about 2^{38} chosen ciphertexts and work of about 2^{62} encryptions is required to find the first round's 75 bit subkey; about 2^{37} pairs are analysed.

Attack using collisions. This attack on 5-round MISTY2 with FL functions but without the output transformation works with collision-searching; it is based on the following observation in the chosen ciphertext model.

Proposition 2. *Given four rounds of MISTY2 starting at round n such that $\tilde{Y}_{n+3} = Y_{n+3}$ holds, i.e. Y_{n+3} is not transformed via* FL *before the XOR. Assume that no output transformation with* FL *takes place. Given a set of ciphertexts $C_i = (e_i, f_i, x \oplus e_i, y \oplus f_i)$ where x, y are constant and $\{(e_i, f_i)\}$ form a permutation. After decryption the right half R_n is a permutation.*

Proof. Z_{n+3} is always the constant (x, y) and thus X_{n+3} as well as L_{n+3} is a constant, say (x', y'). On the other hand, R_{n+3} is the permutation $\{(e_i, f_i)\}$. After being XORed with (x', y') this becomes Z_{n+2}, so that also X_{n+2} and L_{n+2} are permutations while R_{n+2} is a constant. Z_{n+1} is a permutation which is the XOR of a constant and a permutation $\tilde{Y}_{n+1}$ which is L_{n+2} possibly transformed by an instance of FL. So X_{n+1} is a permutation. Now the claim follows. □

The attack using Proposition 2 works for example on the five rounds of MISTY2 from round 2 to round 6. Both round 2 and round 6 do not apply any FL functions. An attack using 2^{89} work and 2^{20} chosen ciphertexts works straightforward as in section 4.2 with the same analysis, so the detailed description is omitted here.

In order to use the observation on reducing the amount key material to be guessed the attack uses 2^{28} chosen ciphertexts of the form $C_i = (e_i, f_i, x \oplus e_i, y \oplus f_i)$ where x, y are constants and $\{(e_i, f_i)\}$ form a permutation. Encryption under the unknown key yields plaintexts $P_i = (a_i, b_i, c_i, d_i)$ which we partition into 2^{16} sets B_t such that $P_i \in B_{b_i}$; thus all $P_i \in B_t$ for a given t have the same value $b_i = t$. First, set $\mathrm{AKO}_{i1} = 0$, $\mathrm{AKI}_{12} = 0$. For each 50 bit key guess $k = (\mathrm{AKO}_{11}, \mathrm{AKI}_{11}, k_{23}, \mathrm{AKI}_{13})$ with k_{23} in the role of AKO_{13}, and for each B_t, $t \in \{0, \ldots, 2^{16} - 1\}$ encrypt all $P_i \in B_t$ one round yielding $w_i^t = \mathrm{FO}_k((a_i, b_i)) \oplus (c_i, d_i)$. If we find $w_i^t = w_j^t$, $i \neq j$ then this key must be discarded, and the procedure is started with the next key guess. This takes at most $2^{50} \cdot 2^{28} = 2^{78}$ evaluations of FO comparable to 2^{76} encryptions to complete.

Once a correct k with $k_{23} = \mathrm{AKO}_{12} \oplus \mathrm{AKO}_{13}$ has been found, we have to find the correct 25 bits $(\mathrm{AKO}_{12}, \mathrm{AKI}_{12})$ and set $\mathrm{AKO}_{13} = k_{23} \oplus \mathrm{AKO}_{12}$. Here we use plaintexts P_i where both a_i and b_i vary; about 2^{20} plaintexts from the collection of 2^{28} plaintexts should be sufficient. This requires work of at most $2^{20} \cdot 2^{25} = 2^{45}$ evaluations of FO equivalent to 2^{43} encryptions. The time and

chosen ciphertext requirements are dominated by the first part (2^{76} work, 2^{28} chosen ciphertexts).

The probability that a wrong key guess survives is bounded with the same arguments as in Section 4.2 by Lemma 2 and the birthday paradox, so the details are omitted here.

6 Comparison to KASUMI

The algorithm KASUMI [4] is a MISTY variant that is to be used in next-generation cellular phones. The global structure is a Feistel network with 8 rounds including the final permutation. Its round function consists of FO and FL, applied before resp. after FO in odd resp. even-numbered rounds. The FO function has the same structure as in MISTY with the subkeys KO_{ij}, $1 \le j \le 3$ being applied by XOR before FI but a lacking final XOR of KO_{i4} after all non-linearities; the FI function involves an additional fourth round, and the FL function uses left rotations by one bit before each XOR. The S-boxes $S7$ and $S9$ are bijective, but different from those of MISTY. Each round uses 128 key bits, 32 bits for FL and 96 bits for FO. These are derived by revolving through the key bytes and applying rotations and bitwise additions of constants.

The usage of the basic Feistel structure without FL functions in the data path makes KASUMI susceptible to an attack based on the same 5-round impossible differential as used in Section 4.1, but with the additional difficulty that FL is part of the round functions and FO uses more keying material. The differential can be used as both FO and FL are bijective. It should be noted that a property similar to Property 1 does also hold for KASUMI's FO when it is preceeded by FL as it happens in odd-numbered rounds:

Property 3. Assume that the concatenation of FL and FO has a nonzero output XOR (δ, δ). Denote the input XOR to FL by (α_l, α_r) and its output XOR (the input to FO) by (β_l, β_r). The difference β_r is solely determined by the first round of FL, so is the right half of the data in the first round of FO. In order to have the given output XOR of FO the third round's output and input XOR must both be zero which means that $(\mathrm{KO}_{i3}, \mathrm{KI}_{i3})$ can be ignored. The output XOR (δ, δ) is determined by the second round of FO from the inputs with XOR β_r; additionally, β_r is canceled by the output XOR β_r of the FI in the first round of FO, coming from the left halfs of the inputs with XOR β_l.

The attack on rounds 2 to 7 of KASUMI including the last swap works as follows. In round 7 the function FL is applied before FO, so we can rely on Property 3. The attack uses the same structures as were used in Section 4.1 and looks for pairs with ciphertext XOR $(\delta, \delta, \alpha_l, \alpha_r)$ with the same methods. We expect about such 2^{15} pairs per structure which will be analysed. Let (c_i, d_i, e_i, f_i) and (c_j, d_j, e_j, f_j) be such a pair. In order to use Property K we first fix a guess of the first round subkey KL_{71} of FL in round 7, yielding f_i', f_j' with $\beta_r := f_i' \oplus f_j'$. Then we determine which guesses of $(\mathrm{KL}_{72}, \mathrm{KO}_{71}, \mathrm{KI}_{71})$ yield the XOR β_r after

the first FI. We expect about $2^{48}/2^{16} = 2^{32}$ guesses to fulfill this condition. Then, independently, we check which guess for $(\mathrm{KO}_{72}, \mathrm{KI}_{72})$ yields output XOR δ after the second FI from inputs f_i' and f_j'; here we expect about $2^{32}/2^{16} = 2^{16}$ guesses. Combinations of all these guesses are wrong subkeys and can be discarded. Their expected number is 2^{48} for each guess of KL_{71}, so each analysed pair is expected to discard about 2^{64} subkeys á 96 bits.

After about 2^{17} structures an expected number of $2^{96}/\mathrm{e}$ distinct subkeys are discarded. In total we need about $2^{17}\ln(2^{96}) \approx 67 \cdot 2^{17} \approx 2^{23}$ structures with 2^{55} chosen plaintexts and about 2^{38} analysed pairs to single out the right subkey.

The work requirements for each pair and each guess of KL_{71} are $2 \cdot 2^{48} + 2 \cdot 2^{32} \approx 2^{49}$ computations of the second round of FL and FI. In total this is about 2^{103} computations of FL and FI roughly equivalent to 2^{100} encryptions. Although this is much faster than brute force it is hardly a practical attack because of the high data and work requirements.

7 Conclusion

For MISTY1 the use of keyed linear functions inhibits the attack using the 5-round impossible differential of Feistel networks with bijective round functions; for MISTY2 we cannot make this claim as we did not find an impossible differential longer than 4 rounds.

The attacks on MISTY2 suggest that this structure might be one round weaker than the Feistel structure, at least when the linear functions FL are present. The directional asymmetry of the MISTY2 structure used in FO with embedded 3-round FI suggests that this structure might be stronger in the backwards direction compared to the forward direction.

By adding a fourth round to FI – like done for KASUMI – its equivalent description of FO would not reduce the number of key bits, so the attacks would only need to guess 7 bits more for each FI. If FO had one more round the properties used to improve both the differential and collision-searching attacks would not hold, leaving only the basic forms of attack; but this would require more keying material.

Instead, the changes for KASUMI, i.e. adding a round to FI and employing the linear functions as part of the round function does not require more keying material and seems to make an analysis of the round function very demanding.

Acknowledgments

Thanks are due to Mitsuru Matsui for providing reference [10] and to the anonymous referees for helpful comments and the suggestion to apply the techniques to KASUMI. The author is grateful to Dr. Uwe Deppisch, Alfred Goll and the colleagues of the IT research department of Dresdner Bank for the encouraging work conditions that were very helpful in conducting this research.

References

[1] E. Biham. Cryptanalysis of Ladder-DES. In E. Biham, editor, *Fast Software Encryption: 4th International Workshop*, Volume 1267 of *Lecture Notes in Computer Science*, pages 134–138, Haifa, Israel, 20–22 Jan. 1997. Springer-Verlag.

[2] E. Biham, A. Biryukov, and A. Shamir. Miss in the middle attacks on IDEA and Khufu. In L. Knudsen, editor, *Fast Software Encryption, 6th international Workshop*, Volume 1636 of *Lecture Notes in Computer Science*, pages 124–138, Rome, Italy, 1999. Springer-Verlag.

[3] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer Verlag, Berlin, 1993.

[4] ETSI/SAGE. Specification of the 3GPP Confidentiality and Integrity Algorithms – Document 2: KASUMI Specification, Version 1.0. 3G TS 35.202, December 23, 1999. `http://www.etsi.org/dvbandca/3GPP/3GPPconditions.html`.

[5] L. R. Knudsen. DEAL — A 128-bit block cipher. Technical Report 151, Department of Informatics, University of Bergen, Bergen, Norway, Feb. 1998.

[6] A. W. Marshal and I. Olkin. *Inequalities: Theory of Majorization and Its Applications*, volume 143 of *Mathematics in Science and Engineering*. Academic Press, New York, 1979.

[7] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology - EuroCrypt '93*, Volume 765 of *Lecture Notes in Computer Science*, pages 386–397, Berlin, 1993. Springer-Verlag.

[8] M. Matsui. New block encryption algorithm MISTY. In E. Biham, editor, *Fast Software Encryption: 4th International Workshop*, Volume 1267 of *Lecture Notes in Computer Science*, pages 54–68, Haifa, Israel, 20–22 Jan. 1997. Springer-Verlag.

[9] K. Sakurai and Y. Zheng. On non-pseudorandomness from block ciphers with provable immunity against linear cryptanalysis. *IEICE Trans. Fundamentals*, E80-A(1):19–24, January 1997.

[10] M. Sugita. Higher order differential attack of block ciphers MISTY1,2. Technical Report ISEC98-4, Institute of Electronics, Information and Communication Engineers (IEICE), 1998.

[11] M. Sugita. Personal communication, January 2001.

[12] H. Tanaka, K. Hisamatsu, and T. Kaneko. Strength of MISTY1 without FL function for higher order differential attack. In M. Fossorier, H. Imai, S. Lin, and A. Poli, editors, *Proc. Applied algebra, algebraic algorithms, and error-correcting codes: 13th international symposium, AAECC-13*, Volume 1719 of *Lecture Notes in Computer Science*, pages 221–230, Hawaii, USA, 1999. Springer Verlag.