Chapter 4

MISTY1

MISTY1 was designed by Mitsubishi Electronics in 1995. Since then it was updated into the KASUMI cipher in order to become an ETSI standard.[1] MISTY1 was also submitted to the NESSIE European development process.[2] The design was made in order to ensure protection against differential and linear cryptanalysis according to Matsui's design paradigm.

4.1 Design Properties

4.1.1 S7 and S9: Algebraic Properties

S7 and S9 are substitution boxes which are based on power functions in $\mathrm{GF}(2^9)$ and $\mathrm{GF}(2^7)$ which are known to be almost bent. This means that $\mathrm{LP}^{\mathrm{S7}} = \mathrm{DP}^{\mathrm{S7}} = 2^{-6}$ and $\mathrm{LP}^{\mathrm{S9}} = \mathrm{DP}^{\mathrm{S9}} = 2^{-8}$ where LP and DP denotes the maximum probability for a linear and differential characteristic.

From the choice of power functions, all output bits of S7 can be expressed as a boolean function of algebraic degree three. Similarly, S9 has an algebraic degree of two. As a consequence we obtain that

$$\begin{aligned}&\mathrm{S7}(a) \oplus \mathrm{S7}(a \oplus b) \oplus \mathrm{S7}(a \oplus c) \oplus \mathrm{S7}(a \oplus b \oplus c) \oplus \\ &\mathrm{S7}(a \oplus d) \oplus \mathrm{S7}(a \oplus b \oplus d) \oplus \mathrm{S7}(a \oplus c \oplus d) \oplus \mathrm{S7}(a \oplus b \oplus c \oplus d)\end{aligned}$$

is a constant which does not depend on a. Similarly,

$$\mathrm{S9}(a) \oplus \mathrm{S9}(a \oplus b) \oplus \mathrm{S9}(a \oplus c) \oplus \mathrm{S9}(a \oplus b \oplus c)$$

is a constant which does not depend on a. As a consequence the output bits of FI do not have the same algebraic degree: the 7 leftmost bits have degree

[1] See `http://www.etsi.org/`.

[2] See `http://www.cryptonessie.org/`.

3, the remaining have degree 4. This also propagates to FO: the 7 leftmost output bits of FO have degree 3, the 9 following bits have degree 4, the 7 next ones have degree 12, and the 9 remaining have degree 16.

4.1.2 S7 and S9: Linear Properties

Since $S7(x)$ can be written $A(x^\alpha)$ in $\mathrm{GF}(2^7)$, S7 has another surprising property. Namely, there exist two affine transformation f and g such that $S7 \circ f = g \circ S7$.

We let

$$f(x) = x^2$$

which is an affine transformation. We have

$$\begin{aligned} S7 \circ f(x) &= A(x^{2\alpha}) \\ &= \mathrm{matrixL}(S7(x) + S7(0)) + S7(0) \end{aligned}$$

with

$$\mathrm{matrixL} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

so

$$g(x) = \mathrm{matrixL}(x + S7(0)) + S7(0).$$

S9 was supposed to be similar to S7. We have not found any similar property for S7 though. This seems to mean that S9 was built according to a scheme which is not the documented one.

4.1.3 FI and FO

The design of FI and FO induce the following unexpected property

$$\mathrm{FO}_l(a, b) \oplus \mathrm{FO}_l(a, c) = \mathrm{FO}_l(d, b) \oplus \mathrm{FO}_l(d, c)$$

for any 16-bit a, b, c, d where FO_l denotes the left half of the FO output. The same property holds for FI when a and d are 9-bit long, and b and c are 7-bit long.

4.1.4 FL

We can think that MISTY1 is not exactly a Feistel scheme because of the FL linear permutation. We can however represent MISTY1 with this linear permutation at the input and output of the FO functions.

4.1.5 The Key Schedule

The key schedule is quite symmetric. It simply consists in splitting the key into eight 16-bit strings and computing other 16-bit strings by the same FI operation. The obtained 16 16-bit strings are directly used as subkeys.

4.2 Differential and Linear Cryptanalysis

4.2.1 The Russian Doll Design

The MISTY1 design is made on a clever way to use the Nyberg-Knudsen theorem which enables the amplification of upper bounds on LP and DP values. S7 and S9 are made in order to have all LP and DP values less than 2^{-6} and 2^{-8} respectively. From the construction, we obtain that all LP and DP values for FI are less than 2^{-14}. FI is then plugged into a similar structure in FO which ensures that all LP and DP values are less than 2^{-28}. Finally, this guarantees that all LP and DP values for three rounds of MISTY1 are less than 2^{-56}.

4.2.2 The Bounds are Tight

With $\Delta = \texttt{0x40}$ we notice that the DP coefficient of the $\Delta \to \Delta$ differential characteristic is 2^{-14} for FI (for any key). From this we obtain that the DP coefficient of the three following characteristics for FO are 2^{-28}

$$\begin{aligned} \Delta\Delta &\to \Delta\Delta \\ \Delta 0 &\to \Delta 0 \\ 0\Delta &\to 0\Delta \end{aligned}$$

Thus the DP coefficient of the three following characteristics for a three-round Feistel scheme with FO are 2^{-56}

$$\begin{aligned} \Delta'\Delta' &\to \Delta'\Delta' \\ \Delta' 0 &\to \Delta' 0 \\ 0\Delta' &\to 0\Delta' \end{aligned}$$

with Δ' equal to $\Delta\Delta$, $\Delta 0$ or 0Δ, assuming that no FL function interfere with the Δ'. (This assumption is quite reasonable since the characteristics have low Hamming weight.)

A similar analysis holds for linear characteristics with $\Delta = 1$.

This means that we can potentially break MISTY1 reduced to four rounds by using regular differential or linear cryptanalysis with about 2^{56} known or chosen plaintexts.

4.3 Other Attacks

4.3.1 Algebraic Degree

We can use the algebraic properties of FO: namely the algebraic degree of three of the seven leftmost output bits. If we pick sixteen chosen plaintexts of the form (a, b_i) where $b_1, \ldots, b_{16}$ are such that the set of all b_i is an affine space of dimension four, we know that the sum of the seven leftmost bits of the input of FO3 is zero when the corresponding bits of KL3 are all set to one. This is already a distinguisher against three rounds.

This also gives a simple test in order to recognize FL6, KI4 and KO4 for an attack against four rounds.

4.3.2 Higher Order Attack

Similarly, the properties of FO leads to a more efficient distinguisher against three rounds since only four chosen plaintexts are required instead of sixteen. This can also be transformed into a key recovery attack against four rounds.

4.3.3 Side Channel Cryptanalysis

Like for other block ciphers, assuming that we can trace the Hamming weight of CPU registers throughout the computation process, we can easily break MISTY1 by power analysis. The design of MISTY1 does not seem to offer much more potential weaknesses to side channel cryptanalysis, but with the table lookups. As for other block ciphers with table lookups, assuming that we can speed up the clock signal in order to make the tables invisible or that we can tamper the tables in memory, fault analysis may be able to break the cipher. We thus recommend that implementations care about power analysis and on the memory tempering attacks.

4.3.4 Weak Keys

From the key schedule it appears that if the secret key is $K = uuuuuuuu$ where u is any 16-bit string, then all FO functions use the same subkeys, and all FL functions use subkeys which are alternately swapped: FL1, FL3, FL5, FL7 use the same keys, and FL2, FL4, FL6, FL8 use the same keys which are obtained from the other FL functions by exchanging the two subkeys. Although it is not quite clear how to use these properties, these keys may look like weak keys.

4.3.5 Related Keys

Let $K = K_1K_2K_3K_4K_5K_6K_7K_8$ be any secret key. If we define $K^* = K_2K_3K_4K_5K_6K_7K_8K_1$, then all FO functions will be shifted by one position and FL functions will be permuted. These may be used as related keys in special attack models.

4.3.6 Decorrelation

The FO function cannot be assumed to be pseudorandom since we have

$$\mathrm{FO}_l(a,b) \oplus \mathrm{FO}_l(a,c) = \mathrm{FO}_l(d,b) \oplus \mathrm{FO}_l(d,c)$$

for any a, b, c, d. At least, FO is not decorrelated to the order four. It is however likely to provide decorrelation to the order two by showing that FI is so (unless the unexpected property of S7 spoils decorrelation). This result may be quite similar to the one of the Peanut construction. This would thus give a other (and more complete and general) security proof for the resistance against differential and linear cryptanalysis.

4.4 Available Literature

The seminal theoretical work regarding the design of MISTY has been published in [10] and the whole cipher design in [11]. Pseudorandomness of MISTY has been investigated in [17]. Furthermore, KASUMI has been proposed and accepted as a standard by ETSI (`http://www.etsi.org`) and proposed to NESSIE (`http://www.cryptonessie.org`).

The differences between MISTY1 and KASUMI are:

- the place of the FL permutations in the Feistel scheme,
- some rotations were added in FL for KASUMI,

- the choice of the substitution boxes S7 and S9,
- the number of rounds in FI (there is one more round in KASUMI).

4.5 Conclusion

MISTY1 is innovative in the sense that it is the first real-life algorithm which was built in order to be provably secure against differential and linear cryptanalysis. The construction paradigm is however very restrictive and needs to use highly nonlinear substitution boxes. Efficient ones usually have strange properties like low algebraic order. For this reason, many unexpected internal properties were found in MISTY1: a low algebraic order in S7 and S9 which has consequences in FI and FO, a linear transformation which can go through S7, and a weakness of the left output of the FI and FO design. This last property enabled the attack against three rounds with only four chosen plaintexts. Finally, we notice the key schedule is quite minimal and we have weak keys.

Since we did not find the same property for S9 and S7, we suspect that S9 was not built according to the documented paradigm. We thus recommend to explain this.

The MISTY1 paradigms leads to differential and linear characteristic probabilities upper bounds which are tight.

Resistance against side channel attacks is standard.

High order decorrelation is impossible because of the FI and FO design. We however suspect that we can prove the decorrelation of order two which would produce another proof of security against differential and linear cryptanalysis which is more general.

Here are our conclusion about MISTY1.

1. **Discovery of unexpected internal properties: "−−".** We have found too many internal properties.
2. **Randomness provided by the key schedule: "−".** The key schedule is quite minimal and provide weak keys.
3. **Resistance against differential and linear cryptanalysis: "++".** The design paradigm provides provable security against these attacks.
4. **Resistance against side channel attacks: "+".** Resistance is quite standard: we only have bitwise operations and tables.

5. **Maturity of the algorithm: "++".** This algorithm may consider as a senior one which has already been adopted as a standard. The quality of literature on this algorithm outline important maturity.

6. **Overall security confidence: "+".** This looks quite strong.

7. **Beauty of the design: "++".** We appreciate the design which provides provable security.