付録Ｂ．ＭＩＳＴＹ１の詳細評価について

1　はじめに

これは，電子政府事業に用いる暗号方式に関する応募資料（暗号技術仕様書 MISTY1 及び自己評価書 MISTY1[Mitsubishi][M96]）に基づき，詳細評価するために作成したものである。アルゴリズムに関する詳細は省略したので、仕様書を参照して頂きたい。

2　ＭＩＳＴＹ１のアルゴリズム

ＭＩＳＴＹの仕様は下記のとおりである。

- ブロック長:64 ビット
- 鍵長:128 ビット
- 段数:n(ただし，n は，4 の倍数。$n = 8$ を推奨。)

以下にデータランダム化部の概要を示す。

MISTY1 は FO 関数と呼ばれる段関数を使った、Feistel 構造を持ち、２段毎に補助関数 FL が挿入される。全体構造を図 2 に示す。

関数 FO は，32 ビット入出力の関数であり、その内部では、ＭＩＳＴＹ構造と呼ばれる３段の FI 関数処理が行われる。（図 2 参照）i 段目 FO 関数には、16 ビットの拡大鍵 $KO_iij(1 \leq j \leq 4)$4 つと 16 ビットの拡大鍵 $KI_{ij}(1 \leq j \leq 3)$ ３つの合計１１２ビットが供給される。１つ目の添え字 i は i 段目 FO 関数を表し、２つ目の添え字 j は、FO 関数内の FI 関数の順番を表す。

関数 FI は，１６ビット入出力の関数であり、入力された 16 ビットを，左 9 ビット及び右 7 ビットに分割して，排他的論理和 $\oplus$ 及び置換表 S_7, S_9 による変換処理を行う。それは、FO 関数に相似な構造である。各 FI_{ij} には 16 ビットの拡大鍵 KI_{ij} が供給され、左 7 ビットを KI_{ij1} とし，右 9 ビットを KI_{ij2} として使用される。このとき，置換表 S_7, S_9 は、それぞれ 7 ビット、９ビット入出力の全単射関数である。

3　S-BOX S(X) に関する評価

3.1　ブール多項式次数及び項数

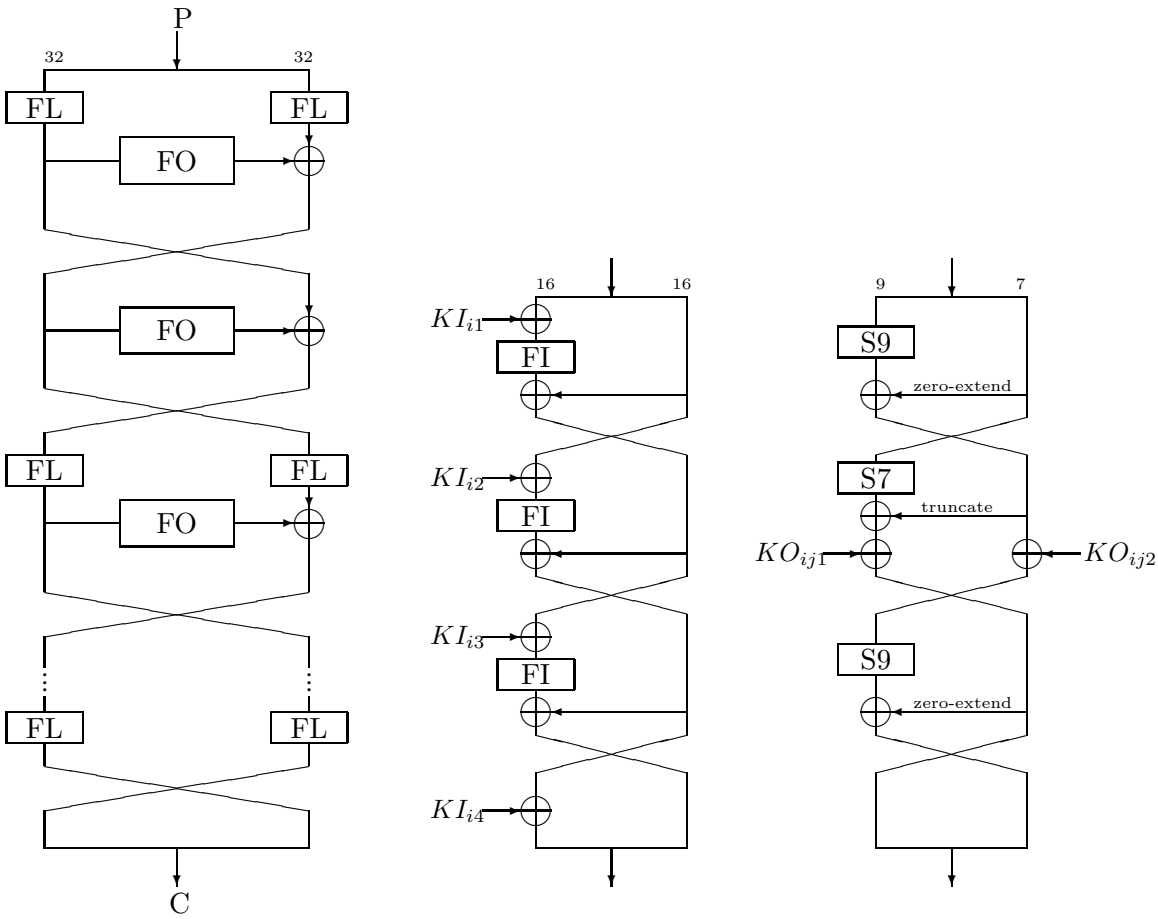
MISTY1 の関数 FI には、2 種類のＳボックス、S_7 及び S_9 がある。入出力を $(y_0, y_1, ..., y_6) = S_7(x_0, x_1, ..., x6)$,$(y_0, y_1, ..., y_8) = S_7(x_0, x_1, ..., x8)$ としてブール展開式は、表 1 及び表 2 のとおりである。S_7 は、7bits 入出力の 3 次の全単射関数であり、S_9 は、9bits 入出力の 2 次の全単射関数である。

表 1: S_7 のブール展開式

出力ビット	入力ビット	次数	項数
y_0	$x_0x_1x_6 \oplus x_0x_2x_5 \oplus x_0x_3x_4 \oplus x_0x_5x_6 \oplus x_3x_5x_6 \oplus x_1x_3 \oplus x_1x_5 \oplus x_2x_6 \oplus x_4x_5 \oplus x_0 \oplus 1$	3	11
y_1	$x_0x_5x_6 \oplus x_1x_4x_6 \oplus x_2x_3x_6 \oplus x_2x_4x_5 \oplus x_0x_2 \oplus x_0x_4 \oplus x_0x_6 \oplus x_1x_5 \oplus x_3x_4 \oplus x_3x_6 \oplus x_6 \oplus 1$	3	12
y_2	$x_0x_1x_4 \oplus x_0x_2x_3 \oplus x_0x_3x_6 \oplus x_0x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_4x_5 \oplus x_0x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_1x_6 \oplus x_3x_6 \oplus x_4x_6 \oplus x_4$	3	13
y_3	$x_0x_1x_2 \oplus x_0x_4x_6 \oplus x_1x_3x_6 \oplus x_1x_4x_5 \oplus x_0x_3 \oplus x_2x_4 \oplus x_2x_6 \oplus x_5x_6 \oplus x_0 \oplus x_1 \oplus 1$	3	11
y_4	$x_0x_3x_5 \oplus x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_1x_5x_6 \oplus x_4x_5x_6 \oplus x_0x_4 \oplus x_1x_6 \oplus x_2x_3 \oplus x_2x_5 \oplus x_5 \oplus 1$	3	11
y_5	$x_0x_1x_2 \oplus x_0x_1x_5 \oplus x_0x_2x_4 \oplus x_1x_2x_3 \oplus x_2x_5x_6 \oplus x_0x_3 \oplus x_0x_5 \oplus x_0x_6 \oplus x_1x_4 \oplus x_3x_5 \oplus x_0 \oplus x_1 \oplus x_2$	3	13
y_6	$x_0x_3x_6 \oplus x_1x_2x_6 \oplus x_1x_3x_5 \oplus x_2x_3x_4 \oplus x_2x_5x_6 \oplus x_0x_1 \oplus x_0x_3 \oplus x_0x_5 \oplus x_1x_6 \oplus x_2x_5 \oplus x_3x_5 \oplus x_4x_6 \oplus x_3$	3	13

表 2: S_9 のブール展開式

出力ビット	入力ビット	次数	項数
y_0	$x_0x_4 \oplus x_0x_5 \oplus x_1x_5 \oplus x_1x_6 \oplus x_2x_6 \oplus x_2x_7 \oplus x_3x_7 \oplus x_3x_8 \oplus x_4x_8 \oplus 1$	2	10
y_1	$x_0x_2 \oplus x_0x_6 \oplus x_0x_8 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_8 \oplus x_4x_5 \oplus x_5x_8 \oplus x_3 \oplus x_7 \oplus 1$	2	13
y_2	$x_0x_1 \oplus x_0x_4 \oplus x_0x_6 \oplus x_1x_3 \oplus x_1x_7 \oplus x_2x_4 \oplus x_3x_4 \oplus x_3x_7 \oplus x_4x_5 \oplus x_5x_6 \oplus x_4 \oplus x_8$	2	12
y_3	$x_1x_2 \oplus x_1x_5 \oplus x_1x_7 \oplus x_2x_4 \oplus x_2x_8 \oplus x_3x_5 \oplus x_4x_5 \oplus x_4x_8 \oplus x_5x_6 \oplus x_6x_7 \oplus x_0 \oplus x_5$	2	12
y_4	$x_0x_3 \oplus x_0x_5 \oplus x_2x_3 \oplus x_2x_6 \oplus x_2x_8 \oplus x_3x_5 \oplus x_4x_6 \oplus x_5x_6 \oplus x_6x_7 \oplus x_7x_8 \oplus x_1 \oplus x_6$	2	12
y_5	$x_0x_3 \oplus x_0x_8 \oplus x_1x_4 \oplus x_1x_6 \oplus x_3x_4 \oplus x_3x_7 \oplus x_4x_6 \oplus x_5x_7 \oplus x_6x_7 \oplus x_7x_8 \oplus x_2 \oplus x_7$	2	12
y_6	$x_0x_1 \oplus x_0x_8 \oplus x_1x_4 \oplus x_2x_5 \oplus x_2x_7 \oplus x_4x_5 \oplus x_4x_8 \oplus x_5x_7 \oplus x_6x_8 \oplus x_7x_8 \oplus x_3 \oplus x_8 \oplus 1$	2	13
y_7	$x_0x_1 \oplus x_0x_4 \oplus x_0x_7 \oplus x_1x_2 \oplus x_1x_6 \oplus x_1x_8 \oplus x_2x_3 \oplus x_3x_6 \oplus x_4x_7 \oplus x_6x_7 \oplus x_1 \oplus x_5 \oplus 1$	2	13
y_8	$x_0x_1 \oplus x_0x_5 \oplus x_0x_7 \oplus x_0x_8 \oplus x_1x_2 \oplus x_2x_5 \oplus x_3x_6 \oplus x_3x_8 \oplus x_5x_6 \oplus x_6x_8 \oplus x_0 \oplus x_4 \oplus 1$	2	13



(i) MISTY1　　(ii) FO 関数　　(iii) FI 関数

図 1: ブロック暗号 MISTY

4　F 関数 $FO(X)$ の評価

4.1　FL 関数のブール多項式次数

データランダムか部は、FO 関数と FL 関数で構成される。FL 関数は、３２ビット入を拡大鍵３２ビットに基づき撹拌し、３２ビットを出力する関数で、入力に関し線形であり、そのブール多項式次数は１次である。

4.2　FO 関数のブール多項式次数（形式的代数次数評価）

S_7 及び S_9 の代数次数がそれぞれ３次及び２次であることを利用して、F O 関数の代数次数を形式的に解析した。次数の追跡においては、単純な代数次数だけでなく、係わりを持つ入力ビット数による制限（次数≦入力ビット数）を考慮した。結果を図 2 に示す。記号 $< i >$ はその変数ブロックの次数が i 次であり、$< i|j >$ は、変数の左ブロックが i 次、右ブロックが j 次 である事を表す。図には、この FO 関数の出力が、次段に行く際に FL 関数を通る事を想定した FL 関数通過後の形式的代数次数も示してある。FO 関数は、出力ビットの位置により、次数が３次から

表 3: F 関数のブール展開式項数

次数	最大項数	最小項数	平均項数	期待値
1	23	1	14.3	16
2	261	26	140.1	248
3	2189	8	902.5	2480
4	11423	0	4017.9	17980
5	39051	0	12939.9	100688
6	83402	0	26948.0	453096

期待値:次数 d で取りうる項の種類 ${}_{32}C_d$ の 1/2

１２次までの範囲となる。

4.3 FO 関数のブール多項式項数

F 関数 (拡大鍵は全て０とする）の出力ビットについて、代数次数６次までの項を調査した。結果は，表 3 のとおりである。３２変数の積がランダムに各出力ビットの展開式に登場すると考えたときの期待値に比べ、２次式以上の項数が少ない。また４次以上で最小項数が０の出力ビットがあるが、これは 4.2 節の形式的代数次数評価の３次の出力ビットブロックに対応する。F関数の項数に偏りが見られることは、攻撃方程式を拡大鍵の総当たりでは無く線形化等の解析的技法を使い計算量を削減できる可能性がある。実際、文献 [THK98] の攻撃に見られるように、F関数１段に関しては、線形化する事によって、攻撃計算量の大幅な削減ができる場合がある。

4.4 高階差分攻撃及び補間攻撃の評価

4.4.1 代数次数評価（形式的次数評価）

MISTY-1 の暗号化関数のコア部分は、FO 関数による Feistel 構造である。FL 関数を除いて FO 関数のみで構成した場合の評価と、完全な MISTY-1 の評価を行う。

FL 関数無しの場合、以下となる。FO 関数の次数は、4.2 節のように、３次から１６次である。単に FO 関数の代数次数評価を用いるならば、平文の左半分を固定にし、右半分を変数と取るのが最も次数の上昇は、最も遅い。この場合、２段通過後３次、３段通過後 16*3=48 次（FO 関数のデータの流れを辿ると、3*3=9 次が最低次数となることはない）となる。従って、形式的次数評価では、攻撃方程式を立てる位置は、２段 FO 関数通過後、即ち３段目出力左半分である。１段消去型攻撃を想定するならば、３階差分で４段が攻撃可能である。

FL 関数付きの場合、前述の平文選択に対し、２段 FO 関数通過後１２次となる。従って、１段消去型攻撃で４段が１２階差分で攻撃可能である。

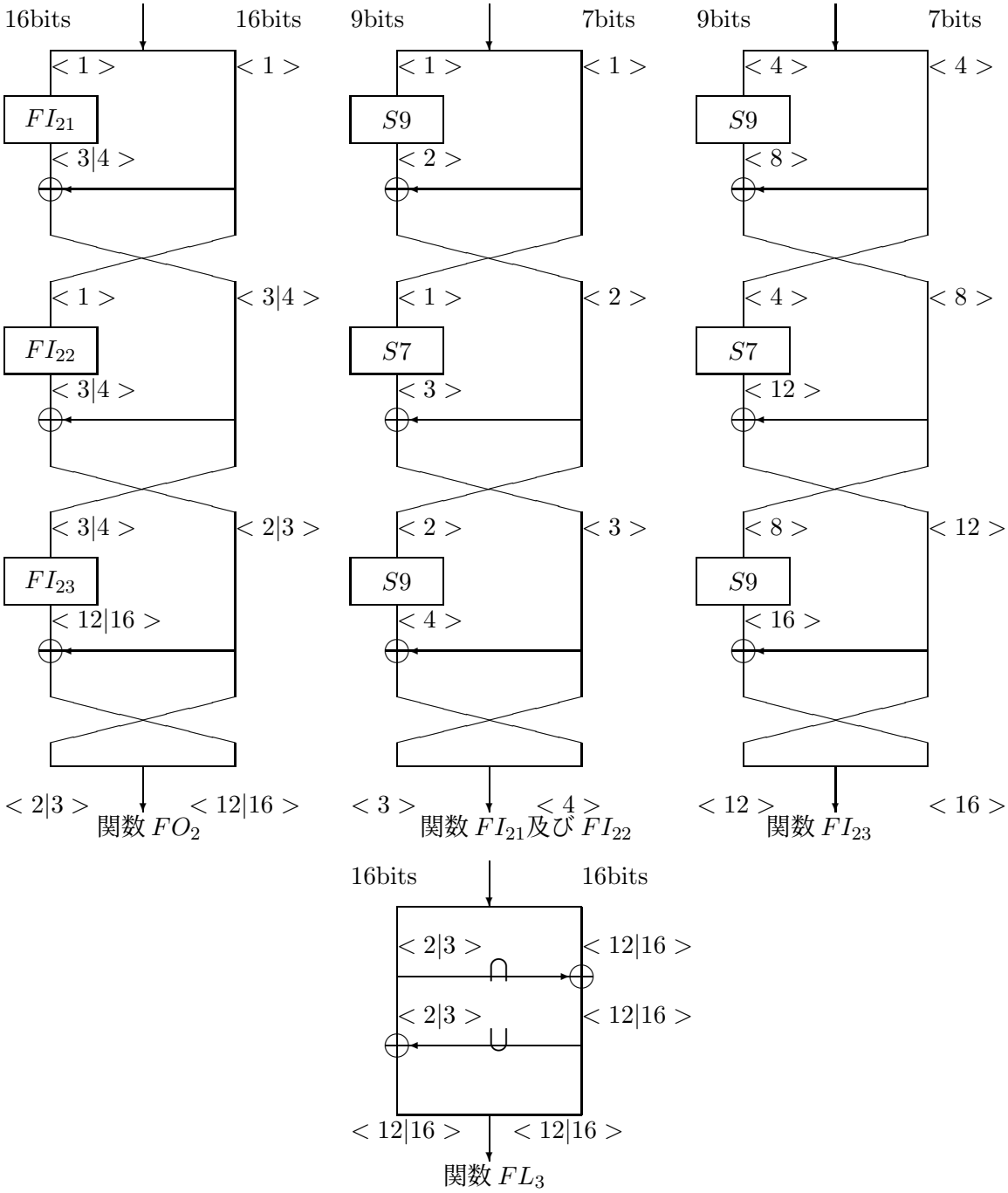


図 2: MISTY1 の構成要素及び代数次数

4.4.2 選択型高階差分による評価

前節では、平文右半分のみを変数に取るという条件のみで解析した。ここでは、FL 関数の無い MISTY1 に対し、もう少し細かな探索を行う。入力平文を左右 2 つの 32bits ブロックに分割し、それぞれ P_L, P_R とする。第 1 段目の入力である P_L を固定値とし、$P_R = (X_5, X_4, X_3, X_2, X_1, X_0)$ として、高階差分値を探索した。このとき、$X_i \in GF(2)^7 (i = 0, 2, 3, 5), X_i \in GF(2)^2 (j = 1, 4)$ である。最初に S_7 に入る小ブロック X_i に付いては 7 階差分まで、S_9 に入るものについては隣りの小ブロックと合わせて 9 階差分までの範囲で攻撃可能となる変数小ブロックを探索した。結果として、最良なものは、X_0 以外を固定値とした 7 階差分であり、4 段目出力変数の 7 ビットに関し、7 階差分値が定数 $0X6D$ となる。これは、文献 [THK98],[THK98] で報告されている 7 階差分の選び方であり、自己評価書 [Mitsubishi] でも引用されている。この場合、7 階差分を使って、１段消去型攻撃で５段が攻撃可能となる。

FL 関数のある完全な MISTY1 に対しては、8 階以下の高階差分攻撃を探索した結果として、２階差分で４段 MISTY が攻撃可能である事が報告されている [TIK01]。

4.5 32 階高階差分

ｎビット入出力の全単射Ｆ関数で構成される Feistel 型暗号の場合、平文の右半分（２段目Ｆ関数に入る方）を変数に取るならば、４段目出力の左半分がｎ階差分で０となる。MISTY1 の場合は、関数 FO は、32bits 入出力の全単射関数であるので、32 階差分の高階差分攻撃が可能である。この場合１段消去型攻撃を想定すれば、５段が攻撃可能となる。なお、FL 関数も３２ビット入出力の全単射関数であり、変数の右半分３２ビットと左半分３２ビットは、独立な FL 関数で処理されるので、上述の３２階差分攻撃は、FL 関数付きの場合も成立する。

３１階差分での可能性を探索する為に、３１階差分及び３２階差分について計算機実験をしたところ、31 階差分で、高階差分攻撃可能なものは見いだせなかったが、（当然の事ながら）３２階差分は０となり５段までのＭＩＳＴＹは、１段消去型高階差分攻撃可能であることが確認できた。

4.6 SQUARE 攻撃

MISTY1 の構成部品の S_7 及び S_9 ボックス並びに FI 関数、FO 関数及び FL 関数が全単射関数である。その構造から、FL 無し MISTY1 では、S_7、S_9、FI,FO を単位とする７、９、１６、３２階差分を SQUARE 型攻撃の考えで調査する必要がある。結果として、4.4.2 節で示した 7 階差分以上に効果的な差分は得られなかった。FL 関数付きの場合、調査すべきは FO を単位とする３２階差分であり、前節の３２階差分と同じ結果となった。

4.7 高階差分攻撃耐性の評価

以上の調査及び付録Ｋの線形和攻撃を総合して、現在までに知られている最も効果的な高階差分の選び方は、FL 関数なしの場合文献 [THK98] のものである。

文献 [THK98] では、６階差分を使って、７ビット幅の攻撃方程式を立て、平文側の中間変数２３ビットと５段目拡大鍵３２ビットの非線形方程式を線形化し１１８個の項数（未知数）で解いている。この場合必要なのは１７組の６階差分であり必要平文数は $2^6 * 17 = 1088$ であり、計算量は 2^{17} 回の FO 関数計算量である。

最近、Steve Babbage らは [SL00]、この攻撃に対し解析を行い、S_7 の代数特性にこの攻撃が起因する事を明らかにしている。さらに、線形／差分攻撃に対する最強性及び代数次数３の条件下で、S_7 を別のものに置き換える事を検討したが、それは、数学的に不可能であるとしている。

文献 [THK98] の等価変形を行えば、FO 関数１段当たり等価拡大鍵ビット数は７５ビットである。FL 関数無し６段 MISTY1 は、本文３．２節＜線形化＋総当たり攻撃＞の手法で、解読可能である。即ち、6 段目の等価拡大鍵 75 ビットを総当たりし、残りの５段を上述の方法で解く手法である。本文（３．１０）式を使い、必要平文数は $2^6 * 17 = 1088 \simeq 2^{11}$、計算量は $2 * 2^{6+75} * 17 * 118 \simeq 2^{93}$ の FO 関数計算量であり、秘密鍵 128 ビットの総当たりより少ない。なお、最初の２倍は、２段消去型攻撃を FO 関数計算量に換算する為の倍数である。

FL 関数付きの MISTY の場合、３２階差分を使って１段消去型攻撃を行うと鍵の総当たりの場合 FO 関数に等価変形しても７５＋１６ビット FL 関数に３２ビットの鍵があり、計算量は、$2^{32+75+16+32+1} > 2^{128}$ となる。[1] しかし、文献 [THK98] と同じ７ビット分にのみ着目して、32 階差分に対し、攻撃方程式を立てるならば、項数は多くても 118 個であり FL 関数の３２ビット鍵を総当たりしたとしても、計算量は多くても $2^{32+32} * 17 * 118 \simeq 2^{75}$ の FO 関数計算である。この場合必要な平文数は $2^{32} * 17 \simeq 2^{37}$ となる。ここでは、時間の制約で、より効果的な解読アルゴリズムを探索していないが、５段の FL 付き MISTY1 は十分この平文組と計算量で解けると考えられる。

5　結論

MISTY1 に対する詳細評価として, 形式的代数次数解析を含む高階差分解読法及び補間解読法を行った。FL 無し MISTY1 の場合、６段が 2^{11} の平文組及び 2^{93} の FO 関数計算でとけ、FL ありの場合、５段が 2^{37} の平文組及び 2^{75} の FO 関数計算でとけると推定される。しかし、暗号技術仕様書で指定されている 8 段以上の場合には, なお解読は困難であると考える。

また、他の解読法については, 自己評価書において、線形解読法、差分解読法、不能差分解読法、ブーメラン解読法、法 n 解読法、非全射解読法、Luby-Racoff 流ランダム性、鍵スケジュール部関連の解読法、統計量評価及び実装に関連する自己評価を行っており、その記述内容も信頼できる.

以上より、詳細評価の結果として,MISTY1 は十分な強度を有するものと考える.

参考文献

[Mitsubishi] 三菱電機, ”暗号技術応募書／暗号技術仕様書 MISTY ／自己評価書 MISTY1”, IPA 提出資料

[M96] 松井充, ”ブロック暗号アルゴリズム MISTY”, 信学技報 ISEC96-11(1966)

[THK98] 田中秀磨, 久松和之, 金子敏信, ”FL 関数の無い MISTY に対する高階差分攻撃”, ISEC98-5(1998-05)

[THK99] Hidema Tanaka, Kazuyuki Hisamatsu, Toshinobu Kaneko, ”Strength of MISTY1 without FL function for Higher Order Diffrential Attack”, SCI/ISA99

[1] 実際には、５段目には FL 関数は入っていないが、ここでは入っていると仮定して評価している。

[TIK01] 田中秀磨、石井周志、金子敏信, "霞とＭＩＳＴＹの強度評価に関する一考察", SCIS2001-12A,(2001-1)

[S98] Makoto Sugita, "Higher Order Diffrential Attack of Block Cipher MISTY1,2", technical report of IEICE, ISEC98-1

[K99] 青木和麻呂, "線形和攻撃 (Linear Sum Attack)", SCIS'99, Jan. 26-29, 1999

[SL00] Steve Babbage, Laurent Frisch, "On MISTY1 Higher Order Diffremtial Cryptanalysis", ICISC, Dec. 2000