3-4　秘密鍵暗号に対する高階差分攻撃の拡張方法

3-4 An Expansion Algorithm for Higher Order Differential Cryptanalysis of Secret Key Ciphers

田中秀磨　金子敏信
TANAKA Hidema and KANEKO Toshinobu

要旨

共通鍵ブロック暗号に対する選択平文攻撃の一つである高階差分攻撃の拡張方法について示す。通常の高階差分攻撃では最終段の拡大鍵を解くための攻撃方程式を導出する。我々の提案方法は最終段の拡大鍵を推定しながらもう一段上の拡大鍵を解くための攻撃方程式を導出する。この結果、通常の高階差分攻撃と比較すると攻撃可能段数が 1 段増える。64 ビットブロック暗号である変形 MISTY1 は 5 段までの攻撃が知られているが、我々の攻撃方法を適用すると 6 段まで攻撃可能であることが分かった。

We show an expansion method for a higher order differential cryptanalysis which is one of chosen plaintext attack against symmetric block ciphers. Ordinary algorithm of higher order differential cryptanalysis derives an attack equation for sub-keys in the last round. Our algorithm derives an attack equation for sub-keys in previous round using brute force estimating to the sub-keys in last round. As the result, comparing with original algorithm, our algorithm can attack one more round. Though a five round modified MISTY1 which is a 64 bit block cipher can be attacked is well known, when our algorithm is used, a six round modified MISTY1 can be broken.

[キーワード]
選択平文攻撃，ブロック暗号，高階差分攻撃，2 段消去攻撃
Chosen plaintext attack, Block cipher, Higher order differential cryptanalysis, Two round elimination attack

1　はじめに

情報セキュリティシステムは暗号技術がその要素として利用されている。そのため暗号技術の安全性はシステム全体の安全性に直結する問題であり、その安全性に関する正確な状態を知ることは重要である。暗号技術には、鍵の性質から公開鍵暗号と共通鍵暗号に分類される。公開鍵暗号が安全性を数学的な難問題に帰着させているのに対して、共通鍵暗号は利用する関数ごとに安全性を見積もりそれらを組み合わせて構成しているという特徴がある。また共通鍵暗号は、暗号ごとの特徴を利用した攻撃方法も提案され、それが他に応用されるなど攻撃方法の進化発展も目覚ましいという特徴がある。これらの結果、共通鍵暗号における攻撃の研究は、安全性の状態の確認という面から非常に重要なものとなっている。

現代暗号技術では暗号アルゴリズムが公開されていても暗号文から秘密鍵が得られることはないので、共通鍵暗号の攻撃方法は平文とそれに対応する暗号文が幾つか得られたという条件の下で使用された鍵の値を定める、というものである。これを既知平文攻撃という。さらに攻撃者に有利な条件として、攻撃に都合よく平文を選べる選択平文攻撃と呼ばれるものがある。

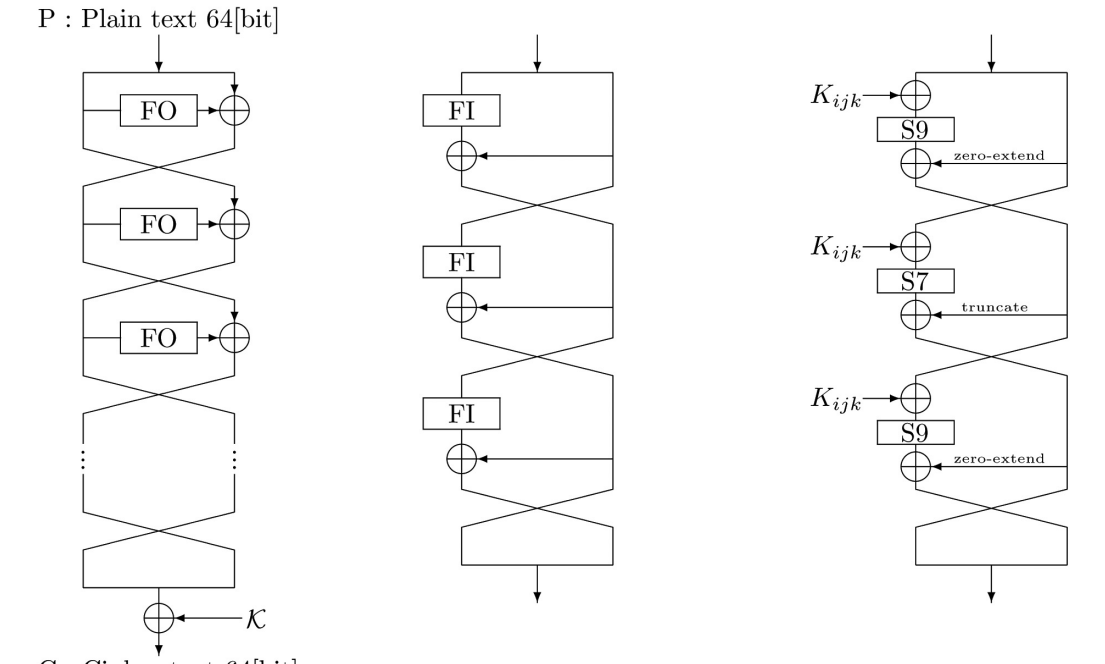

図1 変形 MISTY（$\mathcal{K}$ と K_{ijk} はそれぞれ等価拡大鍵を示す）

既知平文攻撃の代表的なものとして線形解読法が、選択平文攻撃の代表として差分解読法が知られている。一般的には選択平文攻撃に対して強いことが求められる。前述のように共通鍵暗号は幾つかの関数の組合せで構成されているので、攻撃に対する安全性は幾つかの関数を省く、関数の繰り返し回数を減らすなどした変形版に対して行い、攻撃が可能である限界と仕様の差をセキュリティマージンとする。計算機能力の拡大によってこのマージンは減少するので、前述のような安全性の状態を見積もることが重要となるのである。

本論文では共通鍵暗号の一方式であるブロック暗号に対する高階差分攻撃[3]の拡張法について示す。ブロック暗号は F 関数と呼ばれる基本関数を繰り返す構造を持つ。この繰り返しを段数と呼ぶ。a 段で構成されているブロック暗号に対して最も効果的な攻撃が $c(<b)$ 段まで攻撃可能であった時、$(a-c)$ 段をセキュリティマージンとする。攻撃者が求める鍵はユーザが直接設定する秘密鍵ではなく、各段で使用される拡大鍵の一部でもよい。これは拡大鍵の一部からでも、それを求めるのに要したコスト未満で残りの未知数を決定可能であるからである。その攻撃の効率は必要となる平文/暗号文組数と計算量で判断され、平文/暗号文組数は n[bit] ブロック暗号の場合は 2^n 組未満であることが求められる。また、計算量は秘密鍵が t[bit] であるならば 2^t 回未満の F 関数計算であることが必要である。

本論文では、選択平文攻撃の一方式である高階差分攻撃の拡張を行い、従来までの方法よりも攻撃可能な段数を増やすことが可能となった。これを 64[bit] ブロック暗号 MISTY1[6] の変形版（図 1）に対して適用し、効果を確認した。MISTY1 は 64[bit] の平文入力/暗号文出力であり 128[bit] の秘密鍵を持つ。関数は FO 関数と呼ばれる F 関数と FL 関数という補助関数で構成され、8 段の繰り返しとなっている。変形 MISTY1 とは FO 関数のみで構成され段数を少なくしたものを指す（図 1）。これは、MISTY1 が FO 関数に安全性の大部分を依存している構成であり、さらに 3 段の構成で差分解読法と線形解読法に対して証明可能安全性を持つと提案

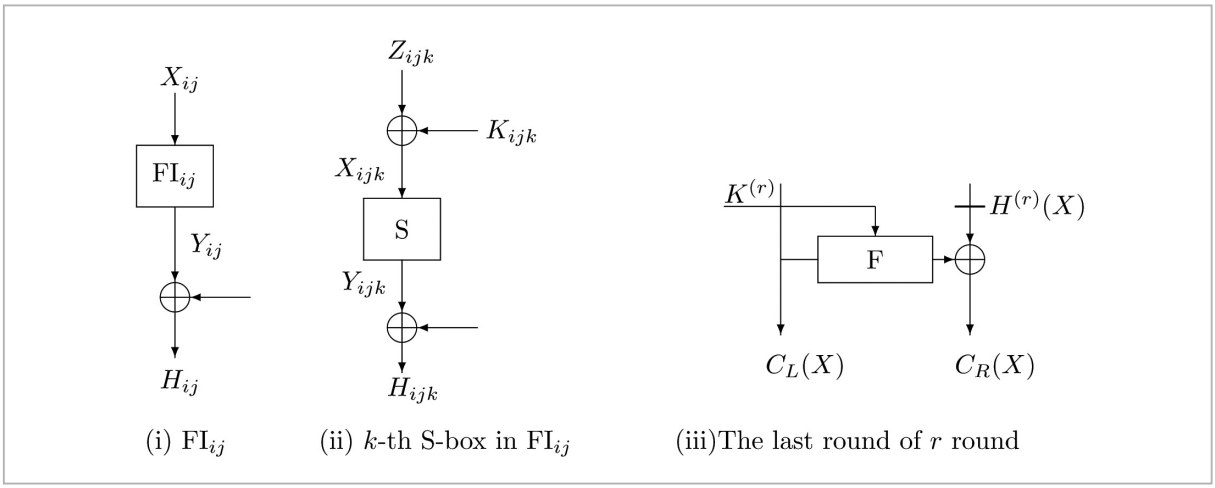

図2　本論文で使用する変数

者が主張しているものであるので適切な仮定である。従来までの安全性評価では、変形MISTY1に対して5段までの攻撃が知られている。本論文で示す高階差分攻撃の拡張により変形MISTY1が6段まで攻撃可能となった。**2**で高階差分攻撃のアルゴリズムと拡張方法として2段消去攻撃を示す。**3**で変形MISTY1の構造について述べ、**4**で変形MISTY1への具体的な攻撃を示す。**5**でまとめについて述べる。

2　高階差分攻撃

2.1　高階差分[5]

$F(X;K)$を$GF(2)^n \times GF(2)^s \rightarrow GF(2)^n$の関数とする。

$$\begin{aligned} &Y=F(X;K) \\ &X\in GF(2)^n,\ Y\in GF(2)^n,\ K\in GF(2)^s \end{aligned} \tag{1}$$

$(a_0, a_1, \cdots, a_{N-1})$を線形独立な$GF(2)^n$のベクトルとし、これらによって張られる部分空間を$V[a_0, a_1, \cdots, a_{N-1}]$とする。ここで、$\Delta^{(N)}_{V_{[a_0,a_1,\ldots,a_{N-1}]}}$を$F(X;K)$の$X$に関する$N$階差分とすると、これは以下のように計算できる。

$$\Delta^{(N)}_{V_{[a_0,a_1,\ldots,a_{N-1}]}} F(X;K) = \sum_{A\in V_{[a_0,a_1,\ldots,a_{N-1}]}} F(X+A;K) \tag{2}$$

以下では$V[a_0, a_1, \cdots, a_{N-1}]$が明らかなとき、$\Delta^{(N)}_{V_{[a_0,a_1,\ldots,a_{N-1}]}}$を$\Delta^{(N)}$と略記する。もし、$\deg_X\{F(X;K)\}=d$であるならば、以下の性質が成立する。

性質1

$$\deg_X\{F(X;K)\}=d \rightarrow \begin{cases} \Delta^{(d+1)}F(X;K)=0 \\ \Delta^{(d)}F(X;K)=\text{const.} \end{cases} \tag{3}$$

性質2

$F(X)$が$GF(2)^{ns} \rightarrow GF(2)^n$の関数であり、$V[a_0, a_1, \cdots, a_{N-1}]=GF(2)^n$であるならば、ある定数$f$に対して$\Delta^{(n)}F(X;K)=\Delta^{(n)}\mathrm{F}(X+f;K)$が成り立つ。

2.2　攻撃方程式

図2(iii)はr段Feistel型ブロック暗号の最終段を示している。$(r-2)$段目からの出力である$H^{(r)}(X)$は以下のように計算できる。

$$H^{(r)}(X)=\tilde{F}(X;K^{(1,2,\ldots,(r-2))}) \tag{4}$$

ただし$\tilde{F}(\cdot)$は$GF(2)^n \times GF(2)^{s\times(r-2)} \rightarrow GF(2)^n$の関数であり、$K^{(1,2,\cdots,(r-2))}$は1段目から$(r-2)$段目までの鍵とする。このように、$H^{(r)}(X)$は平文側から計算できる一方で、暗号文側からも最終段の鍵$K^{(r)}$を推定することによって以下のように計算できる。

$$H^{(r)}(X)=F(C_L(X);K^{(r)})+C_R(X) \tag{5}$$

もし$\deg_X\{H^{(r)}(X)\}=d$であるならば、以下の式が成立する。

$$\Delta^{(d)}\tilde{F}(X;K^{(1,2,\ldots,(r-2))})=\text{const} \tag{6}$$

式(4)(5)(6)より、以下の式が導ける。

$$\sum_{A\in V_{[a0,a1,\ldots,ad-1]}}\{F(C_L(X+A);K^{(r)})+C_R(X+A)\}=\text{const} \quad (7)$$

もしconstの値が定まれば、この方程式を解くことにより$K^{(r)}$の値を定めることができる。それゆえ、以下ではこの方程式を攻撃方程式と呼ぶ。

2.3 攻撃アルゴリズム

2.3.1 1段消去攻撃(代数的解読法)

代数的解読法[9]は下山、盛合、金子によって提案された、攻撃方程式を効率的に解くアルゴリズムである。この解読法はある攻撃方程式を線形方程式へ変形し、方程式を線形式と扱うことにより計算量を大幅に削減するものである。線形化に伴い方程式を解くために必要になる選択平文/暗号文組数は、全数探索で攻撃方程式を解く場合に比べて大幅に増加する場合があるが、計算量は無視できるほどに小さくなる。

攻撃方程式(7)は以下のように書き換えることができる。

$$\begin{aligned}&\sum_{A\in V_{[a0,a1,\ldots ad-1]}}\{F(C_L(X+A);K^{(r)})+C_R(X+A)\}\\&=\sum_{A\in V_{[a0,a1,\ldots ad-1]}}\{F(C_L(X+A);K^{(r)})\}+\sum_{A\in V_{[a0,a1,\ldots ad-1]}}C_R(X+A)\\&=\text{const}\end{aligned} \quad (8)$$

第1項は以下のように解析できる。

$$\sum_{A\in V[a0,a1,\ldots,ad-1]}F(C_L(X+A);K^{(r)})=\sum_{A\in V[a0,a1,\ldots,ad-1]\setminus\{0\}}\{F(C_L(X+A);K^{(r)})+F(C_L(X);K^{(r)})\} \quad (9)$$

ここで、$V[a0, a1, \cdots, ad-1]\setminus\{0\}$は$a_0, a_1, \cdots, a_{d-1}$からall-zeroを除いたベクトルによって張られる部分空間である。その結果、以下の攻撃方程式を得ることができる。

$$\sum_{A\in V[a0,a1,\ldots,ad-1]\setminus\{0\}}\{\Delta^{(1)}_{CR(X+A)+CR(X)}F(C_L(X+A);K^{(r)})\}+\sum_{A\in V[a0,a1,\ldots,ad-1]}C_R(X+A)=\text{const} \quad (10)$$

$F(\cdot)$の全体の次数がD(≧1)であるならば、この方程式は$K^{(r)}$に関して$D-1$次の方程式になっているはずである。$F(\cdot)\in GF(2)^n$であるから、この方程式はn個の$GF(2)$の方程式と見なすことができる。$K^{(r)}\in GF(2)^s$がXの係数として存在するのはXの次数が$D-1$次項以下であり、s個の未知数が存在していると考えることができる。

代数的解読法は、式(10)をn個の線形方程式による$K^{(r)}$に関する連立方程式として扱う。式(10)の$K^{(r)}$に関する次数は$D-1$と見なせるので(D次項はXに関しては定数)、$L=\sum_{i=1}^{D-1}{}_sC_i$の新たな未知数が存在すると考えられる。既に述べたように、1組のN階差分を用いた場合、n個の線形方程式を得ることができる。今、式(10)を解くためには最小でもL個の方程式が必要となるので、$M=\left\lfloor\frac{L}{n}\right\rfloor$の$N$階差分が必要となる。従って$M\times 2^N$の選択平文が必要となる。

最終的に、以下の方程式が得られる。

$$\begin{bmatrix} & A & \end{bmatrix}\begin{bmatrix}k_0\\k_1\\\vdots\\k_{s-1}\\k_0k_1\\\vdots\\k_{s-2}k_{s-1}\\\vdots\\k_0k_1k_2\ldots k_{s-1}\end{bmatrix}=\begin{bmatrix}b_0\\b_1\\\vdots\\b_{L-1}\end{bmatrix} \quad (11)$$

ただしAは$M'\times L$($M'=M\times 2_N$)の係数行列であり、$K^{(r)}=(k_0, k_1, \cdots, k_{s-1})$である。

$a_{ij}\in GF(2)$をAの要素とする。要素a_{ij}とb_iすべては、以下のようにして計算できる。

$$\tilde{F}_j=\sum_{A\in V[a0,a1,\ldots,aN-1]}F(C_L(X+A;e_j) \quad (12)$$

ただしe_jは以下のように計算する。

$$e_j=\begin{cases}\bar{e}_{i1},(0\le j\le s-1)\\\bar{e}_{i1}+\bar{e}_{i2},(s\le j\le {}_sC_2-1)\\\vdots\\(0,0,0,\ldots,0)\in GF(2)^{N/2},(j=L)\end{cases} \quad (13)$$

ただし$\bar{e}_i=(0, 0, 0, \cdots, \underset{\uparrow i=th}{1}, \ldots 0)$を表す。$B={}^t(b_0, b_1, \ldots, b_{L-1})$は以下のように計算できる。

$$B=\tilde{F}_L+\sum_{A\in V[a0,a1,\ldots,aN-1]}C_R(X+A)+\text{const} \quad (14)$$

$A_j={}^t(a_{0,j}, a_{1,j}, \ldots, a_{M',j-1})$, $(0\le j\le L)$とすると、これら以下のように計算できる。

$$A_j=\begin{cases}\tilde{F}_j+\tilde{F}_M,(0\le j\le s-1)\\ \tilde{F}_j+\tilde{F}_{i1}+\tilde{F}_{i2}+\tilde{F}_M,(s\le j\le {}_sC_2-1)\\ \vdots\\ \tilde{F}_j+\tilde{F}_{i1}+\tilde{F}_{i2}+\cdots+\tilde{F}_M\end{cases}\quad(15)$$

この計算手順の繰り返しによって、すべての要素が算出できる。

行列 A と B の要素の計算に必要な計算量は $M\times 2^N\times L$ 回の F 関数計算である。これらを決定した後は、Gauss-Jordan 法などを用いて逆行列を計算すれば、未知数を定めることができる。この計算量は行列 A と B の要素の計算に必要な計算量と比較すると無視できるほど小さい。したがって、必要な計算量は $M\times 2^N\times L$ 回の F 関数計算とみなしてよい。

2.3.2　2 段消去攻撃

ここでは、最終 2 段を全数探索を利用しながらまとめて解く 2 段消去攻撃について述べる。アルゴリズムを簡単に述べると、最終段の拡大鍵については全数探索を利用して攻撃方程式を導き、最終 2 段については代数的解法を適用するというものである。$K^{(r)}$ を正しく推定できれば、$K^{(r-1)}$ は攻撃方程式が不能にならずに解くことができる。しかしながら、もし $K^{(r)}$ が間違えていれば、攻撃方程式が不能になり解くことができない。このようにして、攻撃者は正しく拡大鍵が導けているかの判断ができる。攻撃方程式を以下のように拡張する。

$$[A'][K^{(r-1)}]=[B]\quad(16)$$

ただし A' は $(L+m)\times L$ の係数行列である。

最終段の拡大鍵 $K^{(r)}$ を見積もりながら攻撃方程式を導くことを考える。もし $\mathrm{rank}(A')=L$ であれば、未知数である $K^{(r-1)}$ はこの方程式を解くことにより定めることができる。$A'_i,(0\le i\le L-1)$ を A' の列ベクトルとすれば、この攻撃方程式は以下のように書き換えられる。

$$A'_0k_0+A'_1k_1+A'_2k_2+\cdots+A'_{L-1}k_{L-1}=B\quad(17)$$

この方程式が成立する時、B は $A'_0, A'_1,\cdots, A'_{L-1}$ によって張られる部分空間の要素となっている。そうでない場合は、これらはランダムに選ばれたベクトルとみなすことができる。P をこの方程式が成立する確率とする。ベクトル $A'_0, A'_1,\cdots, A'_{L-1}$ によって張られる部分空間の要素の種類は 2^{L+m} 通りである。一方、B の要素の種類は 2^L であるから P は以下のように計算できる。

$$P=\frac{2^L}{2^{L+m}}=2^{-m}\quad(18)$$

偽の拡大鍵を排除するためには、$2^s2^{-m}\ll 1$ が成立する線形方程式が必要となる。

これは 2^m の鍵候補が存在することを意味する。したがって、正しい鍵の値のみがすべての方程式を満たせるので、2^m だけ余計に計算することにより、偽の値をふるい落とすことを意味している。既に述べたように、1 組の N 階差分からは n 個の方程式しか導けない。したがって、$M'=\left\lfloor\frac{L+m}{n}\right\rfloor$ 組の N 階差分が必要となる。

$M'\times 2^N$ 個の暗号文を 1 段分だけ復号するには $M'\times 2^N$ 回の F 関数計算が必要となる。攻撃方程式を導いた後は L 回の F 関数計算を行って係数行列を定める。それゆえ、最終段の拡大鍵を見積もりながら 2 段分の拡大鍵を解くのに必要な計算量は $M'\times 2^N\times L$ 回の F 関数計算となる。さらに 2^s の候補をふるい落とすのに余計に計算しなければならないので、結果、$M'\times 2^{N+s}\times L$ 回の F 関数計算が必要となる。

結果として、2 段消去攻撃を行う場合、$M'\times 2^{N+s}\times L$ 回の F 関数計算量と $M'\times 2^N$ の選択平文が必要となる。

3　変形 MISTY1

ブロック暗号に対する汎用で強力な攻撃法である線形解読法と差分解読法に対する耐性は、構成する関数の線形もしくは差分確率の最大値に依存する。p をこれらの平均確率とする。Nyberg と Knudsen によって示された理論[8]により、3 段の Feistel 構造の線形もしくは差分確率の最大値は p^2 となる。もし、p^2 が十分小さければ、この性質は線形解読法と差分解読法に対する証明可能安全性と呼ばれている。

MISTY1 の提案者は、MISTY1 で使用されている FO 関数と呼ばれる関数が 3 段の Feistel 構造で構成されている時 $p<2^{-56}$ であることを示し、証明可能安全性を有することを示した[6]。提案者は、FO 関数で十分な安全性を確立してい

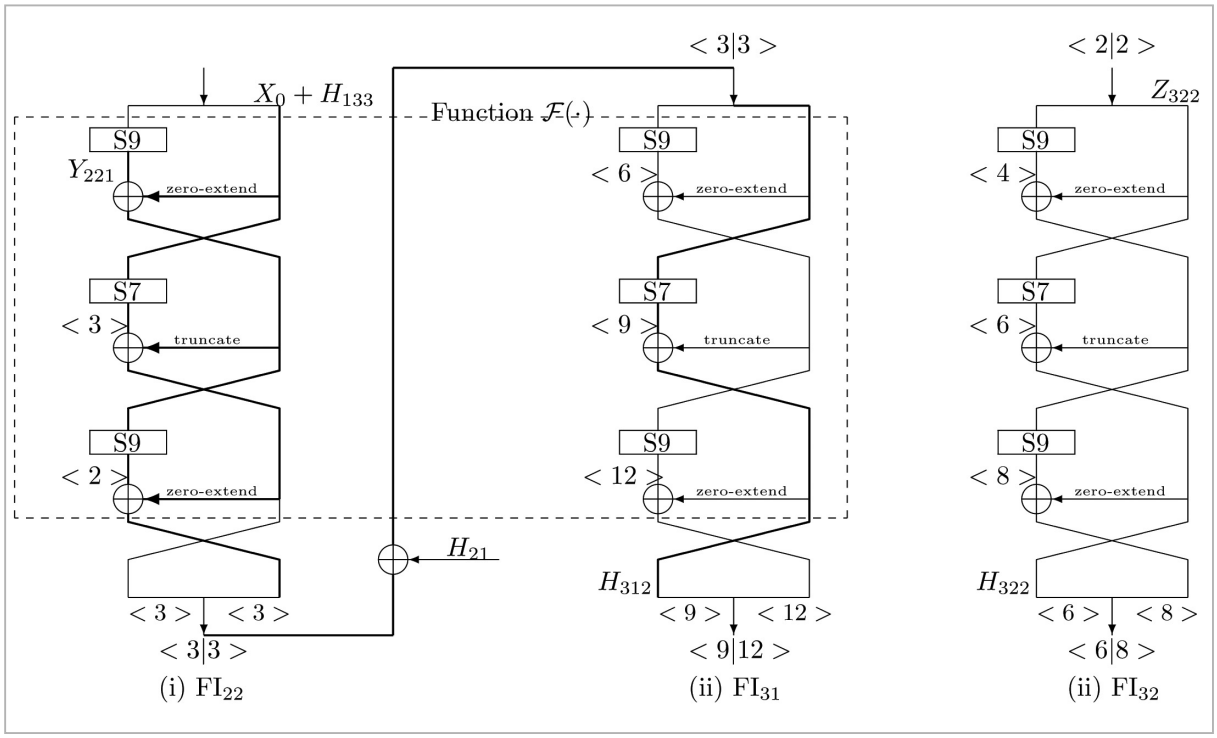

図3 形式的解析による次数の増加（図中では拡大鍵は省略）

ると主張しているが、FL 関数と呼ばれる外部関数を付加してさらなる安全性の達成を目指している。

FO 関数は更に 3 段の FI 関数で構成されるという入れ子構造になっている。各 FI 関数は S7 と S9 と呼ばれる S-box で構成されている。S-box は表で与えられる置換（Substitution）である。S7 は 7［bit］、S9 は 9［bit］であり、FI 関数は非対称な構造を持つ。S7 の次数は 3 次、S9 は 2 次である。

MISTY1 の基本的な仕様は FO 関数と FL 関数の組合せを 8 段繰り返す構造であり、平文/暗号文幅 64［bit］、秘密鍵が 128［bit］である。したがって、MISTY1 は 2^{64} 組未満の平文/暗号文組で 2^{128} 未満の計算量で攻撃可能と判断された場合、安全ではないと判断される。

本論文では、MISTY1 の本質的な安全性を達成している FO 関数と、ブロック暗号の基本的な構造である Feistel 構造の安全性に主眼を置き、FL 関数を無視する。FL 関数を除いた MISTY1 をここでは変形 MISTY1 と呼び、高階差分攻撃に対する安全性の評価を 2 段消去攻撃を用いて評価する。なお、現在までには、5 段の変形 MISTY1 が高階差分攻撃で攻撃可能なことが知られている。本論文では、この攻撃結果よりも更に多段数の攻撃についてその可能性について調査する。以下で用いる変数の位置と名称は図 2 に示すとおりである。

4 変形 MISTY1 に対する攻撃例

4.1 効果的な選択平文

高階差分攻撃の次数は平文の選択の仕方に依存する。次数は、選択平文組数と計算量に影響を与えるので、最も低い次数で攻撃が可能となる効果的な選択平文を探索することは重要である。MISTY1 の構造から、平文は以下のように 8 個のサブブロックに分割できる。

$$P = (X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0)$$
$$X_i \in \begin{cases} GF(2)^7, i = even \\ GF(2)^9, i = odd \end{cases} \quad (19)$$

本論文ではサブブロック単位で効果的な選択平文を探索した。それゆえ、どのサブブロックを変数として選ぶかで出力の次数が決定される。最も次数の増加が遅い場合について探索を行い、その結果、最右端の X_0 を変数と選び、その他のサブブロックを定数に固定した場合が最も効果

表1 H_{312}のブール展開式の一部

$\hat{h}_0$	$x_0x_1x_2x_3x_4x_5x_6 + (y_0 + y_3 + y_5 + y_6 + y_8)x_0x_1x_2x_3x_4x_5 + \cdots + 1$
$\hat{h}_1$	$(y_0 + y_2 + y_4 + y_7)x_0x_1x_2x_3x_4x_5 + \cdots + y_5y_7 + y_5y_8 + y_6y_8 + y_6$
$\hat{h}_2$	$x_0x_1x_2x_3x_4x_5x_6 + (y_0 + y_2 + y_4 + y_5 + y_7 + y_8 + 1)x_0x_1x_2x_3x_4x_5 + \cdots + 1$
$\hat{h}_3$	$x_0x_1x_2x_3x_4x_5x_6 + (y_0 + y_3 + y_4 + y_6 + y_8)x_0x_1x_2x_3x_4x_5 + \cdots + 1$
$\hat{h}_4$	$(y_0 + y_2 + y_3 + y_6 + y_7)x_0x_1x_2x_3x_4x_5 + \cdots + y_6y_7y_8 + y_7 + y_8 + 1$
$\hat{h}_5$	$x_0x_1x_2x_3x_4x_5x_6 + (y_1 + y_6 + y_8 + 1)x_0x_1x_2x_3x_4x_5 + \cdots + y_8$
$\hat{h}_6$	$x_0x_1x_2x_3x_4x_5x_6 + (y_0 + y_2 + y_5 + y_7 + 1)x_0x_1x_2x_3x_4x_5 + \cdots + y_6 + y_7$

的であることが分かった。形式的な次数の増加の見積もりが図3に示されている。記号<i | j>は左のサブブロックの次数がi、右のサブブロックがjであることを表す。

4.2 7階差分を用いた攻撃

前節で選んだ選択平文は7[bit]変数であるので、7階差分を用いた攻撃について考察する。以下のような部分空間 $V^{(7)}$ を利用する。

$$V^{(7)}=V_{[a0,a1,\ldots,a6]}\ ai=(0,0,\ldots,1,\ldots,0)\in GF(2)^{64} \quad (20)$$
$$\uparrow i\text{番目}$$

$H_{32}{}^{L7}$ を FO_3 関数からの出力の左7[bit]を表すものとする。

$$H_{32}{}^{L7}=H_{312}+H_{322}+Z_{322} \quad (21)$$

性質1から、以下の式が成立する。

$$\begin{aligned}\Delta^{(7)}H_{32}{}^{L7} &= \Delta^{(7)}(H_{312}+H_{322}+Z_{322})]_7\\ &= \Delta^{(7)}H_{312}]_7\end{aligned} \quad (22)$$

ただし記号 $]_d$ は d 未満の次数の項を無視する演算とする。

$F(\cdot)$ を図3に示すように $GF(2)^7 \times GF(2)^9 \rightarrow GF(2)^7$ の関数とする。

$$H_{312} = F(X_0 + H_{133} + K_{222}; Y_{221}) \quad (23)$$

Y_{221} は、選択平文中では固定の定数であることに注意。X_0 は $GF(2)^7$ の部分空間を張るので、性質2から以下の式が成立する。

$$\begin{aligned}\Delta^{(7)}H_{312} &= \Delta^{(7)}F(X_0 + H_{133} + K_{222}; Y_{221})\\ &= \Delta^{(7)}F(X_0; Y_{221})\end{aligned} \quad (24)$$

以上より、以下の7階差分が得られる。

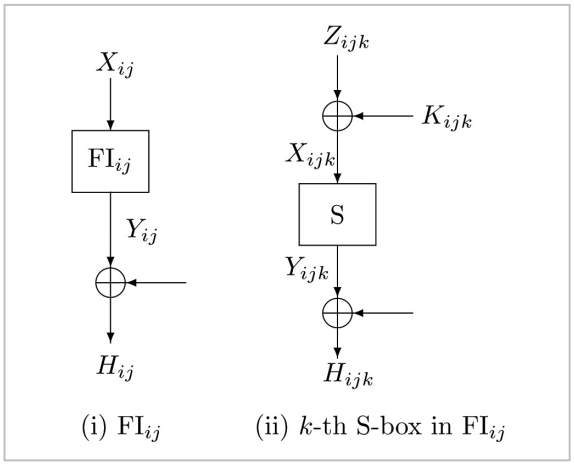

図4 インターネットリスク分析モデル

$$\Delta^{(7)}H_{32}^{L7} = \Delta^{(7)}F(X_0; Y_{221})]_7 \quad (25)$$

H_{312} のブール代数式を計算した結果、以下のことが明らかとなった。

1) H_{312} の次数は7である。
2) $H_{32}{}^{L7}$ の7階差分値は $0x6D$ に等しい。
3) 次数が6の係数は Y_{221} に関する多項式となっている。

表1に計算結果の一部を示す。

$$\begin{aligned}&X_{222}=(x_6,\ldots,x_0), \quad (X_{222}=X_0+H_{133}+K_{222})\\ &Y_{221}=(y_8,\ldots,y_0), \quad H_{312}=(\hat{h}_6,\ldots,\hat{h}_0)\end{aligned} \quad (26)$$

$\Delta^{(7)}H_{32}{}^{L7} = 0x6D$ を用いて、以下の攻撃方程式が導かれる。

$$\sum_{\substack{A\in V^{(7)}\\ K=(K_L,K_R)}} \{FO(C_L(P+A)+K_L; K_{522}K_{521}, K_{512}, K_{511}) + C_R(P+A)+K_R\} = 0x6D \quad (27)$$

最後に追加されている等価鍵 K は図4に示すように移動できる。FO_5 関数中で、K_L は更に K_{Ll} と K_{Lr} に分割できる。

$$K_{511}=K_{511}+K_{LI}^{L9}$$
$$K_{512}=K_{512}+K_{LI}^{R7} \quad (28)$$

さらに、FI_{51} 中では以下のように書ける。

$$K_{521}=K_{521}+K_{LI}^{L9}$$
$$K_{522}=K_{522}+K_{LI}^{R7} \quad (29)$$

よって、攻撃方程式は以下のように書き換えることができる。

$$\sum_{A\in V^{(7)}}\{FO(C_L(P+A);\ K_{522}\ \ K_{521},\ K_{512},\ K_{511})+C_R(P+A)\}=0x6D \quad (30)$$

7[bit]の値 $H_{32}{}^{L7}$ を基に攻撃方程式を導いているので、この方程式は 7[bit]幅である。それゆえ、7[bit]以上の値のものは適切な値が選ばれていることに注意する。

4.3 必要な選択平文組数と計算量

4.3.1 1段消去攻撃

2.3 で示した代数的解法を適用する。

K_{511}, K_{512}, K_{521}, K_{522} に関する項から生成される独立な未知数の種類数について算出する。攻撃方程式は二つの 9[bit]変数 K_{511}, K_{521} と二つの 7[bit]変数 K_{512}, K_{522} で構成され、9[bit]の変数の次数は 1、7[bit]の変数の次数は 2 である。よって、未知数の総数 $L=2\times(9+7+{}_7C_2)=74$ である。1 組の 7 階差分から 7 個の線形方程式が導かれるので、$\left\lfloor\frac{74}{77}\right\rfloor=11$ 組の 7 階差分が必要である。その結果、

$$M\times 2^N=11\times 2^7=1{,}408 \quad (31)$$

の選択平文と

$$M\times 2^N\times L=11\times 2^7\times 74\fallingdotseq 2^{17} \quad (32)$$

の F 関数計算が必要となる。この結果、攻撃者は 5 段構成の変形 MISTY1 の攻撃を、鍵の全数探索よりも効率よく実行できることが分かる。

4.3.2 2段消去攻撃

ここでは、**2.3.2** で示した 2 段消去攻撃を適用した場合について示す。FO 関数は 75[bit]の鍵を持つので $s=75$ である。したがって $m=91$ と設定した。

$$2^s\times 2^{-m}=2^{75}\times 2^{-91}\ll 1 \quad (33)$$

それゆえ、$M'=\left\lfloor\frac{74+91}{7}\right\rfloor\approx 24$ 組の 7 階差分が必要となる。その結果、

$$M\times 2^N=24\times 2^7\fallingdotseq 2^{12} \quad (34)$$

の選択平文と

$$M\times 2^{N+s}\times L=11\times 2^{7+75}\times 74\fallingdotseq 2^{93} \quad (35)$$

の F 関数計算が必要となる。この結果、攻撃者は 6 段構成の変形 MISTY1 の攻撃を、鍵の全数探索よりも効率よく実行できることが分かる。

5 まとめ

本論文では高階差分攻撃の拡張として、代数的解法と全数探索を組み合わせた 2 段消去攻撃を提案した。その場合の、必要な選択平文と計算量についての計算式を示し、変形 MISTY1 に対する具体的な攻撃例で効果を確認した。

本結果により、7 階差分を用いて FL 関数のない MISTY1 が攻撃可能であることが分かった。6 段目の拡大鍵に対して全数探索を、5 段目の拡大鍵に対しては代数的解法を適用し、2^{12} 個の選択平文と 2^{93} 回の F 関数計算が必要となる。それゆえ、128[bit]の秘密鍵の全数探索と比較して 2^{30} 倍以上早い攻撃である。この結果から、少なくとも MISTY1 の FO 関数を用いた Feistel 構造ブロック暗号の場合は、7 段以上で構成しなければ高階差分攻撃に対して安全ではない。

参考文献

1 Babbage, Frisch, "On MISTY1 Higher Order Differential Cryptanalysis", 3rd International Conference on Information Security and Cryptology 2000, LNCS2015, pp.1-13, Springer-Verlag, 2000.
2 Daemen, Govaerts, Rijmen, "The Block Cipher SQUARE", 4th Fast Software Encryption. LNCS1267, pp.149-165, Springer-Verlag, 1997.
3 Jakobsen, Knudsen, "The interpolation attack on block cipher", 4th Fast Software Encryption LNCS1267, pp.28-40, Springer-Verlag, 1997.
4 Knudsen, "Truncated and higher order differentials", 2nd Fast Software Encryption LNCS1008, pp.196-211, Springer-Verlag, 1995.
5 Lai, "Higher order derivatives and differential cryptanalysis", Communications and Cryptology, pp.227-233, Kluwer Academic Publishers, 1994.
6 Matui, "New structure of block ciphers with provable security against differential and linear cryptanalysis", 3rd Fast Software Encryption LNCS1039, pp.205-218, Springer-Verlag, 1996.
7 Moriai, Shimoyama, and Kaneko, "Higher order differential attack of CAST cipher", 4th Fast Software Encryption LNCS1372, pp.17-31, Springer-Verlag, 1997,
8 Nyberg, Knudsen "Provable security against differential cryptanalysis", Journal of Cryptology, Vol.8, No.1, pp.27-37, 1995.
9 Shimoyama, Moriai, and Kaneko, "Improving the higher order differential attack and cryptanalysis of the KN cipher", 1997 Information Security Workshop LNCS 1396, pp.32-42, Springer-Verlag, 1997,
10 Tanaka, Hisamatsu, and Kaneko, "Strength of MISTY1 without FL functions for higher order differential attack", 13th International Symposium, Applied Algebra – Algebraic Algorithm and Error-Correcting Codes 1999 LNCS1719, pp.221-230, Springer-Verlag, 1999.

田中秀磨（たなかひでま）
情報通信部門セキュリティ基盤グループ研究員　博士（工学）
暗号理論、情報セキュリティ

金子敏信（かねこ としのぶ）
東京理科大学教授　博士（工学）
暗号理論、情報セキュリティ