FL 関数の無い 8 段 MISTY2 への高階差分攻撃の高速化

五十嵐保隆[†1]　橋口陽介[†1]　金子敏信[†2]
福島誠治[†1]　八野知博[†1]

MISTY2 は 1996 年に三菱電機の松井が提案したブロック暗号アルゴリズムであり、ブロック長は 64 ビット、鍵長は 128 ビットである。以前に我々は FL 関数の無い MISTY2 で 8 段目の FI_{S2} 関数入力の上位 7 ビットの 32 階差分がゼロとなる特性を発見し、この特性を利用した攻撃手法を報告した。本稿では Ferguson らが提案した部分和法を用いて、解読時の中間データの mod2 頻度分布関数を導出することにより、攻撃に要する計算量を削減し、32 階差分攻撃を高速化できることを報告する。結果として従来の攻撃手法よりも約 2^{17} 倍高速化できることを示す。

The improved 32nd-order differential attack on MISTY2 without FL functions

Yasutaka Igarashi,[†1] Yosuke Hashiguchi,[†1]
Toshinobu Kaneko,[†2] Seiji Fukushima[†1]
and Tomohiro Hachino[†1]

MISTY2 is a 64-bit block cipher with 128-bit secret key proposed by Matsui of Mitsubishi Electric Corp. in 1996. We previously found the 32nd-order differential characteristic of MISTY2 without FL functions, which makes the differential of upper 7 bits of 9-bit input to the 8th-round FI_{S2} function be zero. Using this characteristic, we also showed that 8-round MISTY2 without FL functions can be attacked with 2^{35} of chosen plaintexts and $2^{81.4}$ of computational complexities of FO function. In this paper we reduce the complexities of this attack by using a mod 2 occurrence distribution, which is derived by a partial sum technique proposed by Ferguson et al. We apply this distribution to intermediate data under cryptanalysis, and show that the complexities can be reduced to $2^{64.5}$.

1. はじめに

MISTY2 は 1996 年に MISTY1 と共に三菱電機の松井によって提案された秘密鍵長 128bit の 64bit ブロック暗号である[1)]。MISTY2 は 12 段の FO 関数と 14 個の FL 関数で構成することが推奨されている。FO 関数は非線形関数であるが、FL 関数は秘密鍵が固定されている限りは線形関数である。従って FL 関数は差分攻撃や線形攻撃に対する証明可能安全性を左右するものではなく、これまでに FL 関数の無い MISTY2 の攻撃について幾つか報告がされている。それらの攻撃コストと本稿での攻撃コストを表 1 に示す。杉田らは 5 段目の 7 階差分特性を利用して、選択平文数 2^7 と FO 関数演算回数 2^{39} の高階差分攻撃を FL 関数無しの 5 段 MISTY2 に適用した[2)]。以前に我々は 7 段目の 7 階差分特性を利用して、選択平文数 2^{11} と FO 関数演算回数 2^{83} の高階差分攻撃を FL 関数無しの 7 段 MISTY2 に適用した[3)]。また文献[4)] はこれまでに最も成果の上がっている攻撃の報告であり、我々は 8 段目の FI_{S2} 関数の入力 9bit のうち上位 7bit の 32 階差分がゼロになるという今までに知られていない新たな高階差分特性を発見し、この特性を利用することにより従来は攻撃不可能であった 8 段 MISTY2 が選択平文数 2^{35}、FO 関数演算回数 $2^{81.4}$ で攻撃できることを示した。本稿では文献[4)] の解読アルゴリズムを改良し、解読演算回数を削減する手法を示す。具体的には Ferguson らが提案した部分和法[5)] を利用して、解読時の中間データの mod2 頻度分布関数を導出することにより演算回数を削減する。その結果として演算回数を従来の $2^{81.4}$ から $2^{64.5}$ に削減できることを示す。

表 1　MISTY2 の高階差分攻撃コスト.

攻撃対象	差分特性	平文数	演算回数	文献
5 段, FL 無	5 段, 7 階	2^7	2^{39}	2)
7 段, FL 無	7 段, 7 階	2^{11}	2^{83}	3)
8 段, FL 無	8 段, 32 階	2^{35}	$2^{81.4}$	4)
8 段, FL 無	8 段, 32 階	2^{35}	$2^{64.5}$	本稿

†1 鹿児島大学
Kagoshima University
†2 東京理科大学
Tokyo University of Science

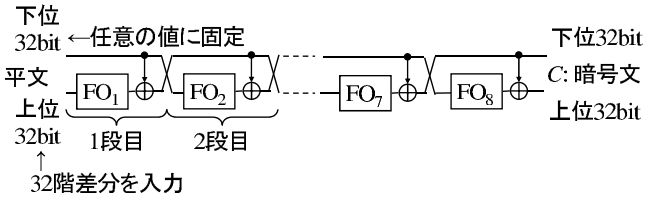

図 1 FL 関数の無い 8 段構成の MISTY2.

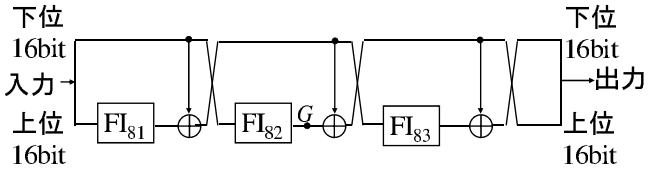

図 2 FO_8 関数.

2. FL 関数の無い 8 段の MISTY2

ここでは攻撃対象とする FL 関数の無い 8 段の MISTY2 の全体構造を示し、その構成要素である FO_i 関数並びに FI_{ij} 関数の等価関数を示す。尚、本稿において FI_{ij} 関数の等価変形は重要な話題ではないので省略する。変形の詳細は文献[4] を参照されたい。

図 1 に FL 関数の無い 8 段構成の MISTY2 を示す。入力平文、出力暗号文ともに 64bit である。構成要素は XOR ($\oplus$) と FO_i (i=1, 2, $\cdots$, 7, 8) である。ここでは 1 つの FO_i 関数とそれに続く XOR を含む 64bit 入出力の回路構造を「段」と呼ぶ。図 2 に FO_8 関数を示す。FO_1 から FO_7 も FO_8 関数と同じ構造である。入出力は 32bit であり、XOR と非線形関数である FI_{8j} (j=1, 2, 3) から構成される。図 3 に FI_{8j} 関数の等価関数を示す。FI_{1j} から FI_{7j} の等価関数も FI_{8j} の等価関数と同じ構造である。入出力は 16bit であり、XOR と S_9 及び S_7 で表される S-box から構成される。S_9 は 9bit の S-box であり、S_7 は 7bit の S-box である。KI'_{8j1} と KI'_{8j3} は共に 9bit の等価鍵であり KI'_{8j2} は 7bit の等価鍵である。

3. 高 階 差 分

本節では高階差分の定義を示し、高階差分の様々な性質のうち本稿に関係する事項及びその性質を利用した攻撃方程式について一般的に述べる[⋆1]。次に我々が文献[4] で報告した MISTY2 の 32 階差分特性とその特性を用いた攻撃方程式を示す。

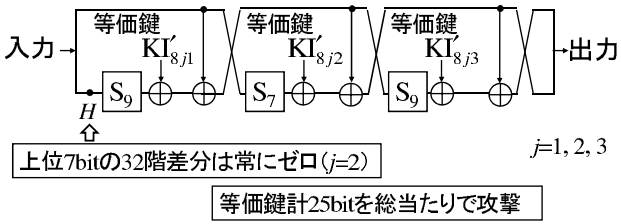

図 3 FI_{8j} 等価関数

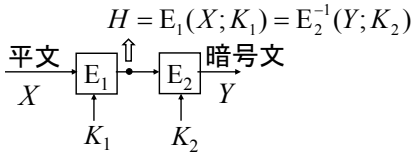

図 4 暗号回路モデル.

3.1 定義、性質及び攻撃方程式[6]

図 4 の暗号回路モデルを例にして高階差分の定義、性質を示し、高階差分を利用した攻撃方程式を示す。

定　　義

E_1, E_2 はそれぞれ暗号化関数の構成要素を表し、$K_1 \in GF(2)^{s_1}$, $K_2 \in GF(2)^{s_2}$ はそれぞれ s_1 bit, s_2 bit の暗号化鍵を表す。$X = (x_1, x_2, \cdots, x_n) \in GF(2)^n$, $H \in GF(2)^m$, $Y = (y_1, y_2, \cdots, y_\ell) \in GF(2)^\ell$ はそれぞれ E_1 への入力 n bit, E_1 の出力 m bit, E_2 の出力 ℓ bit を表し、$H = E_1(X; K_1)$ とする。ここで $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_i$ を $GF(2)^n$ 上の 1 次独立な i 個のベクトルとするとき、これらのベクトルによって張られる $GF(2)^n$ の部分空間 $V^{(i)}$ を入力差分という。そして次式で定義される $\Delta^{(i)}E_1(X; K_1)$ を関数 $E_1(X; K_1)$ の $V^{(i)}$ に関する i 階差分という。

⋆1 高階差分の詳細な性質に関しては文献[6] を参照されたい。

$$\Delta^{(i)}\mathrm{E}_1(X;K_1) \equiv \sum_{A\in V^{(i)}}^{\oplus} \mathrm{E}_1(X\oplus A;K_1). \quad (1)$$

ここで $\sum^{\oplus}$ は XOR による総和を表す。

性　　質

今、$\mathrm{E}_1(X;K_1)$ の X に関するブール代数次数が N ならば、次式のように $N+1$ 階差分 $\Delta^{(N+1)}\mathrm{E}_1(X;K_1)$ は X と K_1 に依存せずにゼロになる性質をもつ。

$$\Delta^{(N+1)}\mathrm{E}_1(X;K_1) = 0. \quad (2)$$

さらに $\mathrm{E}_1(X;K_1)$ のブール展開式が x_t $(1 \le t \le n)$ の j 次項 (例えば $x_{t_1}x_{t_2}\cdots x_{t_j}$) を含まなければ、$j$ 個のベクトル $\{\boldsymbol{x}_{t_1}, \boldsymbol{x}_{t_2}, \cdots, \boldsymbol{x}_{t_j}\}$[⋆1]によって張られる $\mathrm{GF}(2)^n$ の部分空間 $V^{(j)}$ に関する j 階差分 $\Delta^{(j)}\mathrm{E}_1(X;K_1)$ は次式のように X と K_1 に依存せずにゼロになる性質を持つ。

$$\Delta^{(j)}\mathrm{E}_1(X;K_1) = 0. \quad (3)$$

攻撃方程式

今、例として式 (2) が成り立っているとする。この時、関数 E_2 の逆関数を E_2^{-1} とし、K_2 を推定して E_2 の出力 Y から E_1 の出力 H へと遡ることにより次式が成り立つ[⋆2]。

$$\Delta^{(N+1)}\mathrm{E}_2^{-1}(Y;K_2) \equiv \sum_{A'\in V'^{(N+1)}}^{\oplus} \mathrm{E}_2^{-1}(Y\oplus A';K_2) = 0. \quad (4)$$

ここで $V'^{(N+1)}$ は入力差分 $V^{(N+1)}$ によって得られる Y 端の出力差分 (つまり、$\mathrm{GF}(2)^\ell$ 上の部分空間) を表す。式 (4) は暗号化鍵 K_2 の推定が正しい時、常に成立する。一方、推定が誤りの時はランダムに成立すると考えられる。従って推定した K_2 の真偽は式 (4) を用いて検査できる。このように式 (2) のような高階差分の性質を利用した攻撃を高階差分攻撃といい、式 (4) を攻撃方程式という。

3.2 MISTY2 の 32 階差分特性と攻撃方程式

ここでは図 1 に示す FL 関数の無い MISTY2 について我々が文献[4] で報告した 32 階差分特性を示す。初めに入力平文 64bit の内、下位 32bit を任意の値に固定し上位 32bit に 32 階差分を入力する。つまり 0x00000000[⋆3]から 0xffffffff までの全 2^{32} 通りのデータを上位 32bit に入力する。この時、図 3 に示される FI_{82} 等価関数の H 点の 9bit データの内、上位 7bit の 32 階差分がゼロになるという性質を発見した。さらにこの性質を利用して式 (4) に対応する攻撃方程式を立てると次式となることを報告した。

$$\sum_{A'\in V'^{(32)}}^{\oplus} \left\{\mathrm{FI}_{82}^{-1}(G;\mathrm{KI}'_{821},\mathrm{KI}'_{822},\mathrm{KI}'_{823})\right\}^{\mathrm{L}_7} = 0. \quad (5)$$

但し、

$$G \equiv \mathrm{FI}_{83}^{-1}((C\oplus A')^{\mathrm{L}_{16}}\oplus(C\oplus A')^{\mathrm{R}_{16}};\mathrm{KI}'_{831},\mathrm{KI}'_{832},\mathrm{KI}'_{833}) \oplus (C\oplus A')^{\mathrm{L}_{16}}. \quad (6)$$

ここで FI_{82}^{-1} と FI_{83}^{-1} はそれぞれ FI_{82} と FI_{83} の逆関数を表し、C は 64bit の暗号文出力を表す。16bit 変数 G は図 2 中の G 地点の値に対応する。また、$(x)^{\mathrm{L}_y}$ は値 x の上位 y bit のみが演算対象であることを表し、$(x)^{\mathrm{R}_y}$ は x の下位 y bit のみが演算対象であることを表す。式 (5), (6) より計 50 bit の等価鍵 (KI'_{821}, KI'_{822}, KI'_{823}, KI'_{831}, KI'_{832}, KI'_{833}) が解読できる。

4. mod2 頻度分布関数の導入による攻撃計算量の削減

本節では Ferguson らが提案した部分和法[5] を利用して、式 (6) の mod2 頻度分布関数を導出することにより、式 (5) の計算量を削減できることを示す。

はじめに式 (6) において全て (2^{32} 通り) の A' に対する G の具体的な値の頻度分布関数 $f(G)$ を求める。次に $f(G)$ の mod2 に着目した mod2 頻度分布関数 $f'(G)$ ($= f(G) \bmod 2$) $\in \{0, 1\}$ を求める。mod2 に着目する理由は次の通りである。ある変数 x の偶数個の XOR は必ずゼロであり、奇数個の XOR は必ず x である。従って mod2 頻度分布関数を求めておけば、それ以降の演算において変数 x の偶数個の XOR は不要となり、奇数個の XOR 演算結果も x で置き換えることができ、計算量を削減できる可能性がある。具体的には MISTY2 の出力差分 V' の空間よりも変数 G の空間の方が小さければ計算量を削減できる (今回は G の空間の方が小さい)。

次に集合 G_1 を $G_1 = \{g | f'(g) = 1\}$ とすると、式 (5) は次式で書き直せる。

⋆1 $\boldsymbol{x}_{t_1}$ は n bit のうち t_1 bit 目のみが 1 であり、残りは全てゼロである $\mathrm{GF}(2)^n$ 上のベクトルを表す。
⋆2 式 (3) が成り立っている場合も同様のことが成り立つ。
⋆3 記号 0x はこれに続く数字が 16 進数であることを表している。

$$\sum_{G\in G_1}^{\oplus}\left\{\mathrm{FI}_{82}^{-1}(G;\mathrm{KI'}_{821},\mathrm{KI'}_{822},\mathrm{KI'}_{823})\right\}^{\mathrm{L}_7}=0. \quad (7)$$

G は 16bit 変数なので集合 G_1 の要素数は高々2^{16} であり、G が一様ランダムな変数であれば G_1 の要素数の平均は 2^{15} である。従って式 (5) では計 2^{32} 回の XOR 演算が必要となるが、式 (7) では高々2^{16} 回に削減される。

次に式 (6), (7) における計 50bit の等価鍵を総当りで解読する為に必要な選択平文数と FO 関数の演算回数を見積もる。式 (7) は 7bit 分について成り立つ方程式なので、推定した鍵が偽であっても確率 2^{-7} で方程式が成り立つ。また、推定する鍵 ($\mathrm{KI'}_{821}$, $\mathrm{KI'}_{822}$, $\mathrm{KI'}_{823}$, $\mathrm{KI'}_{831}$, $\mathrm{KI'}_{832}$, $\mathrm{KI'}_{833}$) の bit 総数は 50 であり、鍵の候補数は 2^{50} である。従って独立な攻撃方程式を 8 ($=\lceil 50/7\rceil$) つ用意して検査すれば、推定した鍵が最終的に偽である確率は 2^{-6} ($=(2^{-7})^8\times 2^{50}$) となり、真の鍵を十分に特定できる。独立な攻撃方程式を 1 つ用意するには 32 階差分を 1 組用意する必要があるので、攻撃方程式を 8 つ用意するために必要となる選択平文数 D は次式で与えられる。

$$D=8\times 2^{32}=2^{35}. \quad (8)$$

次に 8 つ攻撃方程式を検査するために要する FO 関数の演算回数を考察する。はじめに計 25bit の 3 つの等価鍵 $\mathrm{KI'}_{831}$, $\mathrm{KI'}_{832}$, $\mathrm{KI'}_{833}$ を仮定し、式 (6) における G の mod2 頻度分布関数を作成するためには関数 FI_{83}^{-1} を 2^{32} 回計算する必要がある。さらに計 25bit の 3 つの等価鍵 $\mathrm{KI'}_{821}$, $\mathrm{KI'}_{822}$, $\mathrm{KI'}_{823}$ を仮定し、作成した mod2 頻度分布関数を用いて式 (7) が成り立つか否かの検査をするためには、関数 FI_{82}^{-1} を最大で 2^{16} 回計算する必要がある。計 2^{50} 通りの鍵候補について式 (7) の成立を 1 回検査すると鍵候補数は 2^{-7} 減少して 2^{43} になる。さらに 2^{43} の鍵候補について 1 回目とは独立な式 (7) の成立をもう 1 回検査すると候補数は更に減少して 2^{36} となる。この検査を計 8 回繰り返して、最後に残った鍵候補が真の鍵といえる。ここで FO_i 関数は FI_{ij} 関数を 3 つ含むことと、FI_{ij} 関数と FI_{ij}^{-1} 関数の演算量は等しいことを勘案すると、式 (6), (7) にある FI_{82}^{-1} と FI_{83}^{-1} の演算回数に 1/3 を乗じたものが FO 関数演算回数に相当するといえる。以上をまとめると攻撃に要する FO 関数演算回数 T は次式で与えられる。

$$T=2^{25}\sum_{i=0}^{7}\left\{2^{32}\times\frac{1}{3}+2^{16}\times 2^{25-7i}\times\frac{1}{3}\right\}\approx 2^{64.5}. \quad (9)$$

5. おわりに

本稿では MISTY2 について最も成果の上がっている解読アルゴリズムについて、Ferguson らが提案した部分和法を利用することにより、解読時の中間データの mod2 頻度分布関数を導出し、攻撃計算量を削減した。mod2 頻度分布関数適用前の計算量は約 $2^{81.4}$ であったが、適用後のそれは約 $2^{64.5}$ となり、計算量は約 $1/2^{17}$ に削減することが可能となった。本研究とは別件で我々は部分和法を高速化する手法を提案している[7]。この高速化手法を MISTY2 に適用し、更に攻撃計算量を削減する事が今後の検討課題である。

参考文献

1) 三菱電機 Web site, http://www.mitsubishielectric.co.jp/corporate/randd/information_technology/security/code/misty01_b.html
2) 杉田誠, “ブロック暗号 MISTY1, 2 の高階差分解読について,” 信学技報, ISEC, vol.98, no.48 (19980515), pp.31–40.
3) Y. Hatano, H. Tanaka, and T. Kaneko, “Higher order differential attack of MISTY2 without FL functions,” Proc. of The International Conference on Fundamentals of Electronics, Communications and Computer Sciences, sect.17, pp.6–10, March, 2002.
4) 五十嵐保隆, 金子敏信, “FL 関数の無い 8 段の MISTY2 への 32 階差分攻撃,” 情報理論とその応用シンポジウム, no. 5.2.1, pp. 522–525, 2008.
5) N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting,“Improved Cryptanalysis of Rijndael,” Lecture Notes in Computer Science, 2001, Volume 1978/2001, pp. 136-141, Springer
6) CRYPTREC 応募暗号の高階差分及び補間攻撃耐性について (Ver.1), pp.3–7, 平成 13 年 1 月, http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/113_report.pdf
7) 井上祐輔, 北川明伸, 金子敏信, “高階差分攻撃における攻撃方程式解法の高速化,” 2012 年暗号と情報セキュリティシンポジウム, no.2C1-6, 2012 年 1 月.