ブロック暗号 MISTY1 の新しい高階差分特性

佐藤亮介 †　金子敏信 †
東京理科大学大学院理工学研究科 †

1　はじめに

ブロック暗号 MISTY1 は 1996 年に三菱電機の松井らによって提案された共通鍵ブロック暗号である。
これまでに、MISTY1 の高階差分特性として、38 階差分特性で 4 ラウンド右半分データの上位 7bit 出力の高階差分値が 0 であることが報告されている。[2] 本稿ではこの高階差分特性の理論的理由について調査する過程で新たに判明した特性について示す。

2　高階差分特性

ここでは高階差分特性について説明する。入力 $X \in GF(2)^n$、鍵 $K \in GF(2)^s$ から暗号文 $Y \in GF(2)^m$ を出力する暗号化関数を $Y = F(X;K)$ とする。$F(X;K)$ の X に関する i 階差分は以下の式で定義される。

$$\Delta^{(i)}_{V^{(i)}} F(X;K) = \bigoplus_{a \in V^{(i)}} F(X \oplus a;K) \tag{1}$$

$V^{(i)}$ は $GF(2)^n$ の i 次元部分空間を表し、その要素 a を入力差分とする。以降 $V^{(i)}$ を明記する必要がない限り、$\Delta^{(i)}_{V^{(i)}}$ を $\Delta^{(i)}$ と省略して記す。

また、$F(X;K)$ の X に関する次数が N 次であるならば X の値に関わらず以下の式が常に成立する。

$$deg_x F(X;K) = N \Rightarrow \begin{cases} \Delta^{(N+1)} F(X;K) = 0 \\ \Delta^{(N)} F(X;K) = const \end{cases} \tag{2}$$

3　MISTY1 の高階差分特性

ここで、i ラウンド目の 64bit 入力データを X^i と定義する。1 ラウンド目の入力データ X^1 は平文 P とする。また、X^i を以下のようにサブブロックに分割する。

$$X^i = (X^i_7, X^i_6, X^i_5, X^i_4, X^i_3, X^i_2, X^i_1, X^i_0) \tag{3}$$
$$X^i_L = (X^i_7, X^i_6, X^i_5, X^i_4), X^i_R = (X^i_3, X^i_2, X^i_1, X^i_0)$$
$$X^i_j \in \begin{cases} GF(2)^7 : j = even \\ GF(2)^9 : j = odd \end{cases} \tag{4}$$

ここで、X^i_L、X^i_R をそれぞれ i ラウンド目の左半分、右半分の入出力データと定義する。また、$m$bit データ Z の第 $k$bit を $Z[k](0 \le k < m)$ と表記し、Z の第 $k$bit から第 $l$bit データを $Z[k-l]$ と表記する。

3.1　高階差分特性の調査

38 階差分特性を元に調査したところ、以下の結果を得た。

3.1.1　50 階差分特性

38 階差分特性の延長で 50 階差分を調査した。4 ラウンド右半分データ Y^4_R に以下のような 50 階差分特性がある。
高階差分入力：X^1_R,X^1_7,X^1_5
高階差分値：$Y^4_R[31-9] = 0$

3.1.2　FL 関数を含まない 32 階差分特性

FL 関数を含まない 32 階差分特性を調査し、以下の場所の高階差分値が 16 進数表現で 0x54 であることが判明した。
・4 ラウンド目の FI 関数内 1 つ目 S7 後の上位 9bit と排他的論理和した高階差分値
・4 ラウンド目の FI 関数内 2 つ目 S7 後の上位 9bit と排他的論理和した高階差分値
これは拡大鍵と選択平文の固定 bit の値に依存しない。

3.1.3　FL 関数を含まない 47,48 階差分特性

また，32 階差分特性の延長で 47，48 階差分を調査した。まず、4 ラウンド右半分データ Y^4_R に以下のような 47 階差分特性がある。
高階差分入力：X^1_R,X^1_7,X^1_6 の内 5bit
高階差分値：$Y^4_R[31-9] = 0$

続いて、4 ラウンド右半分データ Y^4_R に以下のような 48 階差分特性がある。
高階差分入力：X^1_R,X^1_7,X^1_6
高階差分値：$Y^4_R[31] = 0$

4　結論

本稿では、計算機実験により、FL 関数を含まない MISTY 1 について、32 階差分特性の定数部分、47 階差分特性、48 階差分特性を発見した。また、FL 関数を含む MISTY1 について 50 階差分特性を発見した。従来に比べ、高階差分値が 0 となる bit 幅が広がった。

参考文献

[1] 齊藤 照夫, 川幡 剛嗣, 中川 弘勝, 角尾 幸保, “MISTY1 の新しい高階差分特性,” SCIS 2011, 2B2-1, 2011.
[2] 望月拓良, 金子敏信, “MISTY1 の新しい高階差分特性,” SCIS 2012, 2C1-4, 2012

Copyright © 2015 IEICE