付録J:IPA 詳細評価対象暗号の線形和攻撃耐性

1. はじめに

情報処理振興事業協会(IPA)詳細評価対象暗号に対して、耐線形和攻撃という視点から調査した結果を報告する。

2. 線形和攻撃に対する強度評価

IPA 詳細評価対象暗号に対して GF(2^8)上の多項式を利用した線形和攻撃の強度評価を行った。評価手法は以下の通りである。

① 平文を $p=(x_1,x_2,\cdots,x_i,\cdots)\quad x_i(1\le i\le 16)$ (64bit 暗号は $x_i(1\le i\le 8)$)と byte 毎に分割し、任意の 1byte を変数とする。他は 0 に固定する。
② その時得られる n 段目の暗号文 $c=(y_1,y_2,\cdots,y_i,\cdots)\ y_i(1\le i\le 16)$ (64bit 暗号は $y_i(1\le i\le 8)$)の y_i を GF(2^8)上の多項式として表す。
③ これを予め用意しておいた、258 個(128bit)のランダムなマスター鍵に対して行う。
④ 得られた 258 本の GF(2^8)上の多項式について、未知係数個数を見積もる。
⑤ ①～④を全ての x_i , y_i に対し計算し最小未知係数個数を見積もる。

全ての8次原始多項式(16 種類)それぞれを法多項式とする多項式基底で、ガロア体 GF(2^8)を考え、上記を実行し最小未知係数個数を示せば表 1 である。

表 1 ： 最小未知係数個数

暗号名	1 段数目	2 段数目	3 段数目	4 段数目	5 段数目
Camellia	1	1	1	255	256
CIPHERUNICORN-A	1	1	256	256	256
Hierocrypt-3	1	1	256	256	256
SC2000	1	1	33	256	256
RC6	1	1	<256	256	256
MARS	1	1	1	1	256
Misty	1	1	256	256	256
Hierocrypt-L1	1	1	256	256	256
CIPHERUNICORN-E	1	1	256	256	256
FEAL-NX	1	1	<256	256	256

*Hierocrypt は S-box 層数を1段とする。
*SC2000 は B 関数と R 関数をそれぞれ1段とする。
*MARS はコア部のみの段数で評価
*Misty は FL 関数を除く。
*FEAL-NX はゲートブランチを除く
*<256 は、256 未満であることを表す。FEAL-NX と RC-6 に関しては、258 個のランダムマスター鍵のもとでは最小未知係数個数の収束性が悪く、正確な数値を決定できていない。