ストリーム暗号の評価
長周期連性テスト
MULTI-S01 編

平成 13 年 1 月 21 日

1　取得条件

FIPS 140 の乱数性評価テストと同様に 20000 bits をサンプリングして，そのデータに含まれる gaps (0 が連続して並ぶ)，および blocks(1 が連続して並ぶ) の長さを調べる．調査対処がストリーム暗号であるため，平文 C と暗号文 M との排他的論理和 $C \oplus M$ の長周期連性テストを行った．FIPS 140 検査に合格する条件は長さ 34 以上のものが存在しないことである．

鍵は，別冊「MULTI-S01 暗号評価に使用したデータについて」に記載した組み合わせ (秘密鍵 C を 400 通り，乱数列番号 D を 25 通り，冗長度 R を 10 通り，合計 100,000 通り) に対し，同別冊に記載したデータに対する暗号化を行い，評価を行った．

つまり，このテストでは 20000 bits のデータを $100,000 \times 1000$ 件生成し，長周期連性テストを行ったことになる．

2　テスト結果

まず度数分布を示す．

適切な分布のように見えるが，サンプリングしたデータから長さが 34 以上のものが 6 種類存在した．次章を参照のこと．

3　評価

FIPS 140 の条件をクリアできないものが発生した．従って (平文 $\oplus$ 暗号文を乱数と見なした場合)，長周期連性テストに関しては，FIPS 140 検査を合格しない．

なお，付録に示した異常が発生したパターンでは，鍵，冗長性，平文に相関はみられない．

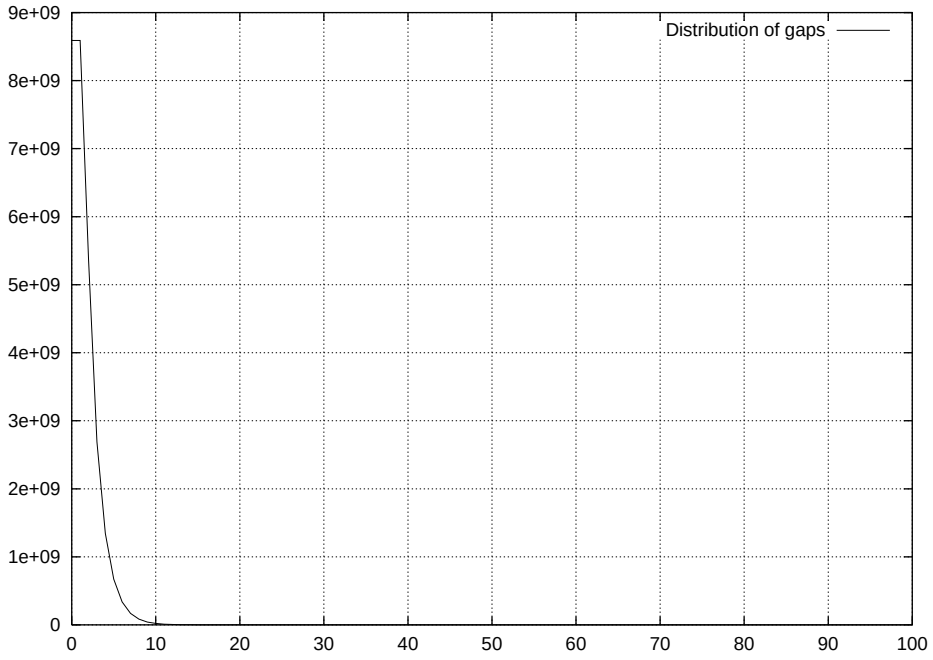

図 1: gaps の度数分布

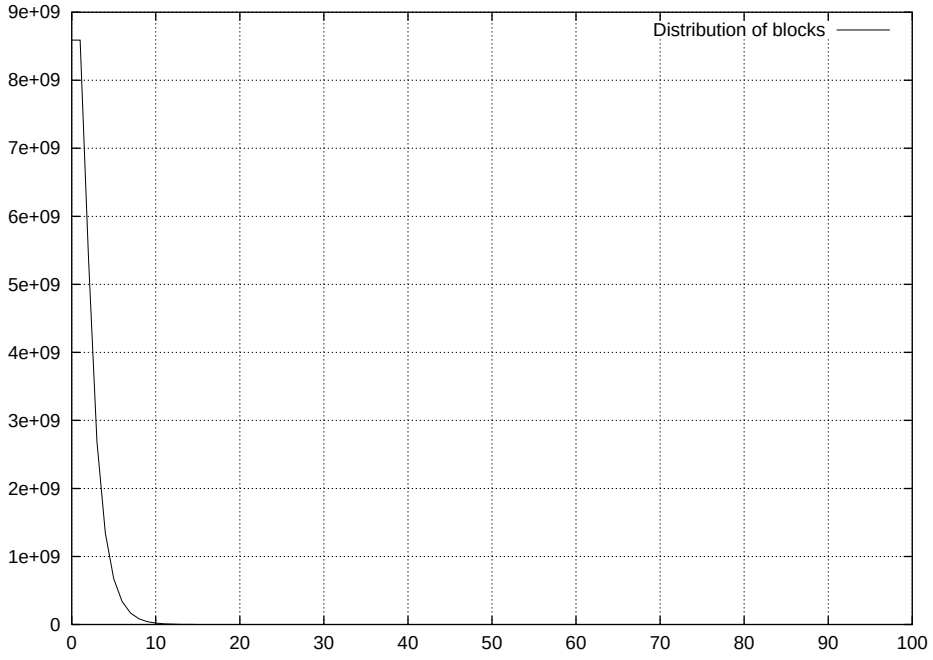

図 2: blocks の度数分布

異常が発生した鍵と平文

フォーマットは次の通り

1. # コメント
2. 長さ， gaps の数，blocks の数

パターン 1

```
#  ca343da001ra001pm021
01, 2548, 2497
02, 1244, 1288
03, 647, 667
04, 299, 296
05, 142, 145
06, 81, 72
07, 31, 34
08, 16, 14
09, 15, 14
10, 5, 4
11, 4, 2
12, 1, 0
13, 0, 1
14, 1, 0
15, 1, 1
16, 0, 0
17, 0, 0
18, 0, 0
19, 0, 0
20, 0, 0
21, 0, 0
22, 0, 0
23, 0, 0
24, 0, 0
25, 0, 0
26, 0, 0
27, 0, 0
28, 0, 0
29, 0, 0
30, 0, 0
31, 0, 0
32, 0, 0
33, 0, 0
34, 0, 0
35, 0, 1
```

パターン 2

```
#  cm098da008ra001pm0c4
01, 2491, 2495
02, 1232, 1272
03, 647, 633
04, 295, 293
05, 167, 150
06, 83, 77
07, 43, 37
08, 16, 22
09, 11, 9
10, 5, 3
11, 2, 2
12, 0, 0
13, 2, 1
14, 1, 1
15, 0, 0
16, 0, 0
17, 0, 0
18, 0, 0
19, 0, 0
20, 0, 0
21, 0, 0
22, 0, 0
23, 0, 0
24, 0, 0
25, 0, 0
26, 0, 0
27, 0, 0
28, 0, 0
29, 0, 0
30, 0, 0
31, 0, 0
32, 0, 0
33, 0, 0
34, 0, 1
```

パターン 3

```
#  ca338da010ra001pm0a0
```

01, 2527, 2492
02, 1232, 1250
03, 607, 607
04, 307, 356
05, 169, 143
06, 82, 83
07, 39, 33
08, 24, 17
09, 9, 13
10, 4, 2
11, 0, 1
12, 0, 3
13, 0, 0
14, 0, 0
15, 0, 0
16, 0, 0
17, 0, 0
18, 0, 0
19, 0, 0
20, 0, 0
21, 0, 0
22, 0, 0
23, 0, 0
24, 0, 0
25, 0, 0
26, 0, 0
27, 0, 0
28, 0, 0
29, 0, 0
30, 0, 0
31, 0, 0
32, 0, 0
33, 0, 0
34, 0, 0
35, 0, 0
36, 0, 1

04, 307, 270
05, 154, 147
06, 89, 85
07, 41, 43
08, 16, 17
09, 7, 17
10, 5, 3
11, 1, 1
12, 0, 3
13, 0, 0
14, 1, 0
15, 1, 0
16, 0, 0
17, 0, 0
18, 0, 0
19, 0, 0
20, 0, 0
21, 0, 0
22, 0, 0
23, 0, 0
24, 0, 0
25, 0, 0
26, 0, 0
27, 0, 0
28, 0, 0
29, 0, 0
30, 0, 0
31, 0, 0
32, 0, 0
33, 0, 0
34, 0, 0
35, 0, 0
36, 0, 0
37, 0, 0
38, 0, 0
39, 0, 1

パターン 4

cm044da010ra001pm043
01, 2488, 2453
02, 1270, 1298
03, 611, 653

パターン 5

ca315da014ra001pi808
01, 2558, 2562
02, 1207, 1231
03, 614, 616

```
04, 341, 297
05, 162, 184
06, 64, 65
07, 36, 42
08, 19, 13
09, 11, 10
10, 6, 4
11, 4, 1
12, 2, 1
13, 1, 1
14, 0, 0
15, 0, 0
16, 1, 0
17, 0, 0
18, 0, 0
19, 0, 0
20, 0, 0
21, 0, 0
22, 0, 0
23, 0, 0
24, 0, 0
25, 0, 0
26, 0, 0
27, 0, 0
28, 0, 0
29, 0, 0
30, 0, 0
31, 0, 0
32, 0, 0
33, 0, 0
34, 1, 0
```

```
09, 5, 8
10, 2, 4
11, 3, 3
12, 1, 2
13, 1, 0
14, 1, 0
15, 0, 0
16, 0, 0
17, 0, 0
18, 0, 0
19, 0, 0
20, 0, 0
21, 0, 0
22, 0, 0
23, 0, 0
24, 0, 0
25, 0, 0
26, 0, 0
27, 0, 0
28, 0, 0
29, 0, 0
30, 0, 0
31, 0, 0
32, 0, 0
33, 0, 0
34, 0, 1
```

パターン 6

```
#  cm08bda023ra001pm0e3
01, 2491, 2461
02, 1258, 1279
03, 621, 626
04, 304, 290
05, 154, 160
06, 83, 83
07, 42, 47
08, 20, 21
```