ストリーム暗号の評価
一様性テスト
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，そのデータの出力分布を調べる．実際には，出力を 4 ビットずつに区切り，その出力結果が 0x 00 から 0x 0f の値を均等に取るかどうかを調べる．このため，次の値の分布を調べる．

$$X_3 = \frac{2^m}{k}(\sum_{i=1}^{2^m} n_i^2) - k \tag{1}$$

なお，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 一様性テストを行った．FIPS 140 検査を合格するためには， $1.03 < X_3 < 57.4$ であることが必要である．

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，一様性テストを行ったことになる．

2 テスト結果の一部

X_3 の度数分布を示す.

度数分布をみる限り，理想的な分布と思われる．しかし，全件チェックしてみると，FIPS 140 の条件に合格しないデータが 4 件存在した.

3 評価

FIPS 140 の条件に合格しないデータが 4 件存在した．従って (平文 $\oplus$ 暗号文を乱数と見なした場合)，一様性テストに関しては，FIPS 140 で示されている基準に達していない.

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.

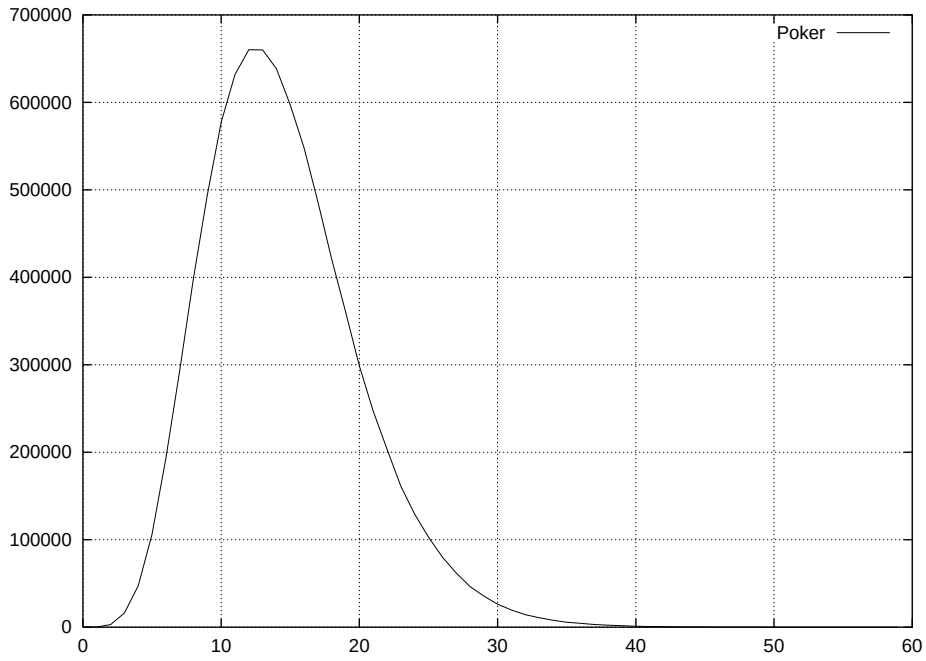
Poker
700000
600000
500000
400000
300000
200000
100000
0
0
10
20
30
40
50
60

図 1: X_3 の度数分布

異常が発生した鍵と平文の組み合わせ

フォーマットは下記の通り

1. # コメント
2. ビットパターン， 発生数
3. 繰り返し
4. X_3 の値

なお，ビットパターンは 16 進数ではなく，10 進数で記載してある．

パターン 1

```
#  ca334da005ra001pm059
0, 1250
1, 1257
2, 1255
3, 1254
4, 1239
5, 1230
6, 1260
7, 1249
8, 1261
9, 1256
10, 1254
11, 1250
12, 1255
13, 1240
14, 1254
15, 1268
X_3=1.027157
```

パターン 2

```
#  cm03eda006ra001pm07b
0, 1256
1, 1216
2, 1282
3, 1220
4, 1209
5, 1347
6, 1182
7, 1374
8, 1164
9, 1188
10, 1192
11, 1213
12, 1401
13, 1268
14, 1266
15, 1254
X_3=58.715655
```

パターン 3

```
#  ca284da009ra001pi203
0, 1298
1, 1357
2, 1229
3, 1311
4, 1210
5, 1225
6, 1298
7, 1326
8, 1260
9, 1166
10, 1299
11, 1156
12, 1203
13, 1104
14, 1323
15, 1267
X_3=60.456869
```

パターン 4

```
#  ca267da017ra001pm008
0, 1211
1, 1370
2, 1171
3, 1327
4, 1253
5, 1345
6, 1314
7, 1144
8, 1168
9, 1360
10, 1221
```

```
11, 1249
12, 1215
13, 1232
14, 1213
15, 1239
X_3=59.982428
```