ストリーム暗号の評価
0/1 等頻度性テスト
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 bits の ON/OFF の頻度を調べる．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 0/1 等頻度性テストを行った．FIPS 140 の検査をクリアするためには，ON (=1) bit の総数 n_1 が $9654 < n_1 < 10346$ でなくてはならない．乱数列の最初の 20000 bits だけではなく，次の 20000 bits(20001-40000)，同様に (40001-60000, 60001-80000) と，20000bits 毎に区切り，各区間を対象に 0/1 等頻度性テストを行った．

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 $100,000 \times 1000 \times 4$ 件生成し，0/1 等頻度性テストを行ったことになる．

2 テスト結果の一部

テスト結果の一部を示す．左から順に bits 数，0 ビットの数，1 ビットの数である．

```
20000, 9949, 10051
40000, 20080, 19920
60000, 30073, 29927
80000, 40016, 39984
20000, 10063, 9937
40000, 20059, 19941
60000, 30039, 29961
80000, 39945, 40055
20000, 9943, 10057
40000, 19920, 20080
60000, 29911, 30089
80000, 39904, 40096
20000, 10051, 9949
40000, 20019, 19981
```

```
60000, 30012, 29988
80000, 40077, 39923
```

各区間で 0/1 は等頻度に発生するように見える．次に，度数分布を示す．

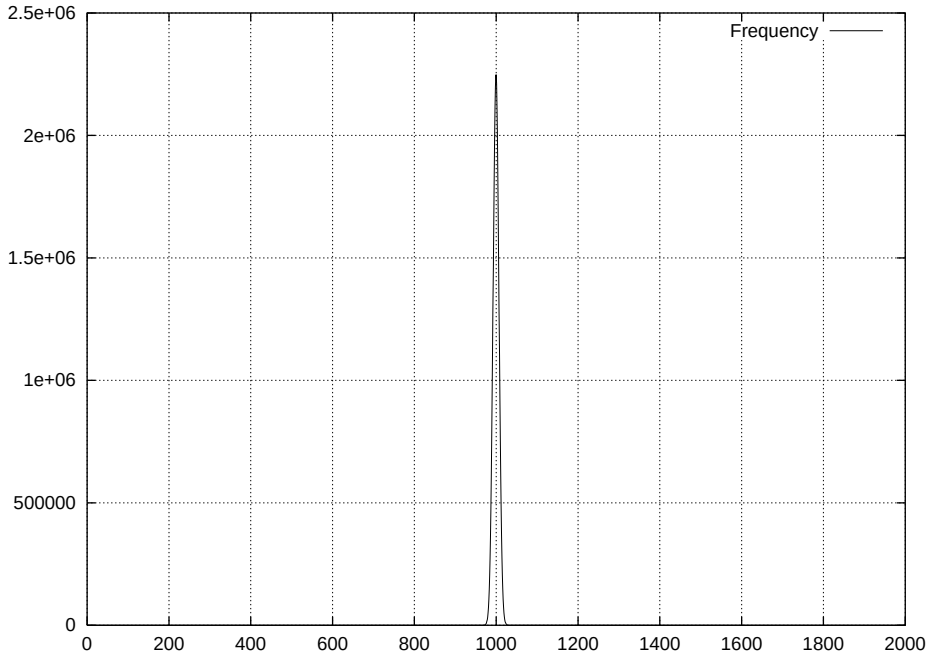

図 1: 0 の出現頻度の度数分布

度数分布をみる限り，理想的な二項分布に従うようであるが，FIPS140 の基準を満たさないものもいくつか存在する．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．異常値 (20000 bits 中の 0 の数，異常が発生した鍵と平文との組み合わせそして，20000 bits ごとの 0/1 出現頻度を示す (後述)．

従って (平文 $\oplus$ 暗号文を乱数と見なした場合)，0/1 等頻度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，次のものに相関を見ることができる．

平文 1 ビット違い 秘密鍵，乱数列番号，冗長度が cm018, da010, ra001 のものについては，異常が 20 件発生する．平文は pr381 から pr400 であり，先頭 2 バイト以外は同じである． MULTI-S01 暗号では，先頭以外が同じ平文を，同一鍵 (秘密鍵，乱数列番号，冗長度) で暗号化すると，最初以外は全く同じ暗号文 が生成される．cm018, da010, ra001, pr281 の組の 0/1 等頻度に偏りがあったため不合格が多発したと思われる．

さて，同一鍵 (秘密鍵，乱数列番号，冗長度) で暗号化を行うことはないので，異常が発生した件数は，13 件と見なすことができる．この 13 個のパターンでは，鍵，冗長性，平文に相関はみられない．

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. 異常値
2. # コメント
3. 先頭からのビット数, 0 のビット数, 1 のビット数

(繰り返し)

```
09643
#  cm02fda001ra001pm032
20000, 10104, 9896
40000, 20150, 19850
60000, 30077, 29923
80000, 39720, 40280

09653
#  cm068da001ra001pm001
20000, 9907, 10093
40000, 19891, 20109
60000, 29970, 30030
80000, 39623, 40377

10387
#  ca274da003ra001pm01f
20000, 10387, 9613
40000, 20478, 19522
60000, 30438, 29562
80000, 40406, 39594

09645
#  ca303da006ra001pm041
20000, 9645, 10355
40000, 19591, 20409
60000, 29414, 30586
80000, 39488, 40512

09624
(以下の 19 個のデータは，いずれも
 0 の数が 9624 個存在する区間がある)
#  cm018da010ra001pr381
20000, 9935, 10065
40000, 19956, 20044
60000, 29580, 30420
80000, 39625, 40375

#  cm018da010ra001pr382
20000, 9925, 10075
40000, 19946, 20054
60000, 29570, 30430
80000, 39615, 40385

#  cm018da010ra001pr383
20000, 9936, 10064
40000, 19957, 20043
60000, 29581, 30419
80000, 39626, 40374

#  cm018da010ra001pr384
20000, 9930, 10070
40000, 19951, 20049
60000, 29575, 30425
80000, 39620, 40380

#  cm018da010ra001pr385
20000, 9938, 10062
40000, 19959, 20041
60000, 29583, 30417
80000, 39628, 40372

#  cm018da010ra001pr386
20000, 9935, 10065
40000, 19956, 20044
60000, 29580, 30420
80000, 39625, 40375

#  cm018da010ra001pr387
20000, 9935, 10065
40000, 19956, 20044
60000, 29580, 30420
80000, 39625, 40375

#  cm018da010ra001pr388
20000, 9923, 10077
40000, 19944, 20056
60000, 29568, 30432
80000, 39613, 40387

#  cm018da010ra001pr389
20000, 9932, 10068
```

```
40000, 19953, 20047
60000, 29577, 30423
80000, 39622, 40378

#  cm018da010ra001pr390
20000, 9929, 10071
40000, 19950, 20050
60000, 29574, 30426
80000, 39619, 40381

#  cm018da010ra001pr391
20000, 9935, 10065
40000, 19956, 20044
60000, 29580, 30420
80000, 39625, 40375

#  cm018da010ra001pr392
20000, 9931, 10069
40000, 19952, 20048
60000, 29576, 30424
80000, 39621, 40379

#  cm018da010ra001pr393
20000, 9926, 10074
40000, 19947, 20053
60000, 29571, 30429
80000, 39616, 40384

#  cm018da010ra001pr394
20000, 9931, 10069
40000, 19952, 20048
60000, 29576, 30424
80000, 39621, 40379

#  cm018da010ra001pr395
20000, 9937, 10063
40000, 19958, 20042
60000, 29582, 30418
80000, 39627, 40373

#  cm018da010ra001pr396
20000, 9929, 10071
40000, 19950, 20050
60000, 29574, 30426
80000, 39619, 40381

#  cm018da010ra001pr397
20000, 9934, 10066
40000, 19955, 20045
60000, 29579, 30421
80000, 39624, 40376

#  cm018da010ra001pr398
20000, 9930, 10070
40000, 19951, 20049
60000, 29575, 30425
80000, 39620, 40380

#  cm018da010ra001pr399
20000, 9933, 10067
40000, 19954, 20046
60000, 29578, 30422
80000, 39623, 40377

#  cm018da010ra001pr400
20000, 9938, 10062
40000, 19959, 20041
60000, 29583, 30417
80000, 39628, 40372
```

ここまでは 0 の数が 9624 個の区間が存在する.

```
10361
#  cm097da013ra001pm03f
20000, 10361, 9639
40000, 20237, 19763
60000, 30341, 29659
80000, 40261, 39739

09641
#  cm04fda016ra001pm051
20000, 10009, 9991
40000, 19650, 20350
60000, 29575, 30425
80000, 39540, 40460

09651
```

```
#  cm0d5da017ra001pm0fe
20000, 9651, 10349
40000, 19699, 20301
60000, 29694, 30306
80000, 39730, 40270

10352
#  cm049da019ra001pm0c7
20000, 9949, 10051
40000, 20301, 19699
60000, 30433, 29567
80000, 40421, 39579

10362
#  cm0e9da020ra001pm00c
20000, 10362, 9638
40000, 20342, 19658
60000, 30289, 29711
80000, 40191, 39809

09651
#  cm076da021ra001pm0fb
20000, 9989, 10011
40000, 19640, 20360
60000, 29594, 30406
80000, 39545, 40455

10380
#  cm095da022ra001p-avi.ab
20000, 9954, 10046
40000, 19979, 20021
60000, 29977, 30023
80000, 40357, 39643

10362
#  cm096da024ra001pm0bc
20000, 10086, 9914
40000, 20072, 19928
60000, 29986, 30014
80000, 40348, 39652
```