擬似乱数生成の評価
0/1 等頻度性テスト
PANAMA(MULTI-S01) 編

平成 13 年 1 月 18 日

1 取得条件

FIPS 140 と同様に 20000 bits をサンプリングして，その中での bits の ON/OFF の頻度を調べる．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) の 4 つの区間を対象に 0/1 性テストを行う．

鍵は，別冊「PANAMA の評価に利用した鍵の種類」にある組み合わせ (秘密鍵を 999 通り，乱数列番号を 100 通り) を対象とし，80000 bits のデータを 99900 件出力した．

つまり，このテストではデータ一つにつき 4 件の評価を行っているので，計 約 40 万件の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, 9927, 10073
40000, 19831, 20169
60000, 29937, 30063
80000, 39857, 40143
20000, 9995, 10005
40000, 20076, 19924
60000, 30060, 29940
80000, 40046, 39954
20000, 9810, 10190
40000, 19913, 20087
60000, 29862, 30138
80000, 39891, 40109
20000, 9992, 10008
40000, 19934, 20066
60000, 29825, 30175
80000, 39728, 40272
```

0/1 の出現頻度分布平均しているように見える．次に度数分布を示す．

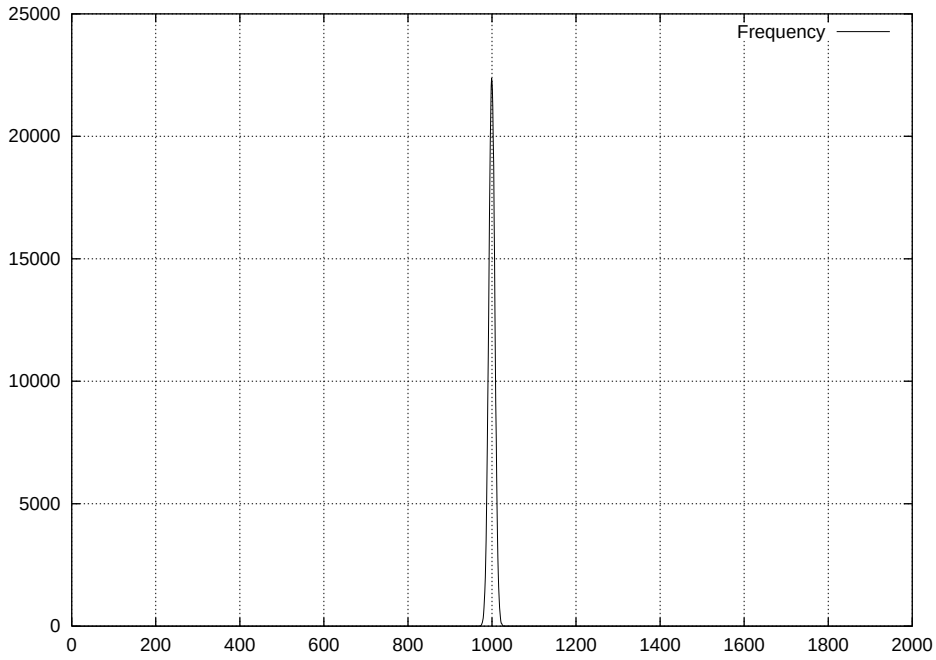

図 1: 0 の出現頻度の度数分布

3 評価

約 40 万件の検査の結果， FIPS 140 の条件をクリアしないものが 1 件あった．下記の 40001 から 60000 ビットまでの 20000 ビット中に 0 の数が 10365 存在する．

```
#  da083ca882.pnm
20000, 10000, 10000
40000, 20046, 19954
60000, 30411, 29589
80000, 40411, 39589
```

0/1 等頻度性テストに関しては，擬似乱数の条件を満たさないと判断する．