擬似乱数生成の評価
0/1 等頻度性テスト
TOYOCRYPT-HR1 編

平成 13 年 1 月 12 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「TOYOCRYPT シリーズの評価に利用した鍵の種類」にある組み合わせ (固定鍵 C を 100 通り，ストリーム鍵 S を 1000 通り) を対象とし，80000 bits のデータを 100000 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 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, 9874, 10126
40000, 19913, 20087
60000, 30017, 29983
80000, 39963, 40037
20000, 10129, 9871
40000, 20163, 19837
60000, 30205, 29795
80000, 40203, 39797
20000, 10014, 9986
40000, 20082, 19918
60000, 30000, 30000
80000, 40110, 39890
20000, 9898, 10102
40000, 19956, 20044
60000, 29934, 30066
80000, 39958, 40042
```

```
20000, 10016, 9984
40000, 20056, 19944
60000, 30030, 29970
80000, 40011, 39989
```

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．

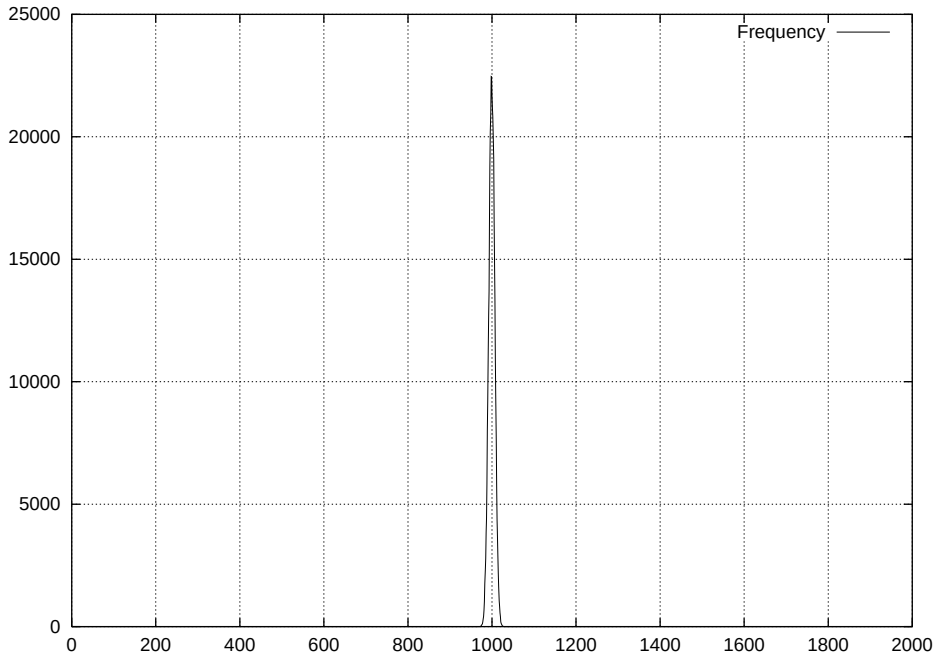

図 1: 0 の出現頻度の度数分布

3 評価

40 万件全ての検査結果は FIPS 140 の条件をクリアした．0/1 等頻度性テストに関しては，擬似乱数の条件を満たすと判断する．