擬似乱数生成の評価
一様性テスト
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，そのデータを 4 bits ずつ分割する．出力系列が真の乱数と区別できないなら，その値 (0x00 から 0x0f) までは等頻度に発生するはずである．実際には常に等頻度ではない．従って次の値の分布を調べる．

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

FIPS 140 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「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，各々の出力の先頭 20000bits を対象に評価を行った．

つまり，このテストでは計 10 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．

```
X_3=15.296000
X_3=15.648000
X_3=18.609600
X_3=19.112000
X_3=11.875200
X_3=19.064000
X_3=10.187200
X_3=10.440000
X_3=12.702400
X_3=14.460800
X_3=12.963200
X_3=10.083200
X_3=15.211200
X_3=7.140800
X_3=15.180800
```

```
X_3=12.584000
X_3=22.025600
X_3=27.667200
X_3=21.968000
X_3=10.686400
X_3=10.142400
X_3=19.432000
X_3=20.609600
X_3=4.660800
X_3=5.872000
X_3=15.750400
X_3=10.417600
X_3=16.483200
X_3=10.024000
X_3=12.305600
X_3=11.952000
X_3=10.996800
```

次に X_3 の分布を図示する．

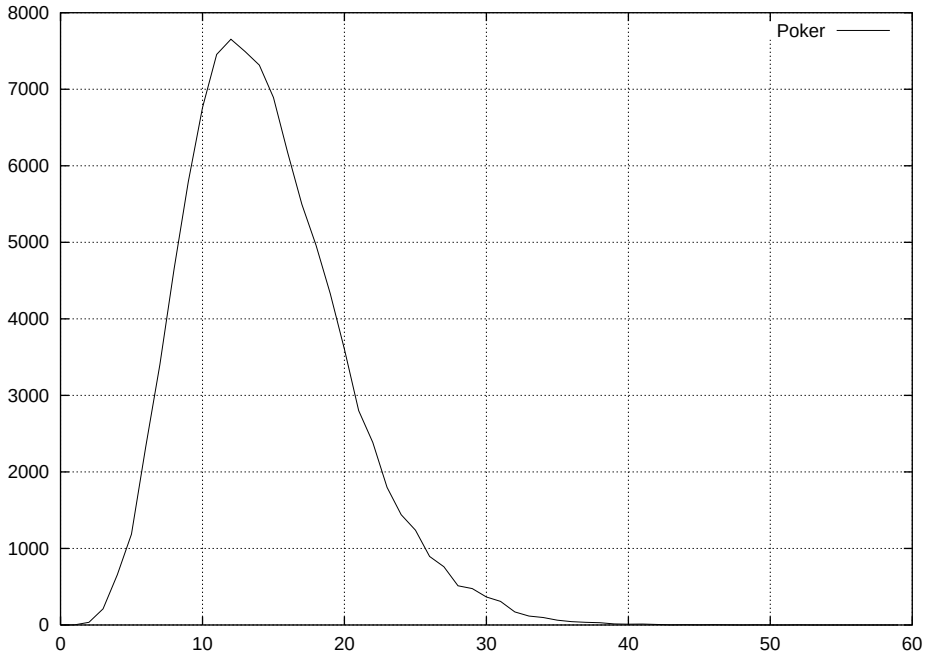

図 1: X_3 の分布

3 評価

10 万件全ての検査結果は FIPS 140 の条件をクリアした．一様性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．