擬似乱数生成の評価
一様性テスト
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「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，各々の出力の先頭 20000bits を対象に評価を行った．

つまり，このテストでは計約 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=15.206400
X_3=10.379200
X_3=19.316800
X_3=9.572800
X_3=9.177600
X_3=21.060800
X_3=11.420800
X_3=10.729600
X_3=6.782400
X_3=30.688000
X_3=10.304000
X_3=20.219200
X_3=13.060800
X_3=5.188800
X_3=15.144000
```

```
X_3=17.809600
X_3=7.664000
```

次に X_3 の分布を図示する．

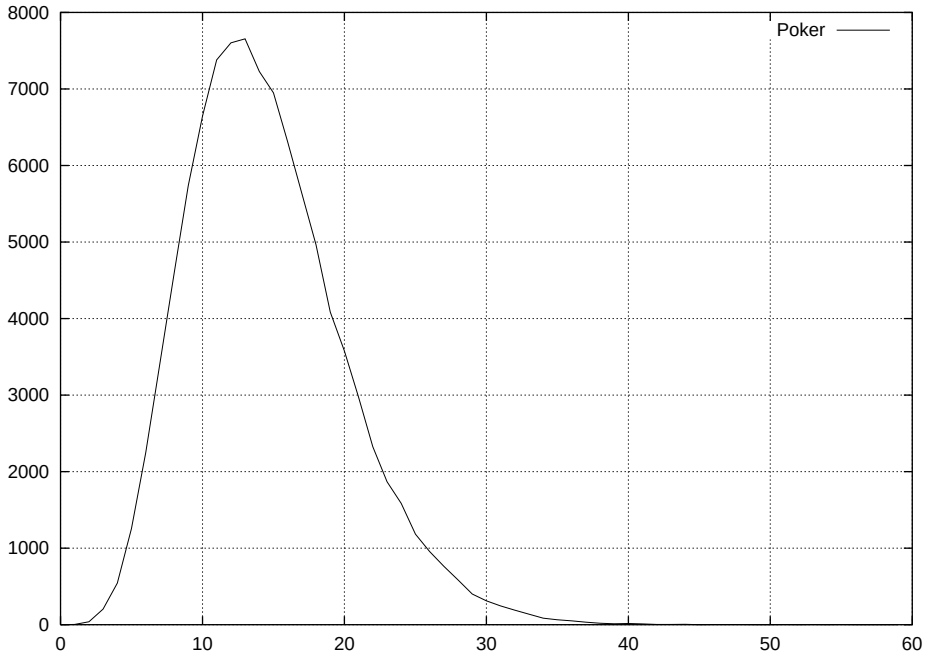

図 1: X_3 の分布

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．一様性テストに関しては，擬似乱数の条件を満たすと判断する．