擬似乱数生成の評価
線形複雑度テスト
TOYOCRYPT-HR1 編

平成 13 年 1 月 12 日

1 取得条件

出力データの先頭 1000 bits について，線形複雑度を実測した．

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．

線形複雑度は，観測ビットに対して傾きが $\frac{1}{2}$ であることが望ましい．そこで，次の値 (分散) を算出し，理想値との差を評価した．

$$\frac{1}{1000}\sum_{1}^{1000}(lc(i)-\frac{i}{2})^2 \tag{1}$$

2 テスト結果

テスト結果は付録に示す．分散の値が，0 に近いほど 理想に近い．すなわち，線形複雑度の拡大具合いを図示すると，傾きが $\frac{1}{2}$ の直線になることが望ましい．なお，線形複雑度は整数値であるため分散 0 になることはない．次に，線形複雑度の分散に関する分布を示す.

3 評価

分散が 10.0 以上となったものはつぎのものである．これらの鍵はいずれも長周期連性テストで問題となった鍵である．

固定鍵	ストリーム鍵
C4001 = 00000000 00000000 00000008 04008001	SB017 = 00000000 00000000 00000000 00040000
C4001 = 00000000 00000000 00000008 04008001	SB018 = 00000000 00000000 00000000 00080000
C4001 = 00000000 00000000 00000008 04008001	SB019 = 00000000 00000000 00000000 00100000

次に，分散値が 10.0 以上となった 3 種類の鍵について線形複雑度の上昇カーブを示す.

線形複雑度が傾き $\frac{1}{2}$ の直線と大きく異なる原因は，乱数列の初期の部分で 0 が連続して発生することにある (長周期連性テストを参照)．その部分を除けば線形複雑度の上昇具合いは理想的であるが，線形複雑度のテストに関しては合格しないと判断する．

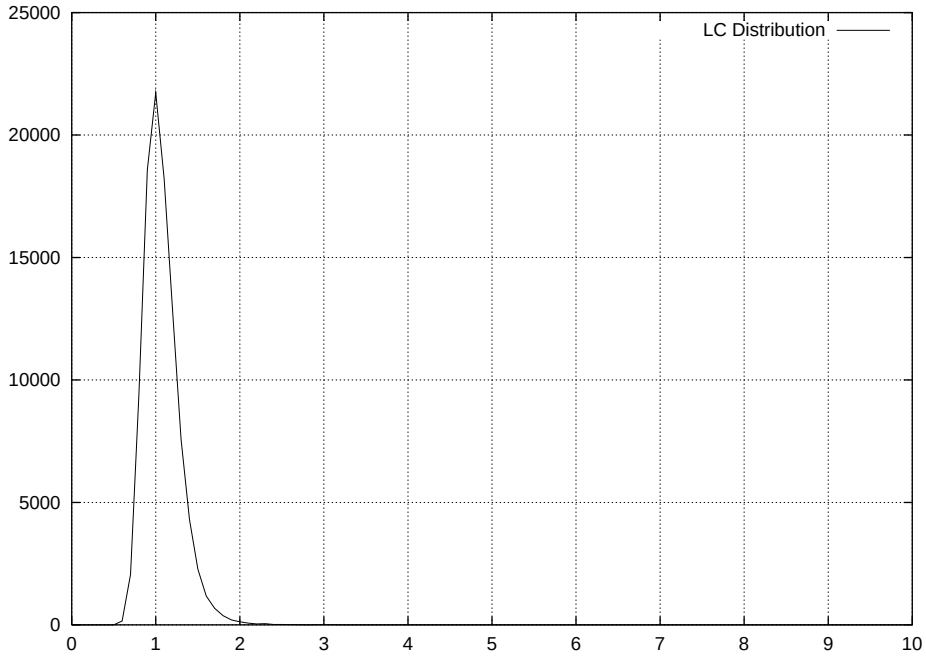

図 1: 線形複雑度の分散に関する分散の分布

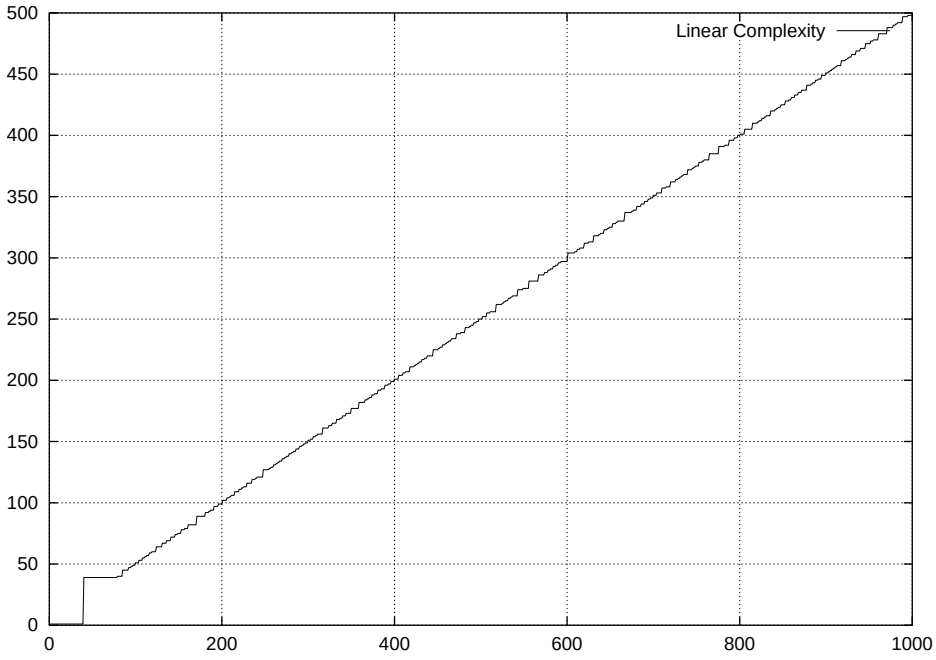

図 2: 固定鍵 c4001, ストリーム鍵 sb017 を利用した線形複雑度

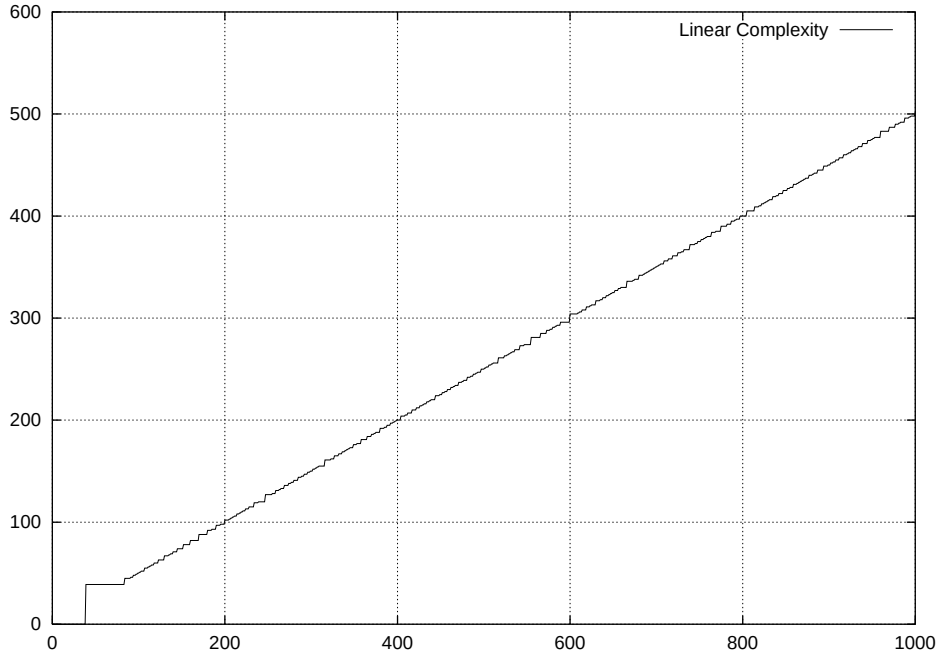

図 3: 固定鍵 c4001, ストリーム鍵 sb018 を利用した線形複雑度

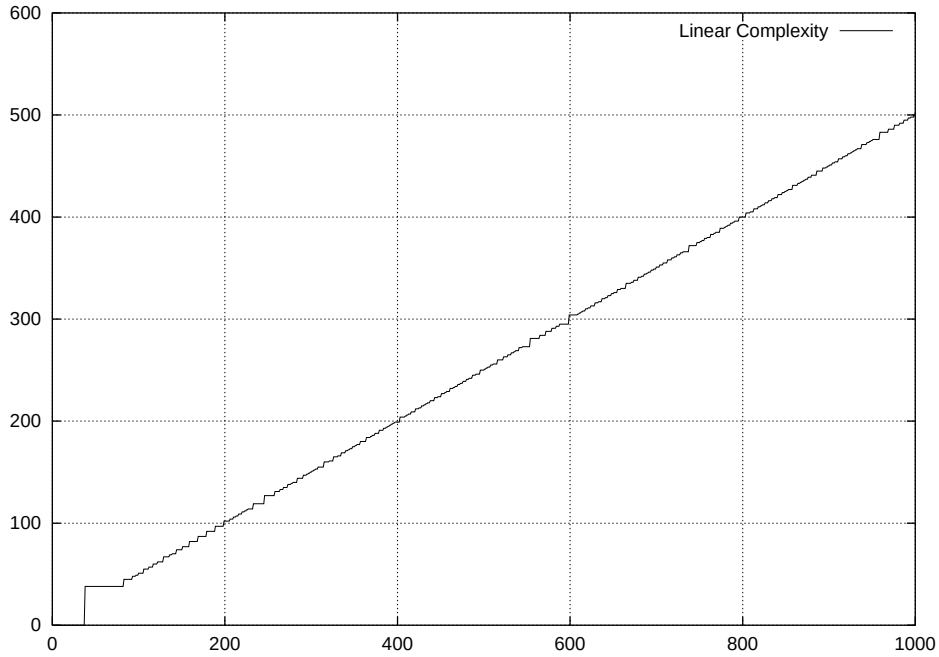

図 4: 固定鍵 c4001, ストリーム鍵 sb019 を利用した線形複雑度

線形複雑度の分散値

0.000000 0
0.100000 0
0.200000 0
0.300000 0
0.400000 0
0.500000 0
0.600000 158
0.700000 2060
0.800000 9423
0.900000 18577
1.000000 21730
1.100000 18221
1.200000 12865
1.300000 7576
1.400000 4308
1.500000 2274
1.600000 1178
1.700000 673
1.800000 373
1.900000 201
2.000000 126
2.100000 70
2.200000 36
2.300000 51
2.400000 19
2.500000 14
2.600000 9
2.700000 8
2.800000 0
2.900000 7
3.000000 4
3.100000 3
3.200000 1
3.300000 2
3.400000 1
3.500000 1
3.600000 1
3.700000 1
3.800000 1
3.900000 0
4.000000 1
4.100000 1
4.200000 1
4.300000 1
4.400000 1
4.500000 0
4.600000 1
4.700000 0
4.800000 1
4.900000 0
5.000000 1
5.100000 1
5.200000 0
5.300000 0
5.400000 0
5.500000 1
5.600000 1
5.700000 0
5.800000 0
5.900000 0
6.000000 2
6.100000 0
6.200000 0
6.300000 0
6.400000 0
6.500000 2
6.600000 0
6.700000 0
6.800000 0
6.900000 0
7.000000 1
7.100000 1
7.200000 0
7.300000 0
7.400000 0
7.500000 1
7.600000 0
7.700000 1
7.800000 0
7.900000 0
8.000000 0
8.100000 1
8.200000 1
8.300000 0
8.400000 0
8.500000 0

```
8.600000 0
8.700000 2
8.800000 0
8.900000 0
9.000000 0
9.100000 0
9.200000 0
9.300000 0
9.400000 2
9.500000 0
9.600000 0
9.700000 0
9.800000 0
9.900000 0
```