

擬似乱数生成の評価 線形複雑度テスト PANAMA(MULTI-S01) 編

平成 13 年 1 月 18 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「PANANA 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。

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。

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

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

分散は最大で 3.9 であり、秘密鍵 ca971、乱数列番号 da057 のときに発生した。その際の線形複雑度の上昇具合をグラフで示す。

グラフから判断する限り、線形複雑度の上昇カーブは傾き $\frac{1}{2}$ である。本方式は線形複雑度のテストに合格したと判断する。

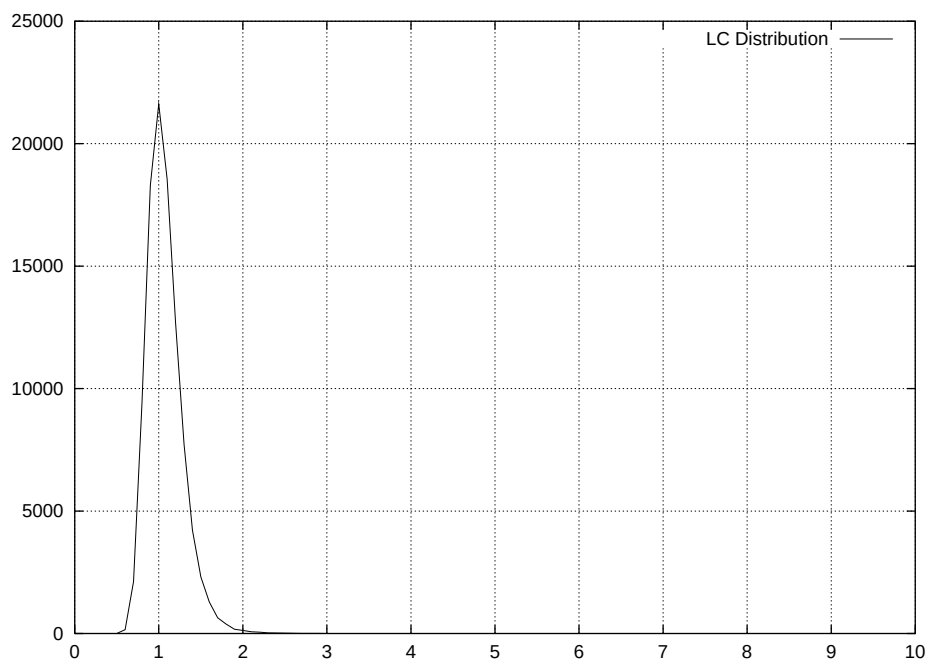


図 1: 線形複雑度の分散に関する分散の分布

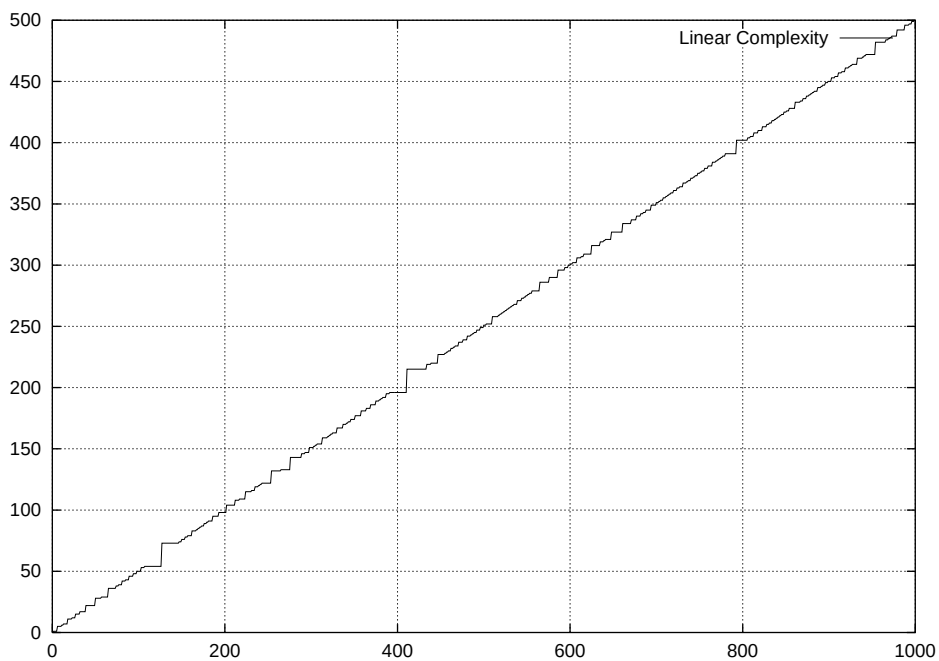


図 2: 分散最大時の線形複雑度上昇具合

線形複雑度の分散値

0.000000 0	4.200000 0
0.100000 0	4.300000 0
0.200000 0	4.400000 0
0.300000 0	4.500000 0
0.400000 0	4.600000 0
0.500000 1	4.700000 0
0.600000 160	4.800000 0
0.700000 2118	4.900000 0
0.800000 9361	5.000000 0
0.900000 18292	5.100000 0
1.000000 21622	5.200000 0
1.100000 18556	5.300000 0
1.200000 12712	5.400000 0
1.300000 7718	5.500000 0
1.400000 4212	5.600000 0
1.500000 2306	5.700000 0
1.600000 1288	5.800000 0
1.700000 645	5.900000 0
1.800000 388	6.000000 0
1.900000 174	6.100000 0
2.000000 123	6.200000 0
2.100000 71	6.300000 0
2.200000 54	6.400000 0
2.300000 25	6.500000 0
2.400000 24	6.600000 0
2.500000 18	6.700000 0
2.600000 11	6.800000 0
2.700000 5	6.900000 0
2.800000 5	7.000000 0
2.900000 3	7.100000 0
3.000000 1	7.200000 0
3.100000 1	7.300000 0
3.200000 1	7.400000 0
3.300000 0	7.500000 0
3.400000 1	7.600000 0
3.500000 2	7.700000 0
3.600000 0	7.800000 0
3.700000 1	7.900000 0
3.800000 0	8.000000 0
3.900000 1	8.100000 0
4.000000 0	8.200000 0
4.100000 0	8.300000 0
	8.400000 0
	8.500000 0

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