ストリーム暗号の評価
線形複雑度テスト
MULTI-S01 編

平成 13 年 1 月 21 日

1　取得条件

平文データの先頭 1000 bits と，暗号文データの先頭 1000 bits との排他的論理和をとり，それを擬似乱数系列と見なし，線形複雑度を計測した．

鍵は，別冊「MULTI-S01 暗号評価に使用したデータについて」に記載した組み合わせのうち，下記のものに絞って計測した．全鍵について計測できなかったのは，コンピュータ資源の制限のためである．

秘密鍵 C を 21 通り (ca[300-309], cm[001-005], 0fb-0ff,100]), 乱数列番号 D を (da001,02,03,06,07,08,10,11,14,15)10 通り，冗長度 R を 1 通り，合計 210 通りに対し，同別冊に記載したデータからランダムに抽出した 204 個のデータに対する暗号化を行い，評価を行った．

つまり，このテストでは 1000 bits のデータを $19 \times 10 \times 204$ 件生成し，線形複雑度を計測したことになる．

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

まず，ランダムに選択したサンプルにおける線形複雑度の上昇具合いをを示す．

次に，線形複雑度の分散値に関する度数分布を図示する．また，付録「線形複雑度の分散に関する分布」に線形複雑度の分散値の分布表を示す．

なお，分散の値が，0 に近いほど 理想に近い．なお，線形複雑度は整数値であるため，分散は 0 にはならない．

3　評価

線形複雑度の観点からは問題はないと考える．

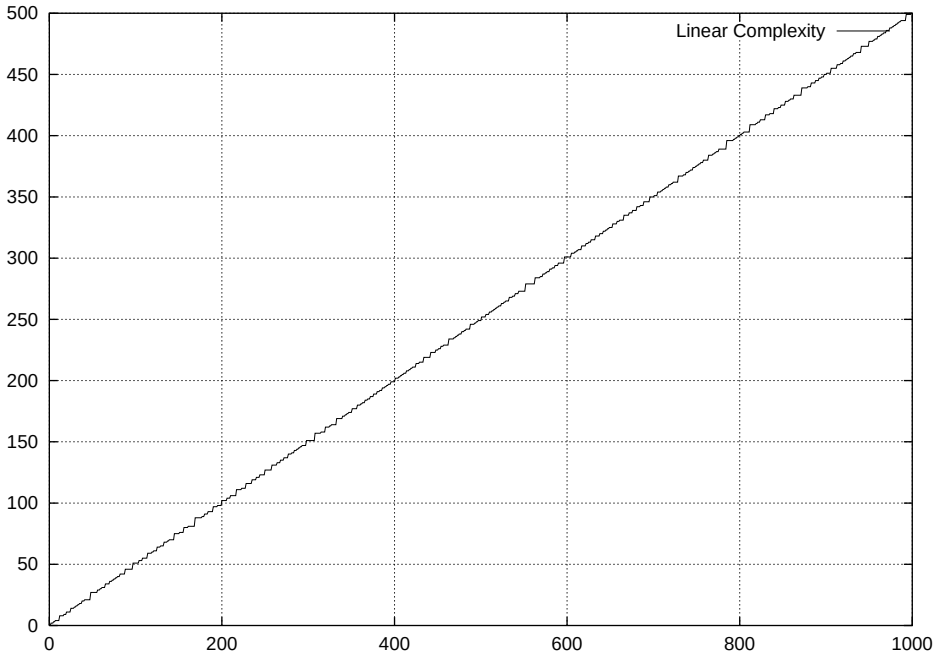

図 1: 上昇具合い

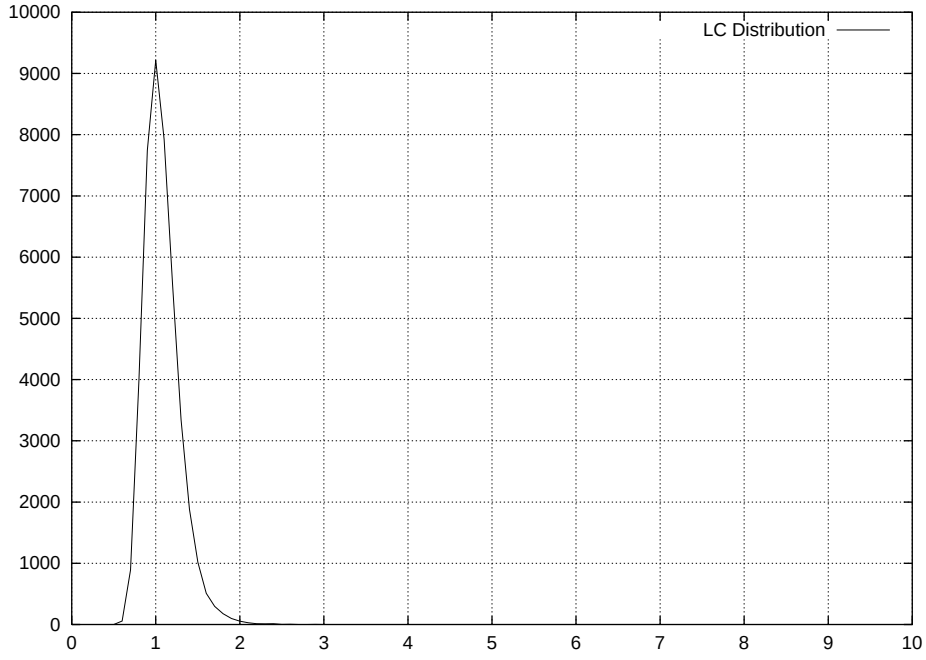

図 2: 線形複雑度の分散値

線形複雑度の分散に関する分布

分散値は 1.0 をピークとなる．フォーマットは次の通り．

1. 分散値，度数

(繰り返し)

```
0.000000 0
0.100000 0
0.200000 0
0.300000 0
0.400000 0
0.500000 0
0.600000 57
0.700000 890
0.800000 3990
0.900000 7744
1.000000 9215
1.100000 7922
1.200000 5564
1.300000 3345
1.400000 1881
1.500000 1018
1.600000 510
1.700000 297
1.800000 177
1.900000 97
2.000000 54
2.100000 29
2.200000 14
2.300000 11
2.400000 13
2.500000 2
2.600000 4
2.700000 1
2.800000 0
2.900000 2
3.000000 0
3.100000 1
3.200000 1
3.300000 0
3.400000 0
3.500000 0
3.600000 1
3.700000 0
3.800000 0
3.900000 0
4.000000 0
4.100000 0
4.200000 0
4.300000 0
4.400000 0
4.500000 0
4.600000 0
4.700000 0
4.800000 0
4.900000 0
5.000000 0
```