ストリーム暗号評価
相互情報量テスト
MULTI-S01 編

平成 13 年 1 月 12 日

1　取得条件

暗号を設計する際，出力結果から入力に関する情報を得ることができないということが必用条件となる．そこで，平文と暗号文の相互情報量を評価することとした．テストの手順は下記の通り．

1. データを作成する．
   - 0/1 出現頻度に偏りのあるデータ
   - 00/01/10/11 出現頻度に偏りのあるデータ
   - 000/001/010/.../111 出現頻度に偏りのあるデータ
2. 上記の平文から暗号文を生成する
3. 単位ビットごとに相互情報量を計算する．

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の中で，出力に偏りを持たせた 32 個のデータ (pi2[01-10], pi4[01-10], pi8[01-12]) に対する暗号化を行い，評価を行った．暗号文から平文の情報が漏ないこと，すなわち，相互情報量が 0 に近いことがテストに合格する条件である．もちろん，相互情報量をビット単位の反転率以外の方法で評価することも可能であるが，本テストに合格することは，必用条件の一つである．

2　テスト結果

テスト結果を示す．相互情報量が大きかった値を以下に示す．

```
0.002399   (最大値)
0.002370
0.002285
0.002280
0.002189
0.002251
```

```
0.002207
0.002200
0.002187
0.002184
```

次に，相互情報量の分布を示す．

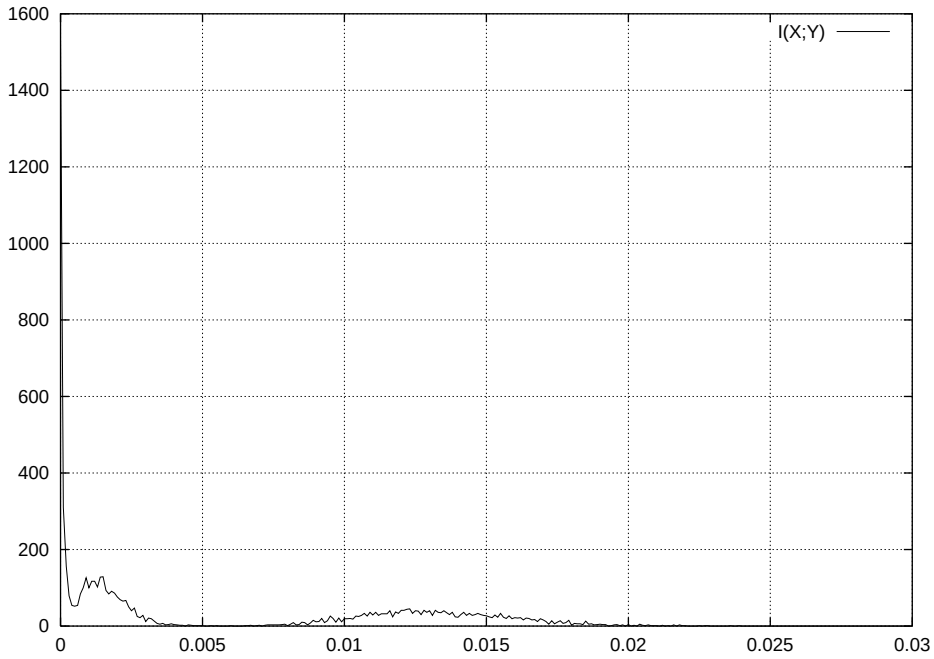

図 1: 相互情報量の分布

3 評価

グラフをみると，次の二つの範囲に偏りがある．

- 0.002-0.003
- 0.010-0.017

しかし，総じて相互情報量の値は小さい．提案方式は相互情報量の観点からの試験に合格したと判断する．