ストリーム暗号の評価
相互情報量テスト
TOYOCRYPT-HS1 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 (1-3 ビット) に相互情報量を計算する．

鍵は，別冊「TOYOCRYPT シリーズの評価に利用したデータについて」に記載した鍵 (固定鍵 C を 100 通り，ストリーム鍵 S を 1000 通り，組合わせは 10 万通り) からランダムに 3000 組を選び，評価した．

2 テスト結果

テスト結果の一部を示す．相互情報量が 0 に近いことが条件であるが，テストの結果，いずれの鍵を利用した場合にも，相互情報量は 0 に近かった．以下に，相互情報量の値が大きいもの順に 10 個列挙する．

```
0.002828
0.002708
0.002643
0.002627
0.002621
0.002572
0.002541
0.002540
0.002538
0.002517
```

3　評価

本項目の検査結果として，分布のグラフを以下に示す.

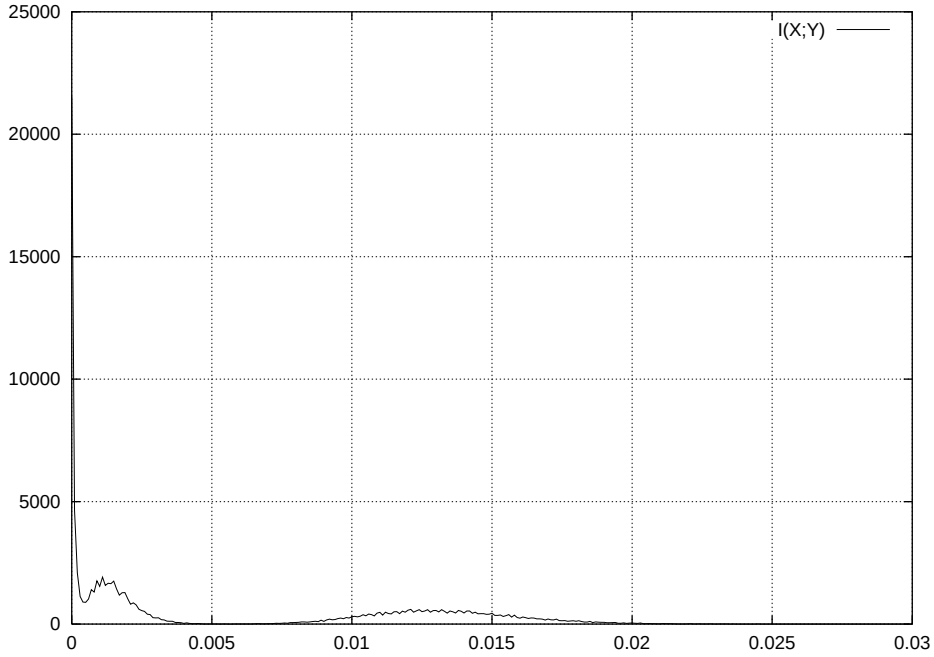

図 1: 相互情報量の分布

相互情報量の計算結果はいずれも 0 に近いので，提案方式は，本テストを合格したと判断する.