擬似乱数生成の評価
Avalanche 性テスト
TOYOCRYPT-HR1 編

平成 13 年 1 月 12 日

1 取得条件

固定鍵 C と，ストリーム鍵 S を微妙に (1 ビットずつ) 変更することにより出力される系列にどの程度の影響が発生するかを調べる．具体的には，ベースとなる鍵を設定し，乱数列を生成する．また，それと 1 ビット違いの鍵を生成し，同様に乱数列を生成する．

出力結果の排他的論理和をとり，その bits の分布を評価する．理想は，乱数長の半分程度のビットが異なっていること (0/1 等頻度性) である．

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) の中で，ビット違いのものをサンプリングする．なお，固定鍵を 1 bit 違いにとることは (既約多項式という条件などから) 実際に発生しないと考えうるので，固定鍵のビット違いのものに関する評価は行わない．

まず，ストリーム鍵は sa001-sa255 までの (sa001,sa002 の組から始まる)254 通りに対して，100 通りの固定鍵による出力の差分 (排他的論理) に対して，0/1 等頻度性を評価する．

次に，同様にストリーム鍵として (ca100..ca109), (ca110..ca119),... (ca480,ca489) の組は，1 ビット違いの鍵 (10 個) であるので，各々の組から 9 通りのストリーム鍵を生成し，100 通りの固定鍵による出力の差分 (排他的論理) に対して，0/1 等頻度性を評価する．

1 bit 違いのストリーム鍵が合計 644 個，その各々に対する固定鍵 100 種類に対する 0/1 等頻度性テストを行った．つまり， 6 万 4400 個のサンプルを生成したことになる．また，大きな乱数列に対する分布をみるため，各々 80000 bits のデータを取得した．

2 テスト結果

生成した二つのデータ (各々80000 bits のビット列
$a_i, b_i, (1 \leq i \leq 80000)$) に対して，次の計算を行った．

$$\sum_{1}^{80000} a_i \oplus b_i \tag{1}$$

付録にビット反転数の度数を示す．本章では度数分布を図示する．

次にビット反転数の度数分布をグラフにした.

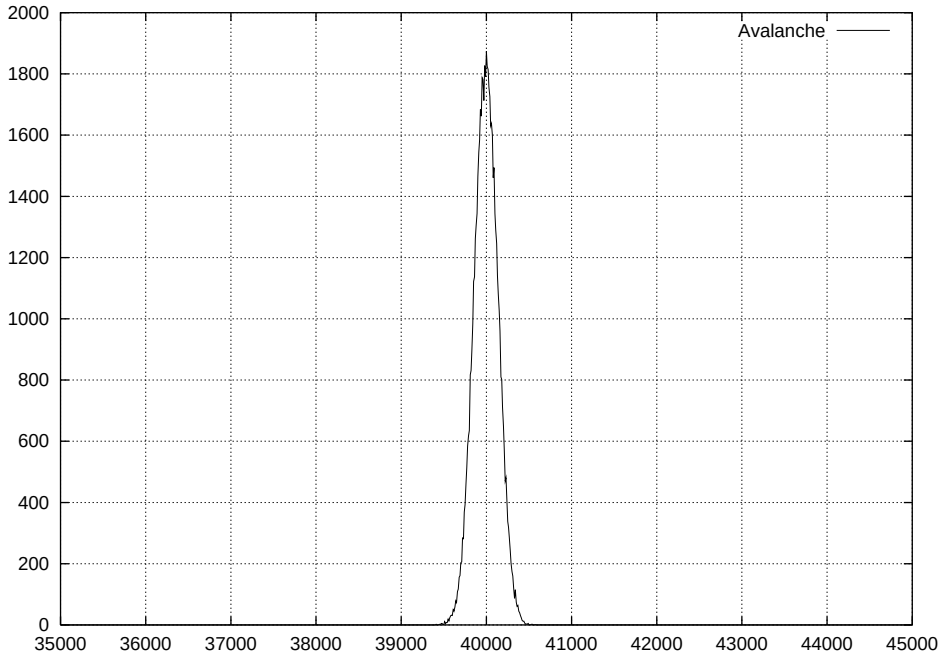

図 1: Avalanche テストによるビット反転数の度数分布

3 評価

ビット反転数の分布の評価の結果，Avalanche テストは合格したと判断する.

付録

ビット反転数の度数

ここまですべて 0

39400 00000
39410 00002
39420 00000
39430 00000
39440 00001
39450 00002
39460 00001
39470 00005
39480 00005
39490 00001
39500 00002
39510 00011
39520 00005
39530 00008
39540 00008
39550 00019
39560 00013
39570 00023
39580 00030
39590 00032
39600 00031
39610 00050
39620 00045
39630 00059
39640 00079
39650 00073
39660 00109
39670 00117
39680 00156
39690 00161
39700 00203
39710 00206
39720 00284
39730 00282
39740 00369
39750 00393
39760 00462
39770 00515
39780 00584
39790 00618
39800 00635
39810 00817
39820 00831
39830 00896
39840 00984
39850 01122
39860 01137
39870 01262
39880 01304
39890 01344
39900 01465
39910 01544
39920 01584
39930 01684
39940 01662
39950 01788
39960 01782
39970 01713
39980 01827
39990 01790
40000 01874
40010 01825
40020 01814
40030 01756
40040 01726
40050 01630
40060 01638
40070 01599
40080 01461
40090 01494
40100 01344
40110 01290
40120 01246
40130 01140
40140 01082
40150 01027
40160 00960
40170 00810
40180 00802
40190 00711
40200 00649
40210 00573
40220 00470
40230 00481

40240 00415
40250 00338
40260 00319
40270 00285
40280 00242
40290 00201
40300 00174
40310 00160
40320 00123
40330 00087
40340 00115
40350 00074
40360 00061
40370 00064
40380 00045
40390 00040
40400 00030
40410 00023
40420 00015
40430 00012
40440 00012
40450 00006
40460 00003
40470 00003
40480 00002
40490 00005
40500 00001
40510 00000
40520 00001
40530 00002
40540 00002
40550 00000
40560 00000
40570 00001
40580 00001
40590 00000
40600 00000
40610 00000
40620 00000
40630 00000
40640 00001
40650 00000
40660 00000
40670 00000
40680 00000
40690 00000
40700 00000
以後全て 0