擬似乱数生成の評価
Avalanche 性テスト
PANAMA(MULTI-S01) 編

平成 13 年 1 月 22 日

1 取得条件

秘密鍵と，乱数列番号を微妙に (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．次に，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「PANAMA 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) の中で，ビット違いのものをサンプリングする．

まず，秘密鍵は cm102-cs200 までの (cm102,cm103 の組から始まる)254 通りに対して，100 通りの乱数列番号による出力の差分 (排他的論理和) に対して，0/1 等頻度性を評価する．

次に，同様に秘密鍵として (ca513..ca514) などの組は，1 ビット違いの鍵であるので，先と同様に 100 通りの乱数列番号による出力の差分 (排他的論理) に対して，0/1 等頻度性を評価する．

1 bit 違いの秘密鍵が合計 740 個，その各々に対する乱数列番号 100 種類に対する 0/1 等頻度性テストを行った．つまり，7 万 4000 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.

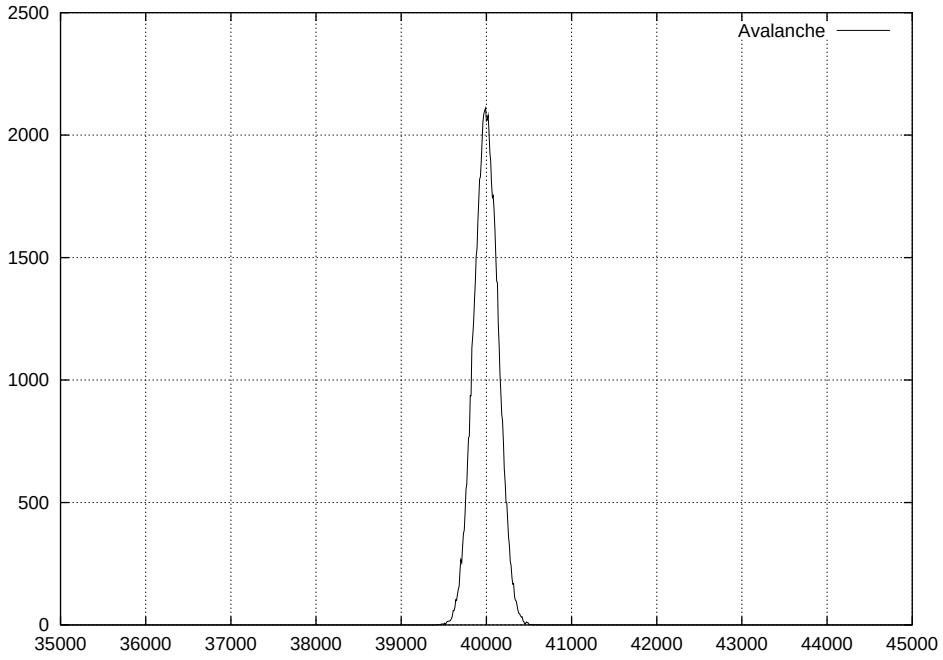

図 1: Avalanche テストによるビット反転数の度数分布

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 00000
39420 00001
39430 00000
39440 00001
39450 00001
39460 00001
39470 00004
39480 00003
39490 00005
39500 00001
39510 00007
39520 00002
39530 00009
39540 00014
39550 00015
39560 00015
39570 00016
39580 00020
39590 00026
39600 00035
39610 00059
39620 00058
39630 00072
39640 00103
39650 00100
39660 00124
39670 00145
39680 00160
39690 00221
39700 00266
39710 00254
39720 00317
39730 00374
39740 00387
39750 00455
39760 00553
39770 00576
39780 00670
39790 00764
39800 00771
39810 00936
39820 00936
39830 01131
39840 01183
39850 01236
39860 01331
39870 01400
39880 01502
39890 01538
39900 01645
39910 01737
39920 01820
39930 01830
39940 01899
39950 01981
39960 02053
39970 02088
39980 02101
39990 02110
40000 02058
40010 02061
40020 02081
40030 02020
40040 01929
40050 01897
40060 01807
40070 01746
40080 01753
40090 01701
40100 01615
40110 01515
40120 01404
40130 01396
40140 01229
40150 01136
40160 01021
40170 00940
40180 00860
40190 00834
40200 00743
40210 00638
40220 00581
40230 00503

40240 00498
40250 00422
40260 00361
40270 00327
40280 00260
40290 00243
40300 00192
40310 00166
40320 00169
40330 00116
40340 00102
40350 00097
40360 00080
40370 00061
40380 00048
40390 00045
40400 00037
40410 00032
40420 00033
40430 00017
40440 00013
40450 00005
40460 00006
40470 00012
40480 00010
40490 00008
40500 00002
40510 00002
40520 00000
40530 00002
40540 00000
40550 00000
40560 00000
40570 00001
40580 00001
40590 00000
40600 00000
40610 00000
40620 00002
40630 00000
40640 00000
40650 00000
40660 00000
40670 00000
40680 00000
40690 00000
40700 00000
以後全て 0