# 擬似乱数生成の評価
# 長周期連性テスト
# TOYOCRYPT-HR1 編

平成 13 年 1 月 21 日

## 1　取得条件

FIPS 140 と同様に 20000 bits をサンプリングして，その中で同一 bits (gaps, blocks) の長さを評価する．このテストでは，長さを 1,2,3,4,5,6,... と可能な限り分解する．出力系列が真の乱数系列とみなせるならば，0 または 1 が数十 bits も連続することはまずない．FIPS 140 を合格する条件は全てのサンプルに対して，長さ 34 以上の gaps または blocks が発生しないことである．

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) を対象とし，各々の出力の先頭 20000bits を対象に評価を行った．

つまり，このテストでは計 10 万件のテストを行ったことになる．

## 2　テスト結果

テスト結果を示す.

### 2.1　gaps の分布

左から順に gaps の長さ，度数である．

```
00001  250046657
00002  124982579
00003  62457293
00004  31254607
00005  15618122
00006  7808637
00007  3901397
00008  1955950
00009  970925
00010  490981
00011  244782
00012  125637
00013  60895
```

```
00014  30584
00015  14668
00016  8016
00017  3865
00018  1884
00019  971
00020  670
00021  214
00022  138
00023  185
00024  29
00025  11
00026  9
00027  3
00028  2
00029  2
00030  1
00031  1
00032  1
00033  1
00034  1
00035  1
00036  1
00037  1
00038  20
00039  0
```
(以下全て 0)

## 2.2 blocks の分布

左から順に blocks の長さ，度数である．

```
00001  249949206
00002  124968692
00003  62520755
00004  31281806
00005  15625345
00006  7808106
00007  3914866
00008  1957182
00009  975762
00010  492495
00011  243024
00012  123518
```

```
00013  59045
00014  30157
00015  14992
00016  6965
00017  3351
00018  2050
00019  981
00020  533
00021  188
00022  104
00023  178
00024  20
00025  13
00026  6
00027  0
00028  2
00029  2
00030  0
00031  0
00032  0
00033  0
00034  0
00035  0
00036  0
00037  0
```

gaps については， FIPS の試験を合格しないものが存在する．付録に度数分布を示す.

度数分布をみる限り，理想的な分布に見えるが，実際には FIPS の条件を満たさない結果もある．このことは，一部の危険鍵 (生成列が乱数性を保てないもの) を除けば、乱数らしい振舞いをするということ、および、今回テストした鍵の中に，危険鍵が含まれていたことを示唆している．

## 3 評価

10 万件の検査の結果は FIPS 140 の試験を合格できないと判断する．鍵の選び方に依存するのだが， gaps が大きくなる傾向が高い.

## 4 長い gaps 発生の理由

長い gaps の発生する鍵は，次のものである.

```
[38]
c4001sa001
c4001sb000
c4001sb001
```

c4001sb002
c4001sb003
.....
c4001sb018
[37]
c4001sb019
[36]
c4001sb020（以下，最大長が 1 づつ減っていく，c4001sb039 まで）

固定鍵 c4001 とは，
C = 00000000 00000000 00000008 04008001
であり，sa001 は
S = 00000000 00000000 00000000 00000001
また，sb0??(00-19) までは，

S = 00000000 00000000 00000000 00000002
S = 00000000 00000000 00000000 00000004
S = 00000000 00000000 00000000 00000008
S = 00000000 00000000 00000000 00000010
S = 00000000 00000000 00000000 00000020
S = 00000000 00000000 00000000 00000040
S = 00000000 00000000 00000000 00000080
S = 00000000 00000000 00000000 00000100
S = 00000000 00000000 00000000 00000200
S = 00000000 00000000 00000000 00000400
S = 00000000 00000000 00000000 00000800
S = 00000000 00000000 00000000 00001000
S = 00000000 00000000 00000000 00002000
S = 00000000 00000000 00000000 00004000
S = 00000000 00000000 00000000 00008000
S = 00000000 00000000 00000000 00010000
S = 00000000 00000000 00000000 00020000
S = 00000000 00000000 00000000 00040000
S = 00000000 00000000 00000000 00080000
S = 00000000 00000000 00000000 00100000

である．原因は「暗号アルゴリズムの詳細評価報告書 擬似乱数生成 TOYOCRYPT-HR1 編」を参照のこと．上記に示した固定鍵 C とストリーム鍵 S を使うと，擬似乱数性を満たさない値 (大きな gap) を生成する．

## 度数分布

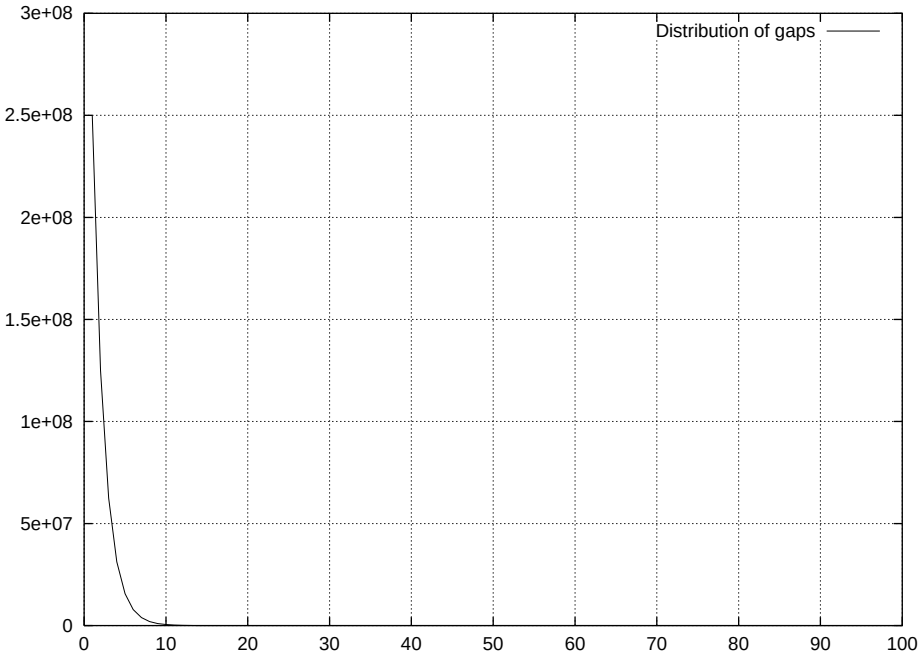


図 1: gaps(OFF bit(=0)) の長さの分布

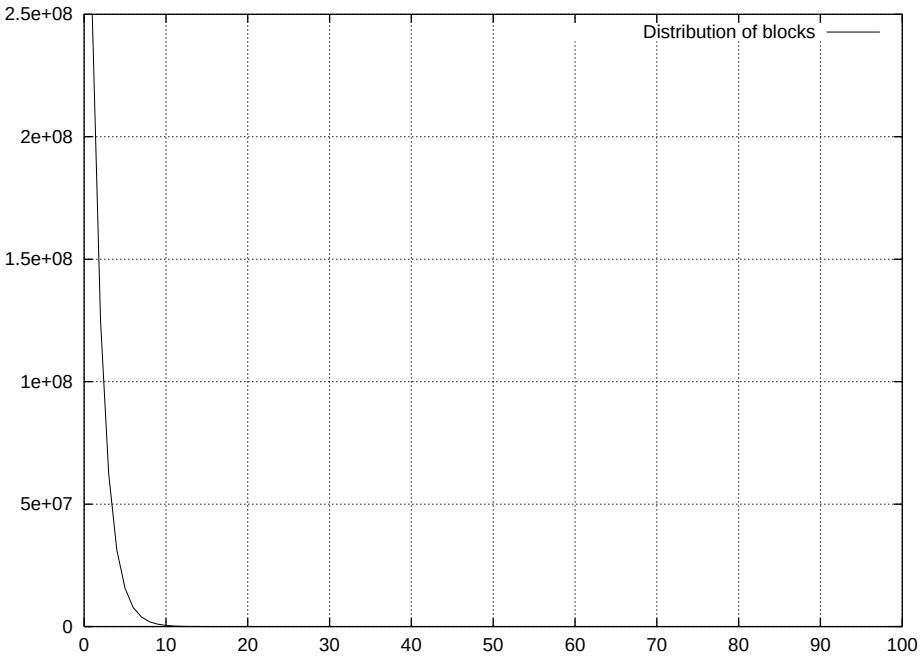


図 2: blocks(ON bit(=1) の長さの分布