ＩＡＳ

KEK060512

真性乱数の生成

齊藤　威
(株)ＩＡＳ総合研究所
saito.t@mx3.ttcn.ne.jp
基礎的な事項に関する問い合わせ

石井孝一、須賀川　進、石島誠一郎
(株）エルイーテック
k_ishii@letech.co.jp
製品サンプルに関する問い合わせ

目次

Ⅰ　真性乱数の生成

1．Introduction (物理乱数の問題点、ランダムとは何か？)

2．熱雑音 (波、変動) の粒子的取り扱い

3．真性乱数の生成
熱雑音→ランダムパルス→真性乱数

4．物理乱数が必ずしもランダムとは限らない

5．乱数検定法の検定

Ⅱ　真性乱数生成器 (GRNG)

1．ランダム性・一様性の保証 (±6σ)

2．生成速度 (～1G byte/sec)

3．故障、意図的攻撃を瞬時に検出

4．ランダム性の常時 (ハード) 検定

番外 (Appendixes)：ＩＡＳ紹介

I A S

Institute for Advanced Studies

← IAP

By Prof.Nishikawa

I 技術開発

(1) 自分の特許15件(50)の製品化

次期開発：二次元放射線検出器（医学利用）

(2) 特許(依頼を受けた）の製品化、企業化

次期開発：牛胃壁粘膜から分離した活性蛋白の商品化

II 科学研究

(1) 極限エネルギー（≧10^{20}eV）宇宙線の観測

コヒーレントチェレンコフ電波の観測。月周回衛星(2009)に搭載予定

(2) 重粒子の検出

Massive elementary particles。宇宙線研究所からAlma Ataへ

(3) 太陽風舟（帆）による超重粒子（Dark Matter）の検出

太陽風舟の帆を検出器（Acoustic)として利用。帆の開発。

(4) 生体有機分子のホモキラリテイ（光学異性体）の起源の研究

数10 Ciの偏極電子（Sr^{90}）を照射。アミノ酸構造の非対称性生成実験

(5) 地球極限環境での微生物の研究

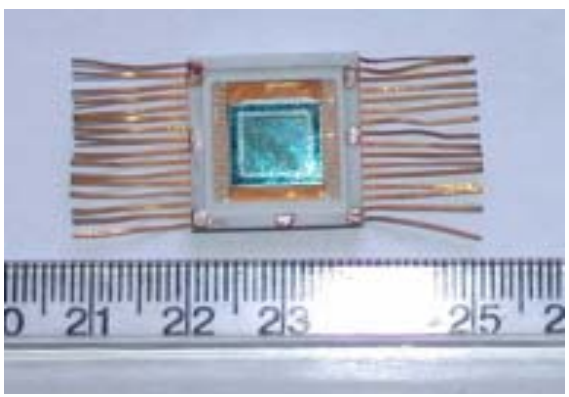
成層圏、東シベリア、北極圏での微生物採取。有用微生物の探査

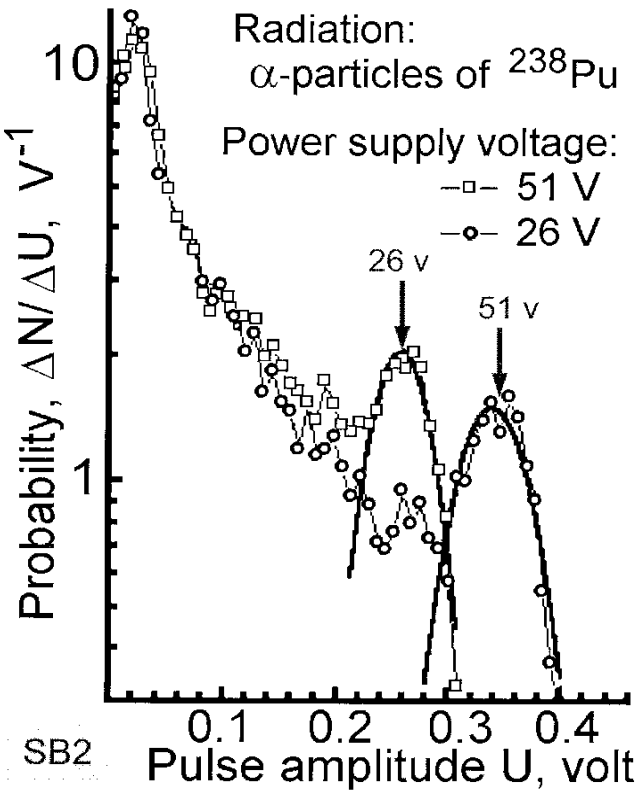
次期開発

二次元放射線測定器

陽電子 (次世代PET、分子イメージング),
γ （TL-201, Tc-99m）、X 線

(1) 高感度。閾値はMIPの10分の1。
(2) リニアリテイ：～10^5 (測定値)
(3) 時間分解能：10 ns以下。
(4) 位置分解法：～100μm。
(5) 高い耐放射線量
(6) 温度ドリフト： ≦1%(-70℃から＋70℃)
(7) S/N(signal/noise):MIPに対して～100。





検出器からの直接のシグナル(電圧値)
シグナルは検出器の内部で約100倍に増幅される。

科学研究

(1) 極限エネルギー (≧10^{20}eV) 宇宙線の観測

Detection of Ultrahigh-Energy Cosmic Rays and Neutrinos by Radio Method Using Lunar Satellite. **Cosmic Research, Vol.44, No.1 pp19-38 (2006)**

Cosmic microwave background, Greisen-Zatsepin-Kuzmin (GZK) cut off, Lunar satellites, Regolith layer, Coherent Cherenkov radio emission

(2) 重粒子の検出

Is there strange-quark matter in galactic cosmic rays?,
Phys. Rev. Lett. 65, 2094(1990), Nuclear Phys 24B, 184(1991).

Cosmic rays, Strange Quark Matter, Technibaryon, Superheavy hydrogen Superheavy isotopes

(3) 太陽風舟 (帆) による超重粒子 (Dark Matter) の検出

Search for Charged Massive Particles of Dark Matter Using Acoustic Detectors, **Proposal to "Solar Sail Mission" (2000)**

Dark Matter, Strangelets, Champs, Solar Sail, Piezoelectric Films, Acoustic signal

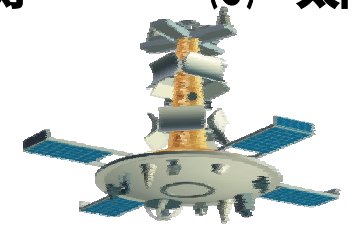
(4) 生体有機分子のホモキラリテイ (光学異性体) の起源の研究。

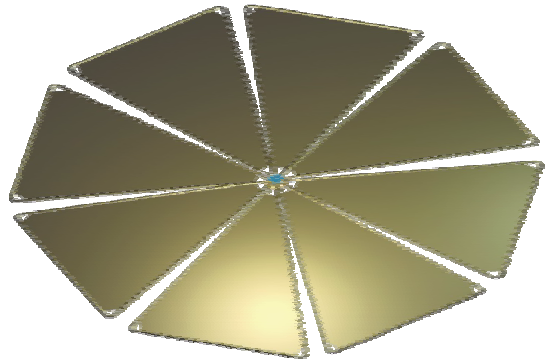
Origins Life Evol. Biosphere 20, 99(1990), 28, 155 (1998).
Journal of Applied Physics 98, 0024907 (2005)

Chemical evolution, Amino acids, Chirality, Super nova explosion , Sr^{90}
Polarized electrons, Week interactions, Metallic complex, Catalysis

(1) 極限エネルギー宇宙線の観測

(3) 太陽風舟 (帆) によるDark Matter) の検出





(2) Massive Particlesの検出

(4) ホモキラリテイ (光学異性体) の起源

1－1　　物理乱数の問題点

- 物理乱数が必ずしも真性乱数とは限らない。

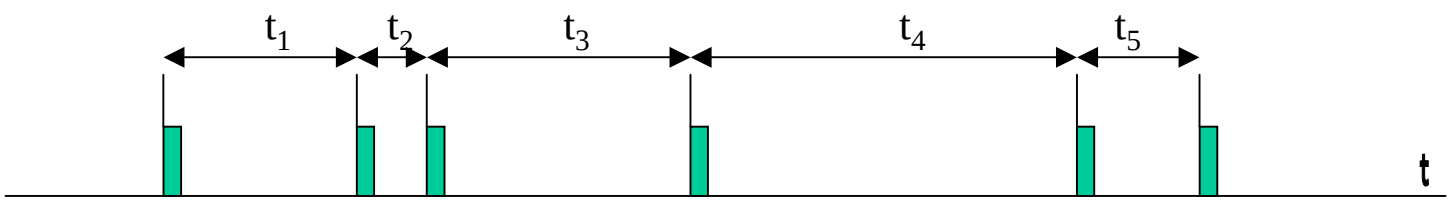
- 物理乱数であれば、

  既存の擬似乱数検定法の**総てに合格**する。

  （合格しない物理乱数は論外）

1－2　ランダムとは何か

数学的に定義することは困難。
ランダム性の定義は、物理学では明瞭。



ある現象において、それぞれの事象が、他の事象と独立に起っている現象を**統計的変動（ランダムな現象）**という。

ランダムな現象では、その事象が単位時間あたりに起こる頻度は、平均値＜n＞の周りに**ポアッソン（Poisson）の式**に従って変動する。　またその事象が起こる時間間隔tの確率密度は、その事象が起こる平均の時間間隔（To）の指数分布[**exp（-t/To）**]となる（**ポアッソン到達**）。

2．　熱雑音の粒子的取り扱い

ランダムパルサー
(1997)

粒子

放射線

統計的変動

1970～

真性乱数

ポアッソン分布･到達

1950～

2002～

熱雑音

真性乱数

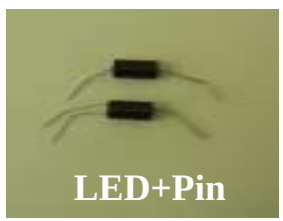
波(変動)

熱雑音

1960～

物理乱数

Nyquist(1928)



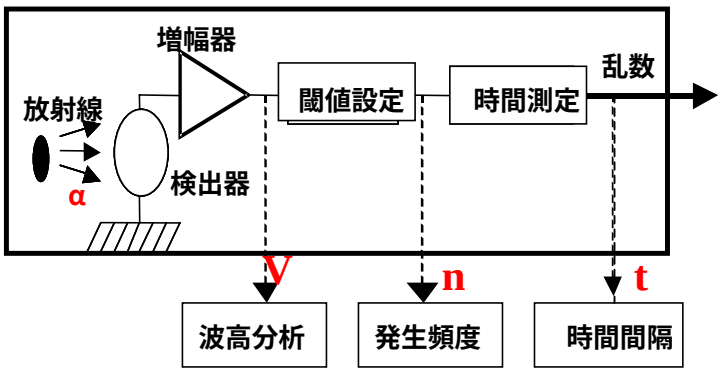
LED+Pin

(1999)

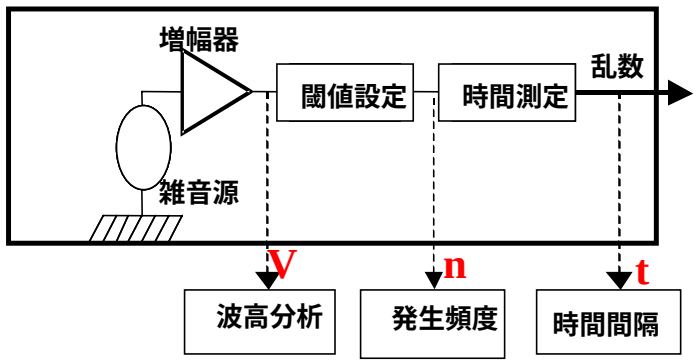
LED+PMT

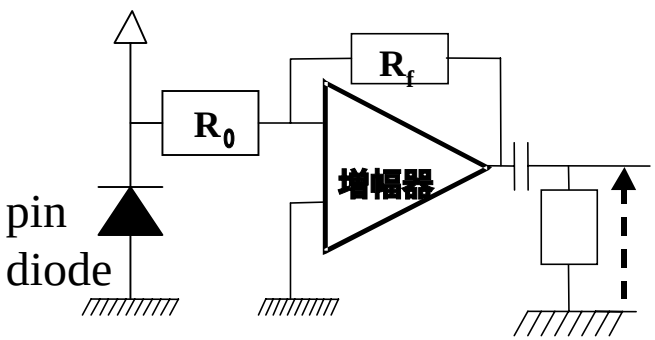
熱雑音(波) の粒子的取り扱い

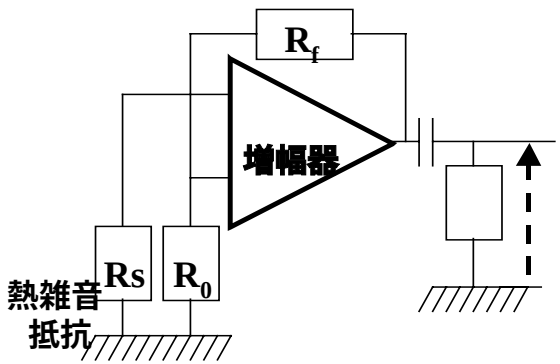
放射線



熱雑音

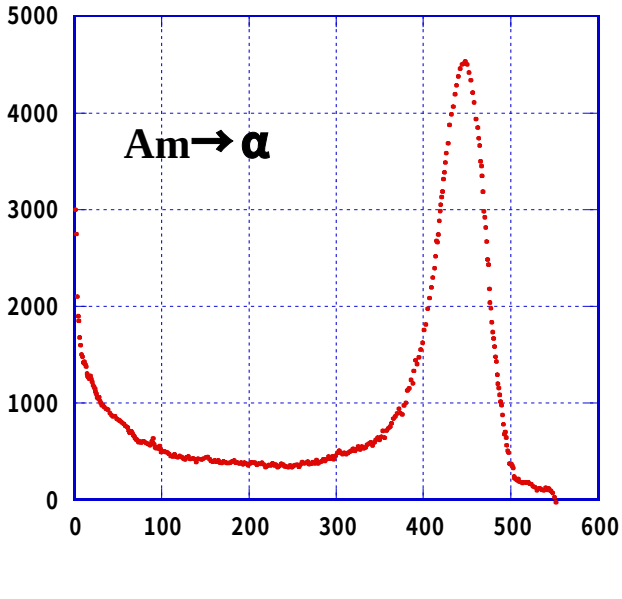






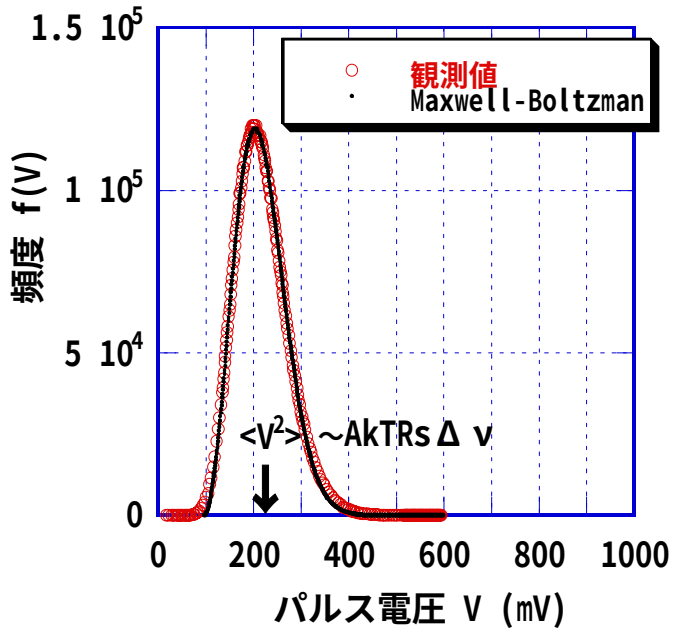
パルス電圧分布 V

放射線



ランダムパルサー（9頁）の波高分布
FWHM = 0.121

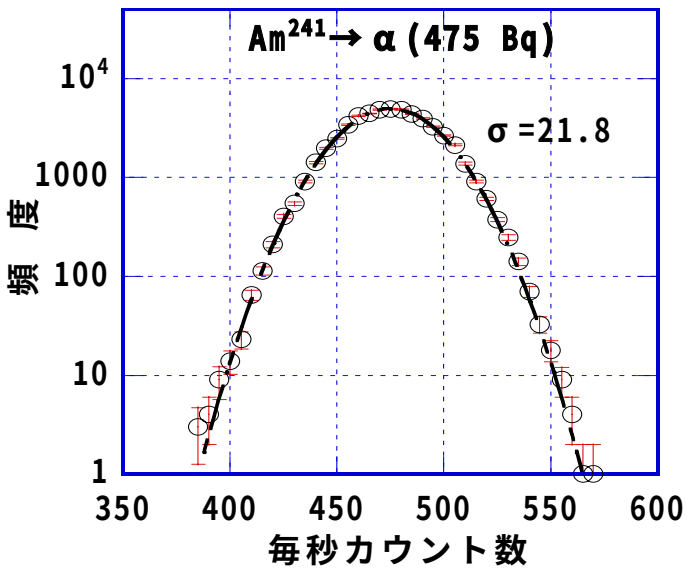
熱雑音



計測値：○
実曲線：$F(V)=V^2\exp(-V^2/2)$
$\langle V^2\rangle \sim AkTRs\Delta\nu$
A：増幅度、k：ボルツマンの常数、
T：温度、Rs：抵抗値、Δν：周波数帯域

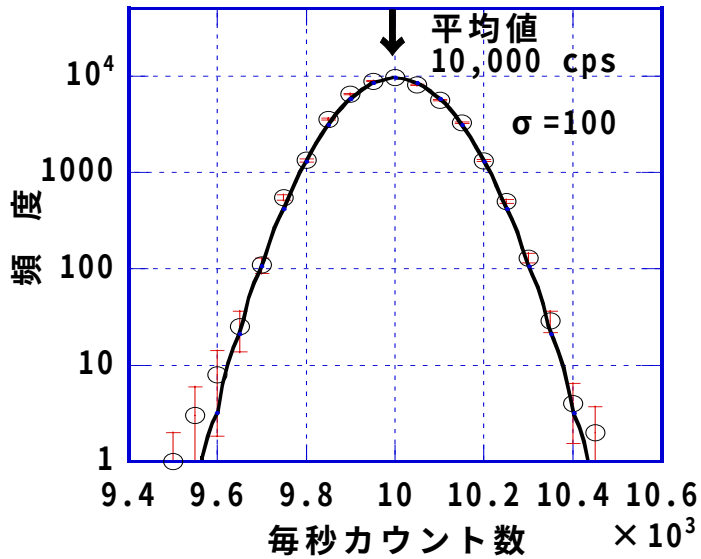
発生頻度 n cps

放射線



< n > = 475 Bq, σ =21.8 (=√475)

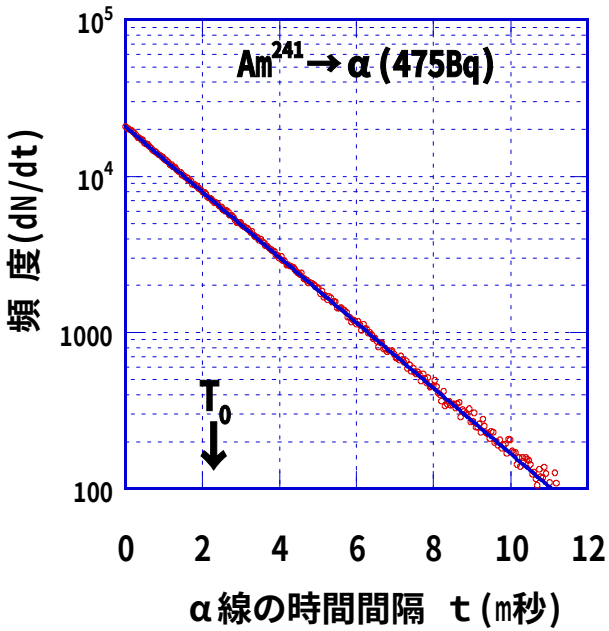
熱雑音



< n > =10,000 cps, σ =100 (=√10,000)

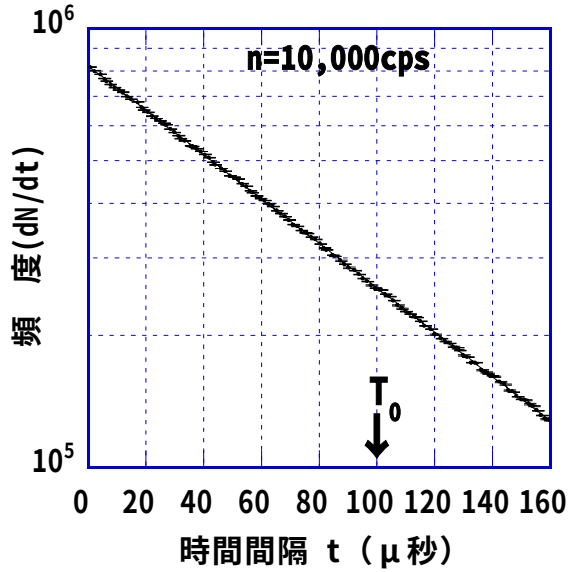
時間間隔　t

放射線



<n >= 475 Bq, T_0 =1/n=2.1m sec

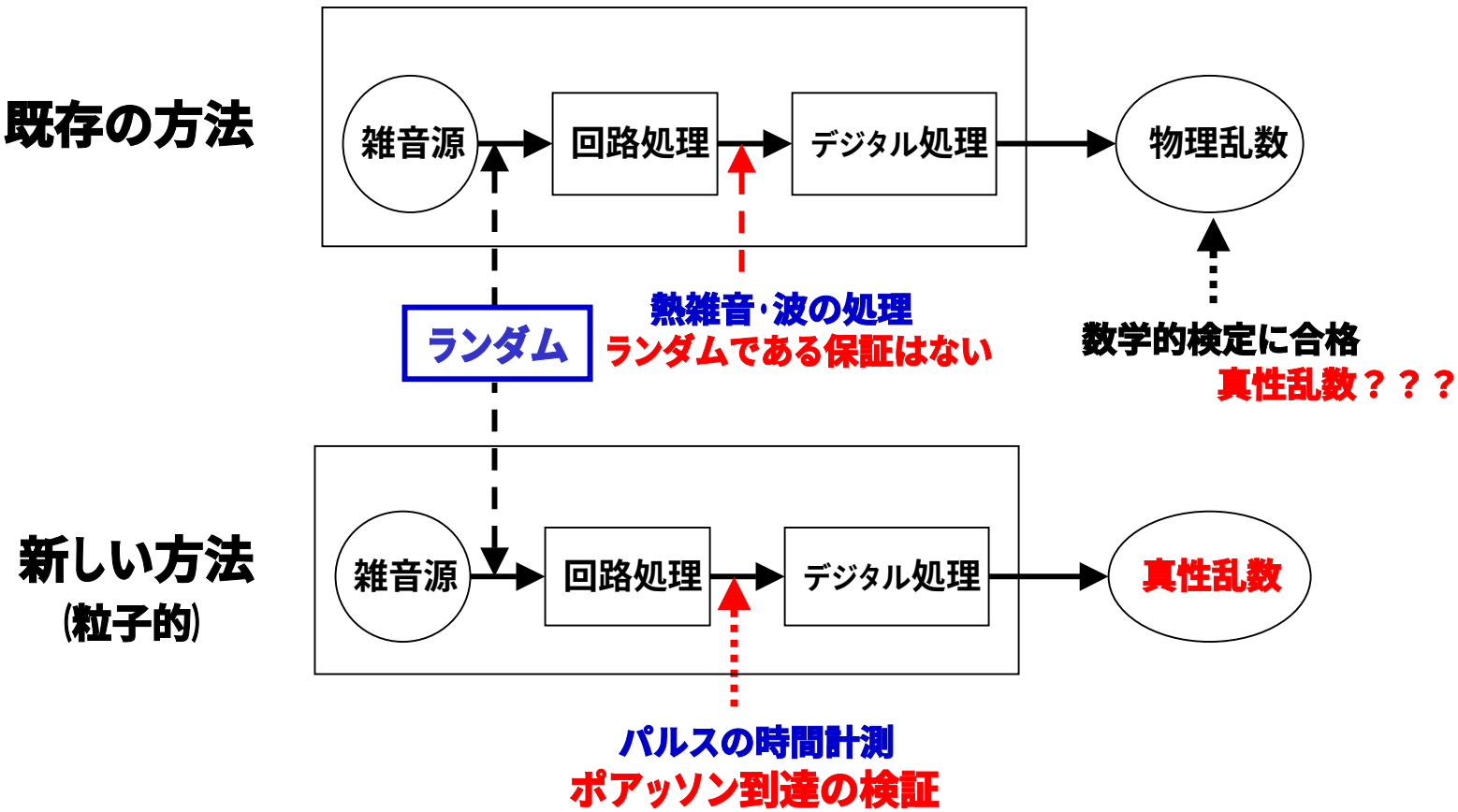
熱雑音



<n>=10,000 cps, T_0=1/＜n＞=100 μ sec

3．真性乱数の生成

新しい方式と既存の方法との比較



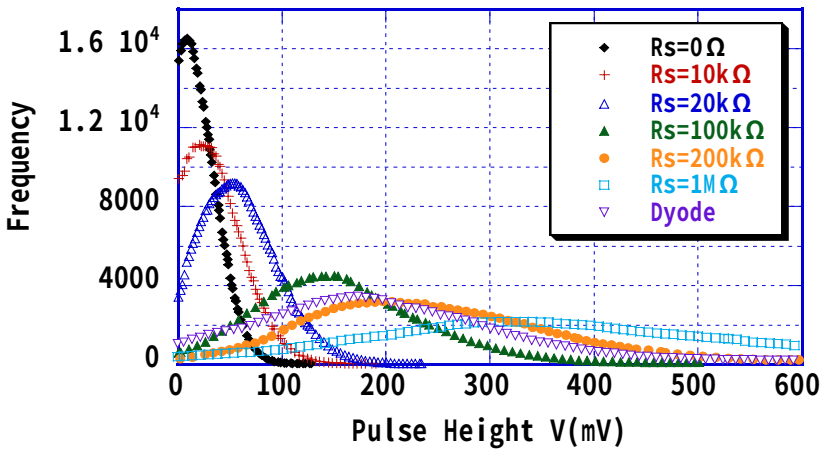
① 熱雑音をランダムパルスとして取り出す

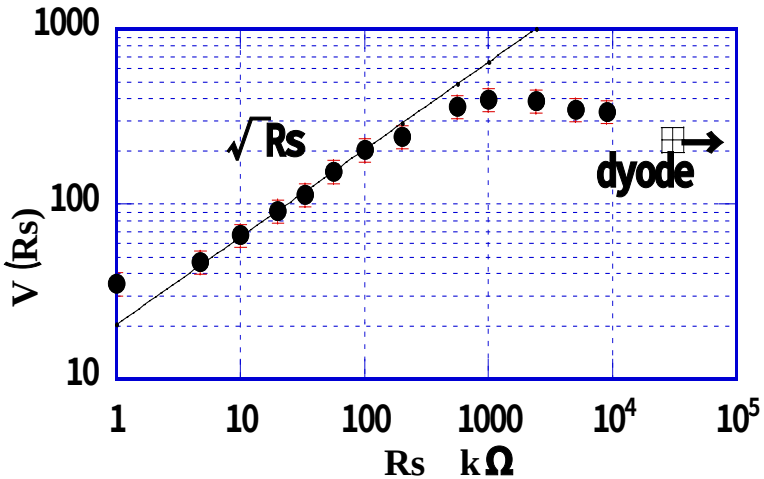
問題

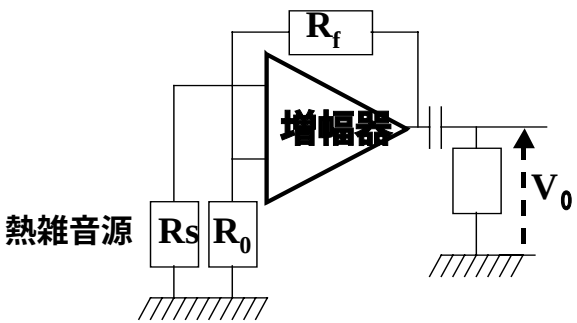
増幅器と熱雑音抵抗Rsの選択

(1) [雑音] = [熱雑音] + [電流雑音 (1/f 雑音)] + [ショット雑音] + [増幅器雑音]

(2) 熱雑音はランダムな現象であるが、それを増幅した電圧パルスがランダムとは限らない。







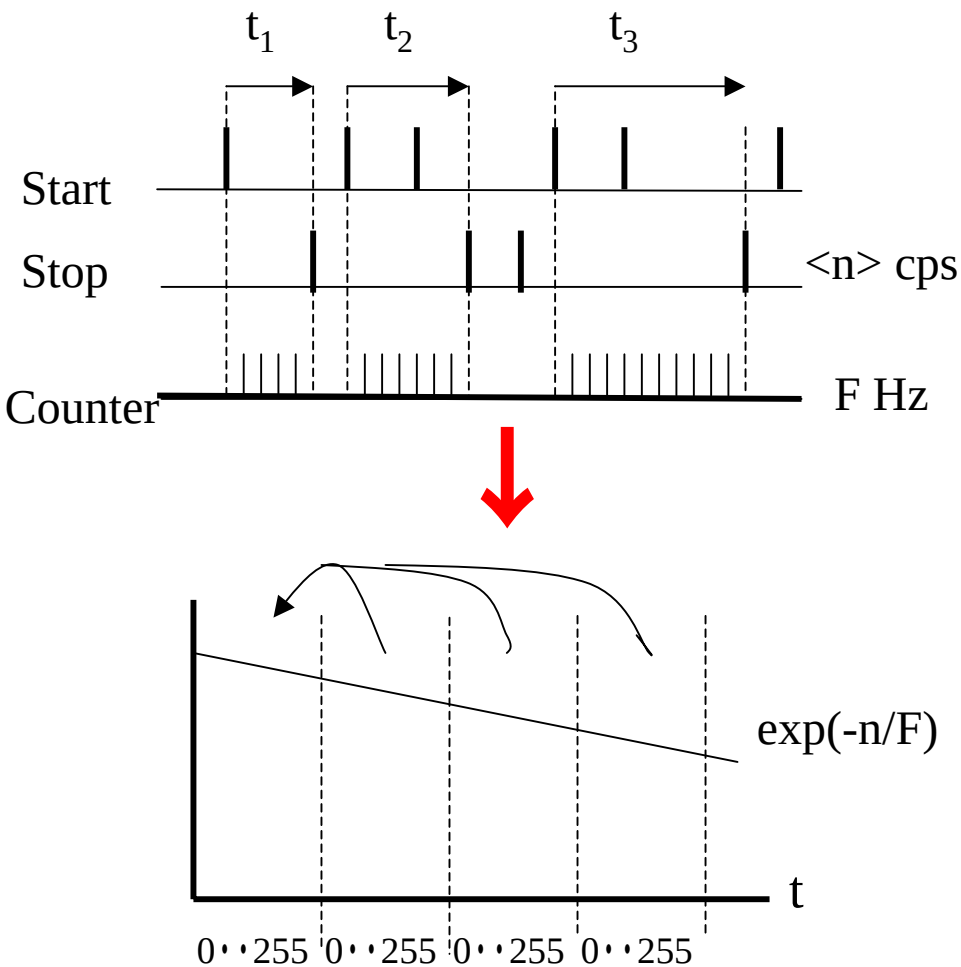
$V(Rs) = \sqrt{[\langle V_0^2 \rangle - \langle V^2(Rs=0) \rangle]}$

$V(Rs=0) = V(R_0, R_f, R_A)$

$\langle V^2(Rs) \rangle \sim kTRs\Delta\nu$ (ナイキストの式)

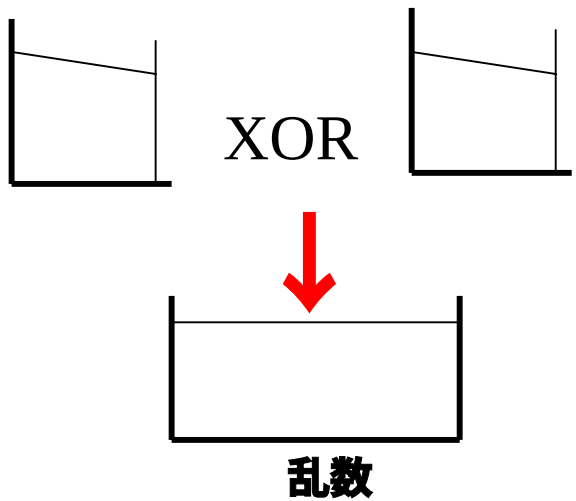
K：ボルツマン常数、T：Rsの絶対温度、Δνは周波数帯域巾

② パルスの時間間隔の計測



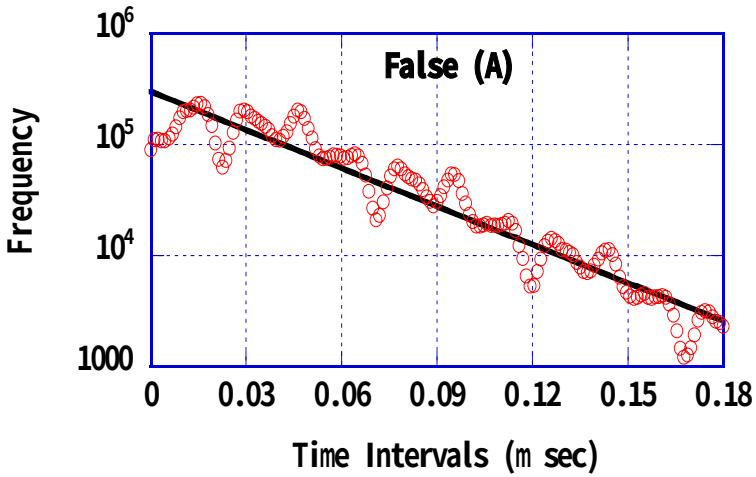
③ 時間分布のポアッソン検定

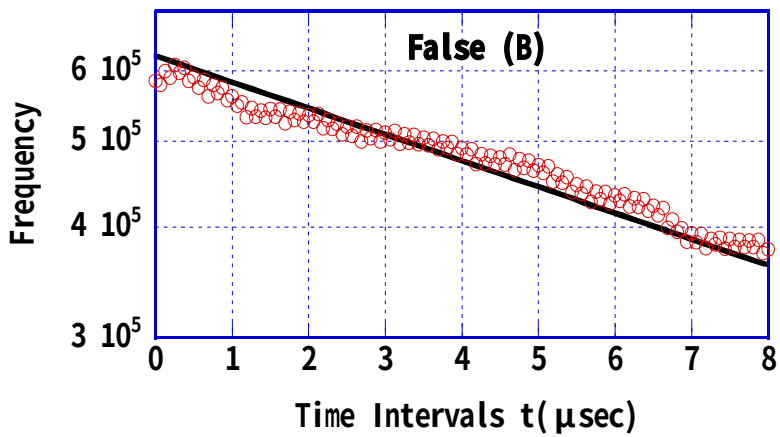
④ ランダム分布 (指数分布) の平坦化

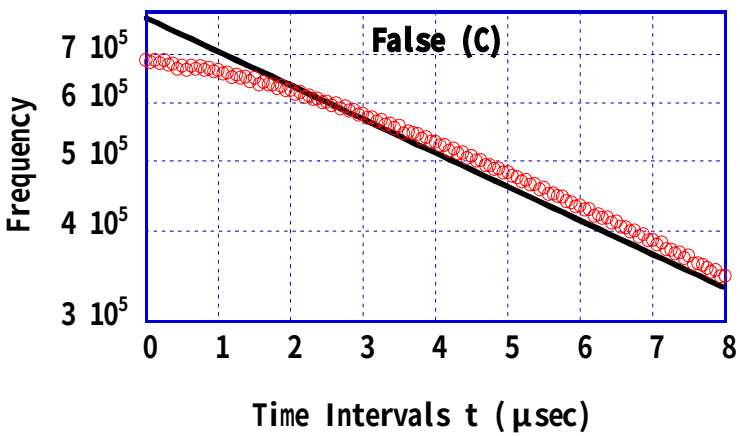


⑤ 乱数分布の一様性検定

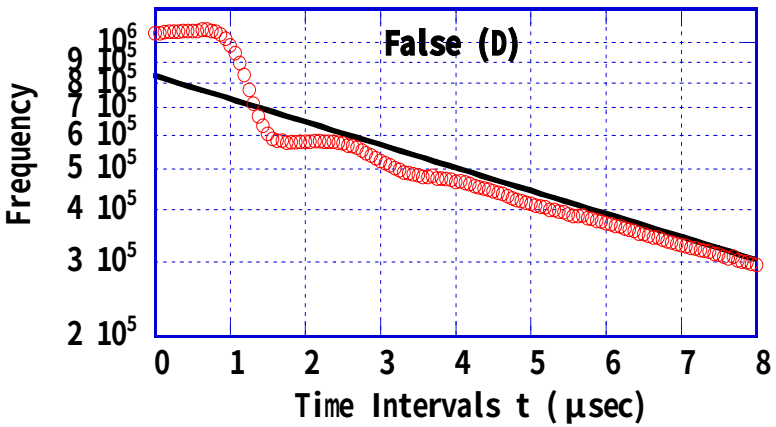
4．物理乱数が真の乱数とは限らない

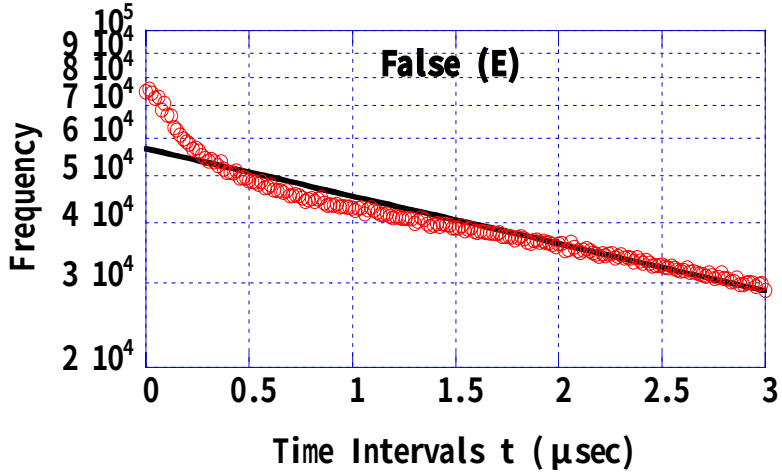


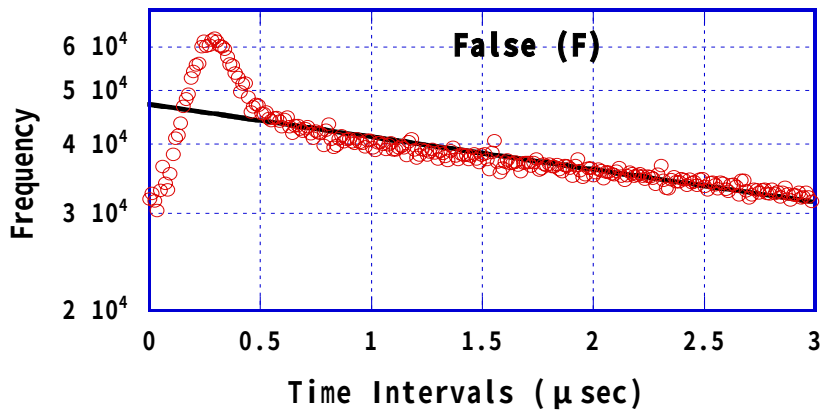




(A)を除く物理乱数[(B)～(E)]が既存の総ての乱数検定法に合格する。


False (D)
Frequency
Time Intervals t (μsec)


False (E)
Frequency
Time Intervals t (μsec)

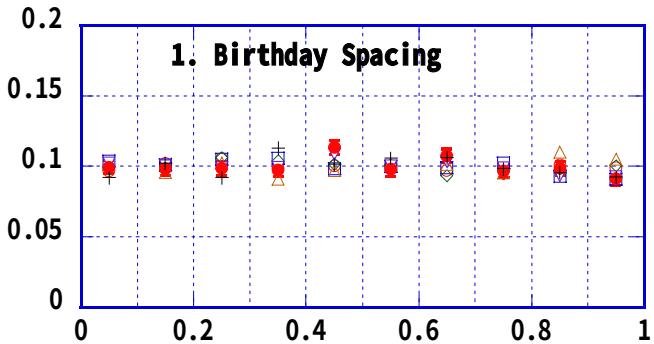

False (F)
Frequency
Time Intervals (μsec)

5．乱数検定法の検定

DEIHARD検定（19項目）

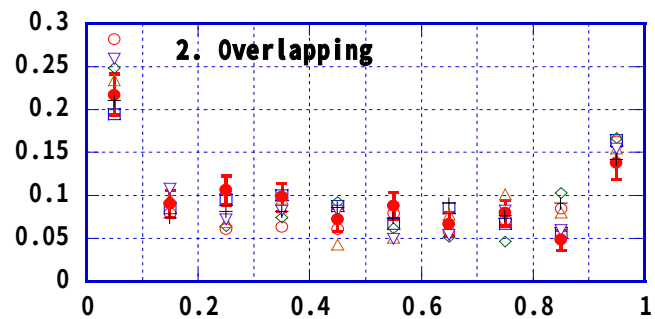
Niniformity of P-value distributions

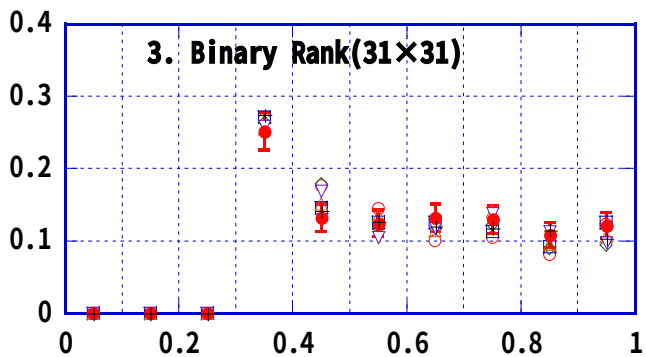
●：真性乱数、○：物理乱数A、□：物理乱数B
◇：物理乱数C、△：物理乱数D、▽：物理乱数E
＋：Mersenne Twister

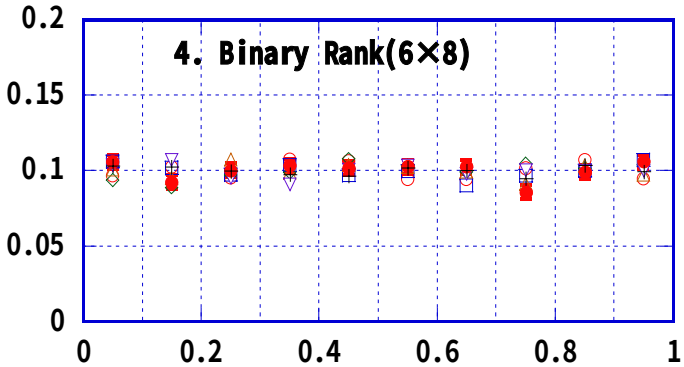


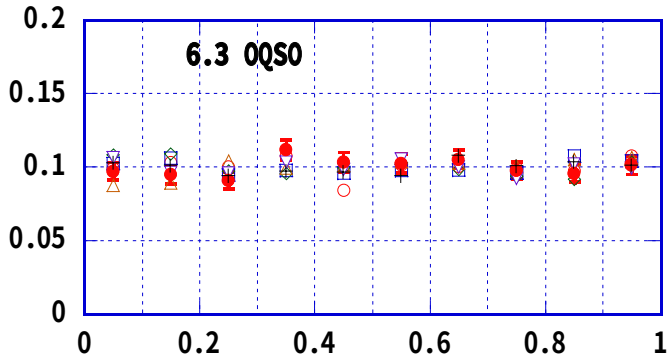
←

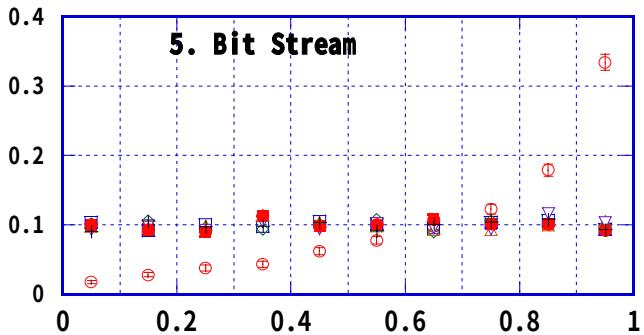
$n = 2^{24}$からランダムに$m=2^9$とって、2回以上現れた値の数は、平均$(2^9)^3/2^{26}$のポアッソン分布にしたがう。500回試行してポアッソン分布と比較したχ2よりP値を計算

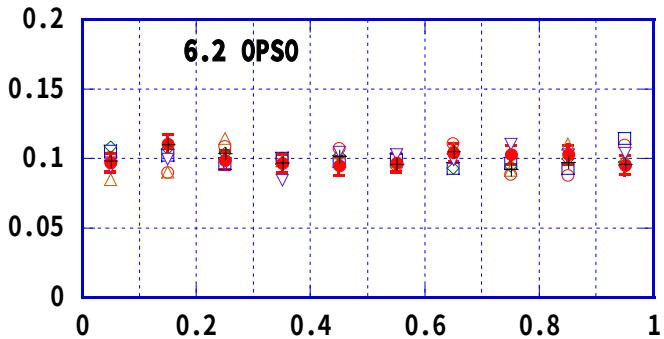


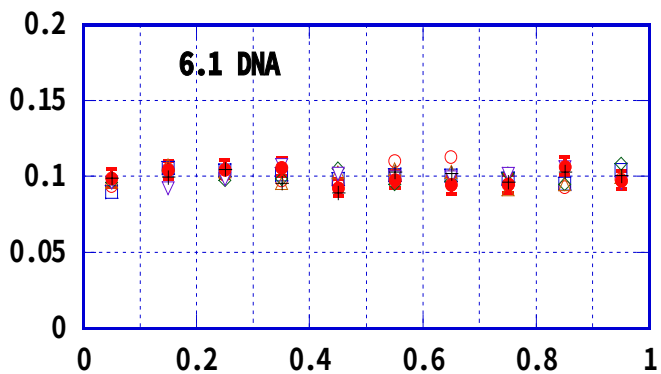


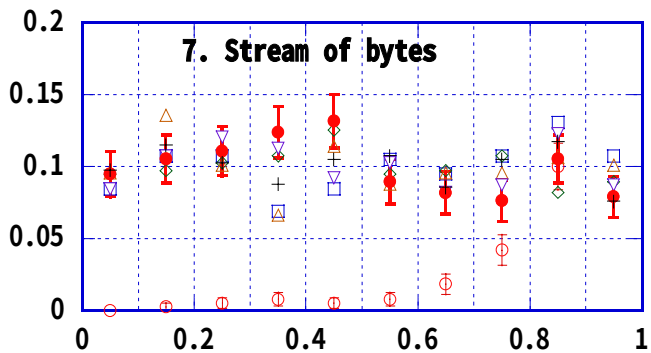

4. Binary Rank(6×8)
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1

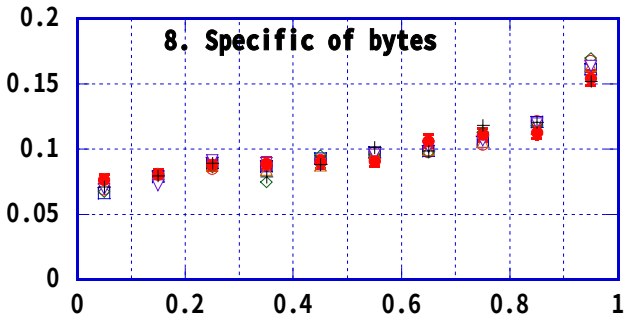

6.3 OQSO
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1

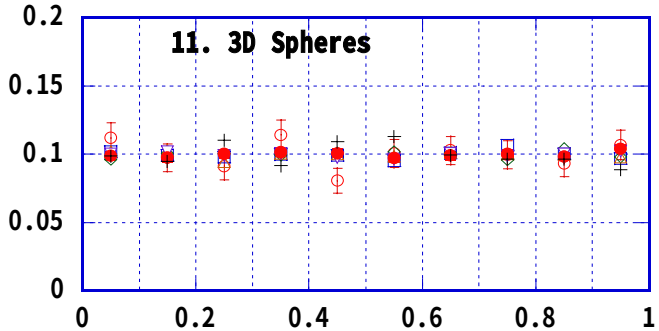

5. Bit Stream
0.4
0.3
0.2
0.1
0
0
0.2
0.4
0.6
0.8
1

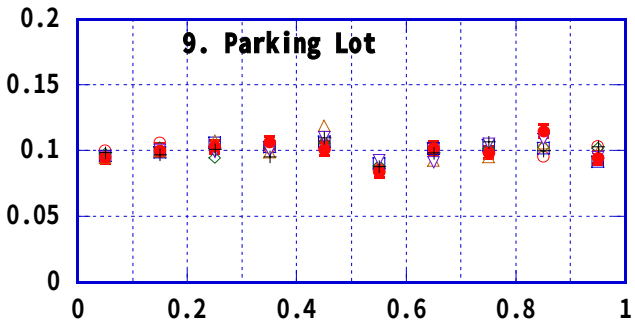

6.2 OPSO
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1

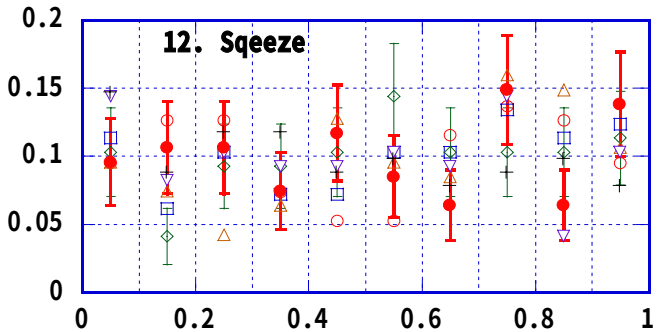

6.1 DNA
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1

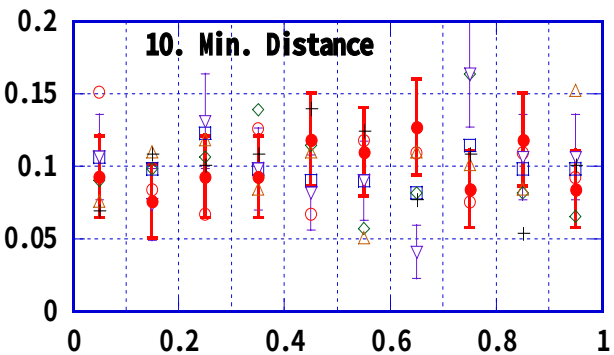

7. Stream of bytes
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1

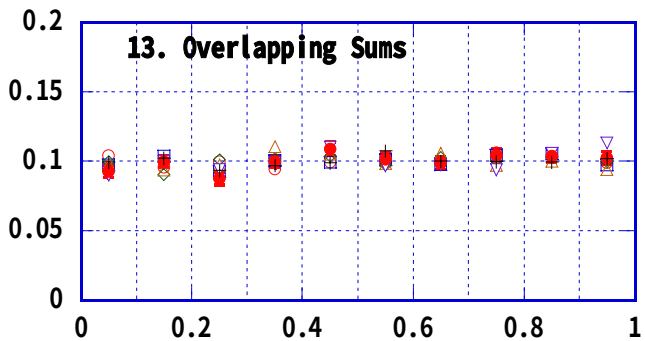

8. Specific of bytes
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1

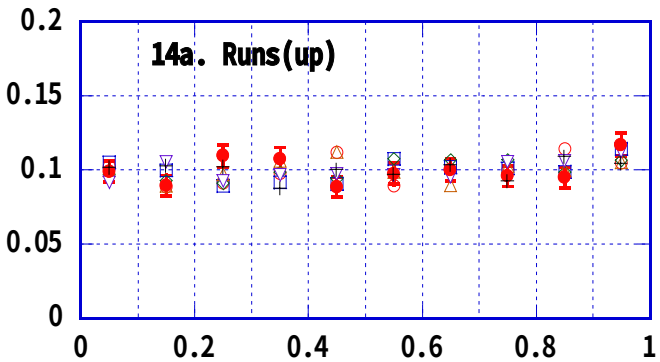

11. 3D Spheres
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1

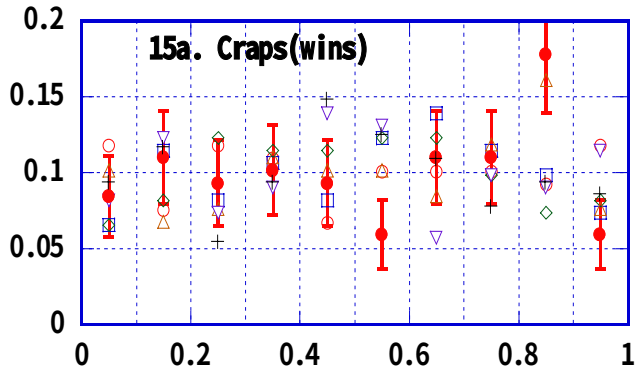

9. Parking Lot
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1

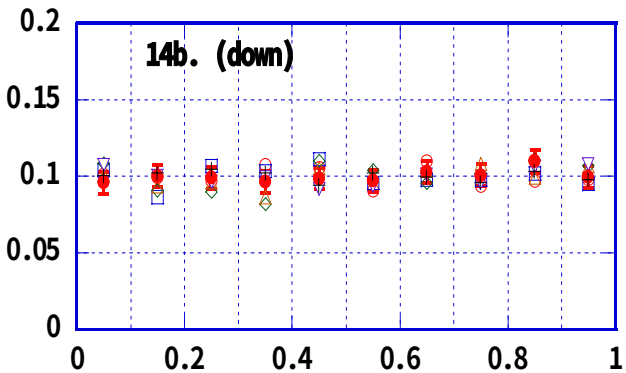

12. Sqeeze
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1

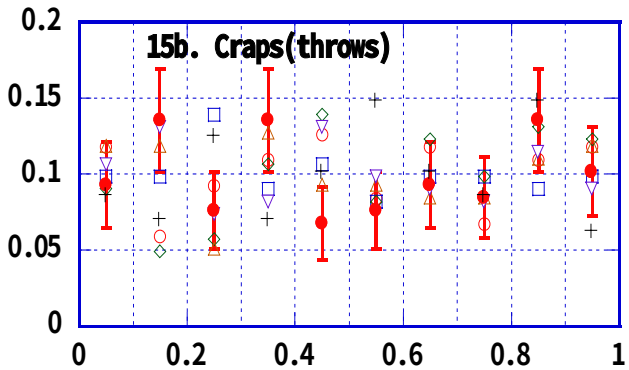

10. Min. Distance
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1


13. Overlapping Sums
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1


14a. Runs(up)
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1

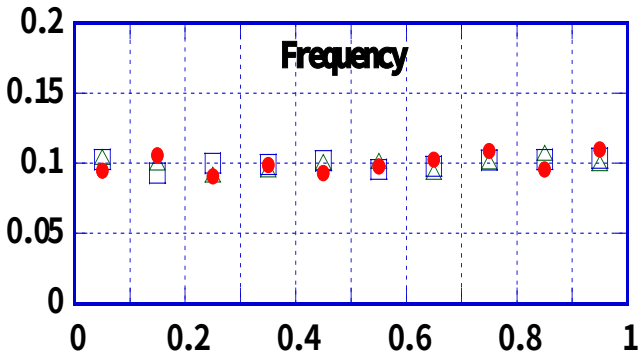

15a. Craps(wins)
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1

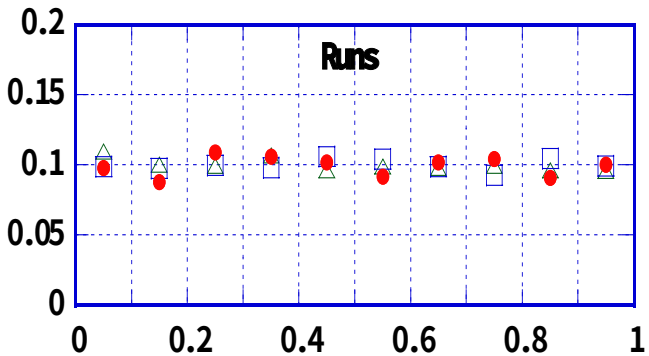

14b. (down)
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1

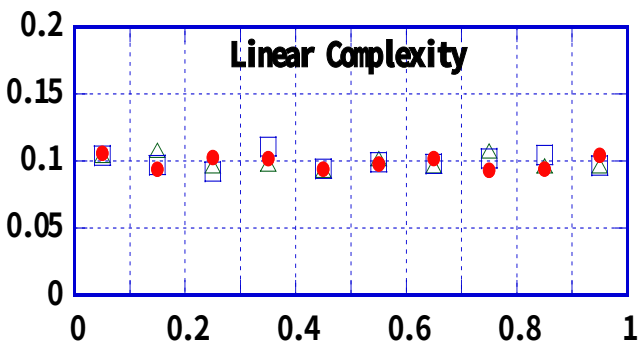

15b. Craps(throws)
0.2
0.15
0.1
0.05
0
0
0.2
0.4
0.6
0.8
1

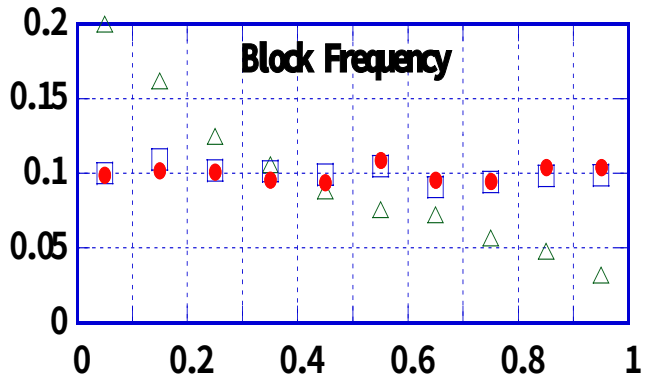
NIST検定 (Uniformity of P-Values)

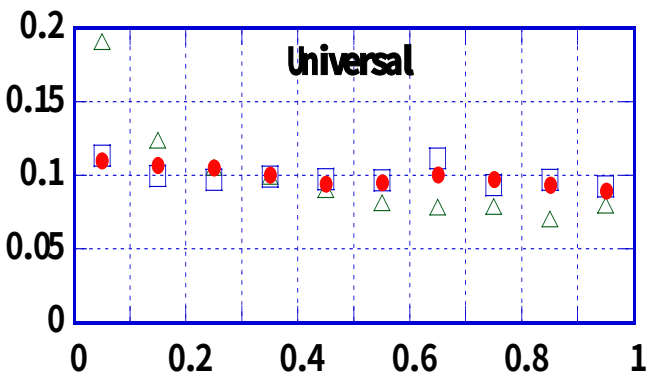
●：真性乱数
△：物理乱数：A
□：物理乱数：B-E











DEIHARD検定

	検定項目	真性	A	B-E
1	Birthday Spacing	○	○	○
2	Overlapping 5-Permutation	－－	－－	－－
3	Binary Rank (31X31)	－－	－－	－－
4	Binary Rank (6X8)	○	○	○
5	Bit stream	○	×	○
6a,b,c	DNA, OPSO, OQSO	○	○	○
7	Count-1 (Stream of Bytes)	○	×	○
8	Count-1 (Specific bytes)	○	○	○
9	Parking Lot	○	○	○
10	Minimum Distance	○	○	○
11	3 D Spheres	○	○	○
12	Sqeeze	○	○	○
13	Overlapping Sums	○	○	○
14a,b	Runs (up), Runs (down)	○	○	○
15a,b	Craps (wins), Craps (throws)	○	○	○

NIST検定（800－22）

	検定項目	真性	A	B-E
1	Frequency	○	○	○
2	Block Frequency	○	×	○
3	Runs	○	○	○
4	Longest Run	○	○	○
5	Binary Matrix Rank	○	○	○
6	D F T（Corrected)	○	○	○
7	Non-overlapping Tem Match	○	○	○
8	Overlapping Temp Matching	○	○	○
9	Universal	○	×	○
10	Lempel Ziv Compression	－－	－－	－－
11	Linear Complexity	○	○	○
12	Serial	○	×	○
13	Approximate Entropy	○	×	○
14	Cumulative Sums	○	○	○
15	Random Excursions	○	○	○
16	Random Excursions Variant	○	○	○

ＩＡＳ真性乱数を不合格にするDIEHARD検定項目＃2は、検定式を導出過程での近似に問題があり、＃3はプログラムミス。
NISTの検定項目＃10は“真の乱数”を仮定した関数に問題がある。**NIST＃10はNIST version1.7では取り消されている。**

II　真性乱数生成器

特長

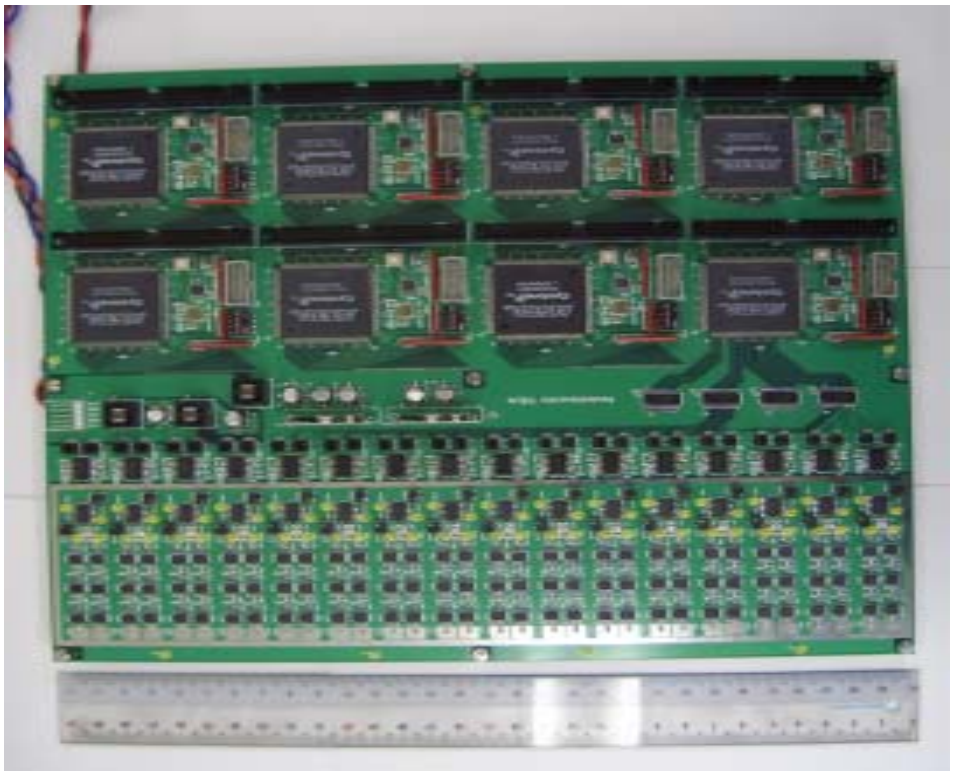
1．　ランダム性･一様性の保証（≧±6σ）

2．　生成速度（～1G byte/sec)

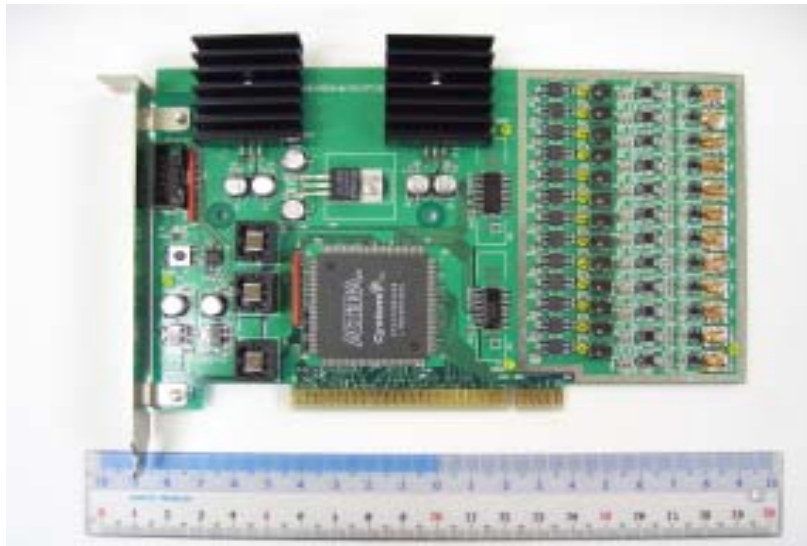
3．　故障、意図的攻撃を瞬時に検出

4．　ランダム性の常時検定

真性乱数生成器プロトタイプ



大型計算機によるシミュレーション
毎秒1GB真性乱数生成器

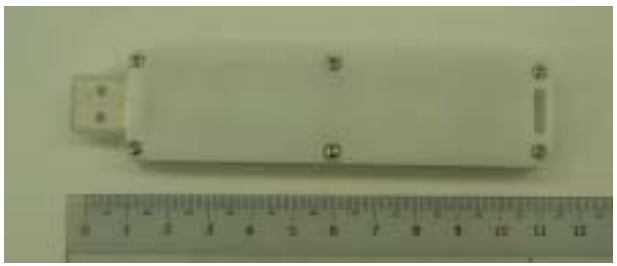


PCあるいはPCクラスター用
毎秒６４MB真性乱数生成器（1/2PCIボード）

現在5CPUによる並列計算が稼動中

製品サンプル

ICカードのCPU内挿入用
回路面積は1mm×1mm　(0.25mm×0.25mm)
稼動テストのために、ICチップになっている。



USB接続
毎秒≧12 Mバイト

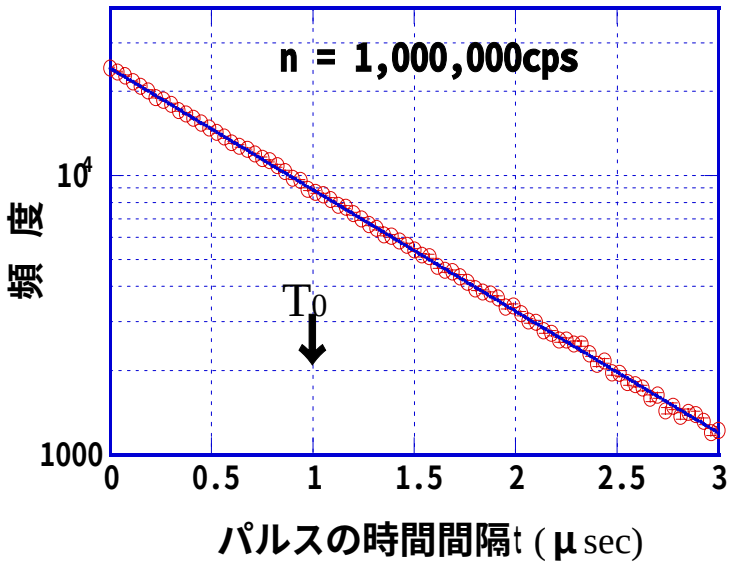
USB接続用
毎秒1～4Mバイト

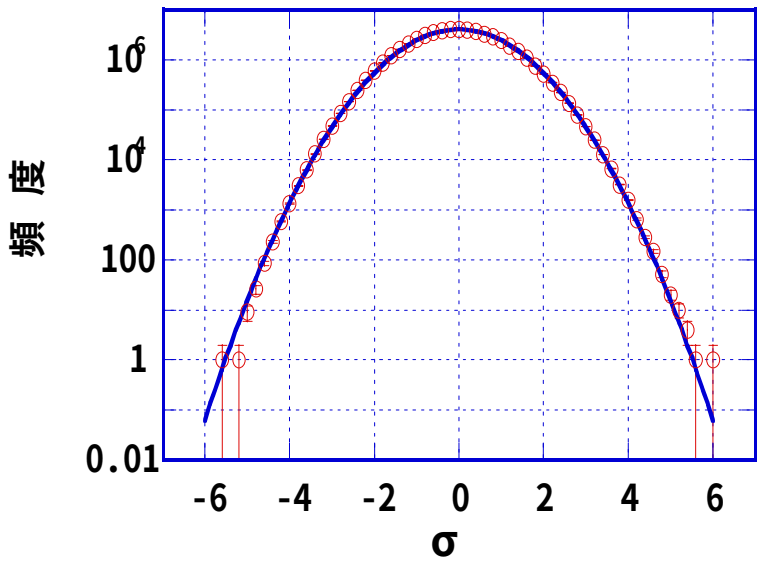
モニター募集中

(サンプル機貸出)

連絡先：k_ishii@letech.co.jp (石井 孝一)

特長1－1　ランダム性の保証





ポアッソン到達:

$\exp(-t/T_0) = \exp(-t/10^{-6})$

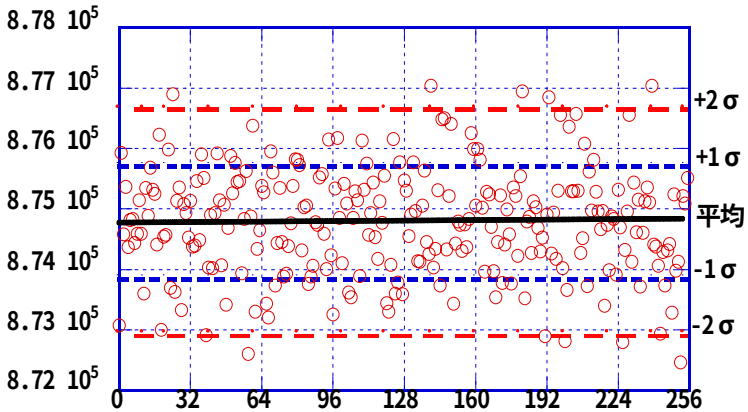
n = 1,000,000

To = 1/n = 1/1,000,000 = 1μ秒

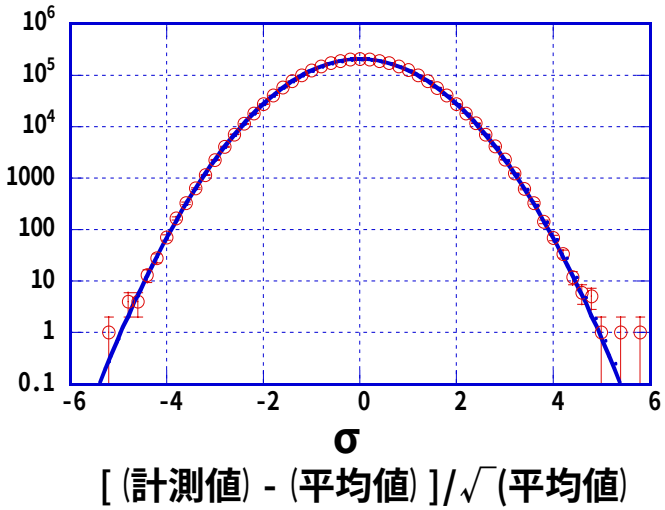
左図と同様の1Mカウントの計測を20万回繰り返したときの計測値と期待値 (**ポアッソン到達**) との比較

時間の計測　←　温度などの環境変化、回路の閾値などに依存しない。

特長1－2　一様性の保証



220Mバイトの8ビット乱数
頻度分布。
σ（偏差値）を右軸に示す。



左の220Mバイトの一様性の計測を
1万回（全データ量2.2×10^{12}バイト）
行ったときの偏差値（σ）分布。

特長2

生成速度：

USB：毎秒2Mバイト～16M バイト

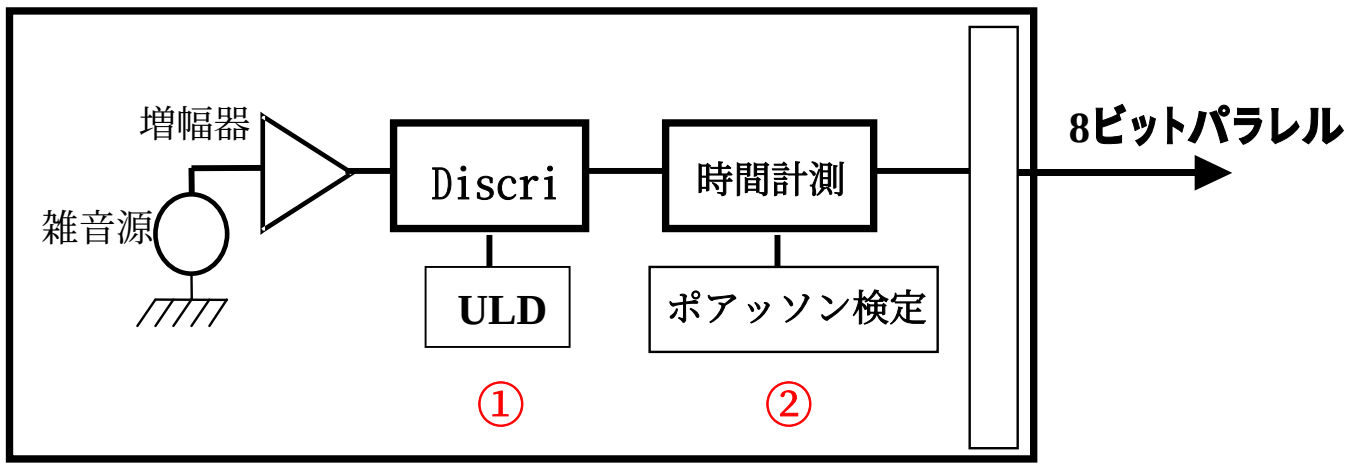
1/2PCIボード： 毎秒64M ～256M → 32PCクラスター(並列計算)
100万Lattice～150秒

要請 に応じて (接続方法に対応して)：
毎秒≧1Gバイト/ボード

サイズ：

ICカードCPU内：0.25mm×0.25 mm:～Mバイト
ICチップ：毎秒2Mバイト

GRNGのチェック機能



チェック①

故障や外的操作があれば、熱雑音に起因する電圧値を大きく超えるので、即（μ秒で）検知することができる。

チェック②

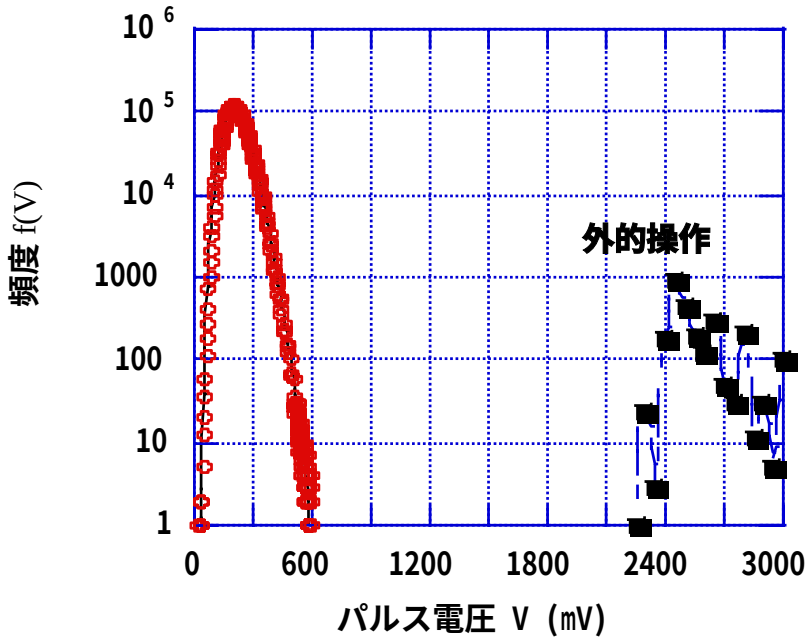
時間間隔の計測値とポアッソン到達を常時比較。

セキュリテイ用では、～ m秒で

シミュレーション用では数秒ごとに

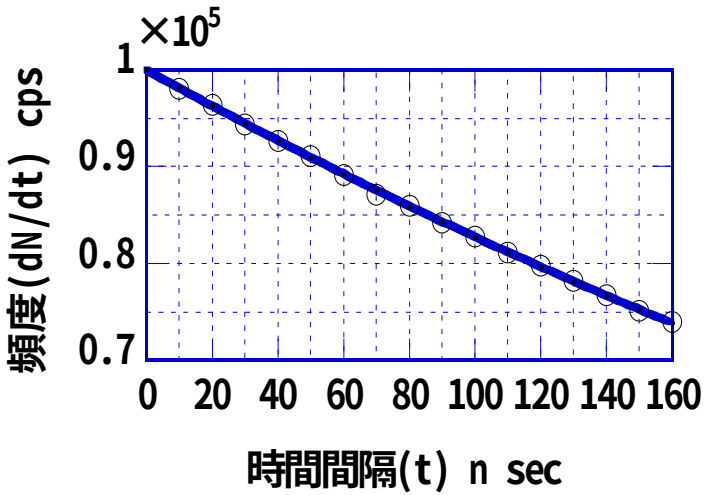
特長3

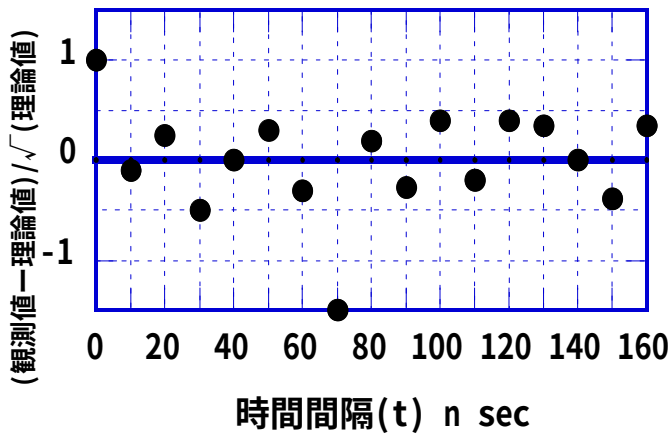
故障、外的攻撃・操作の瞬時検出



特長4

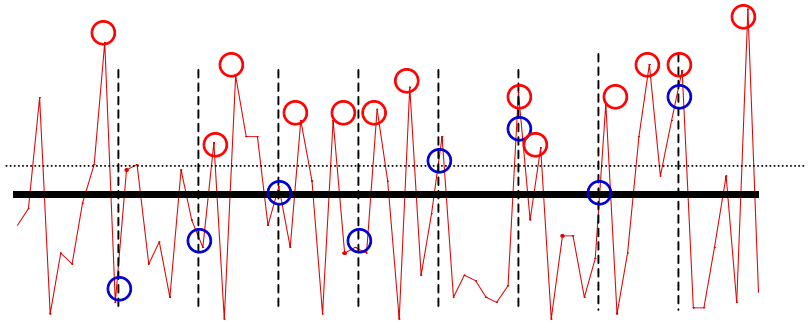
乱数性の常時自己検定

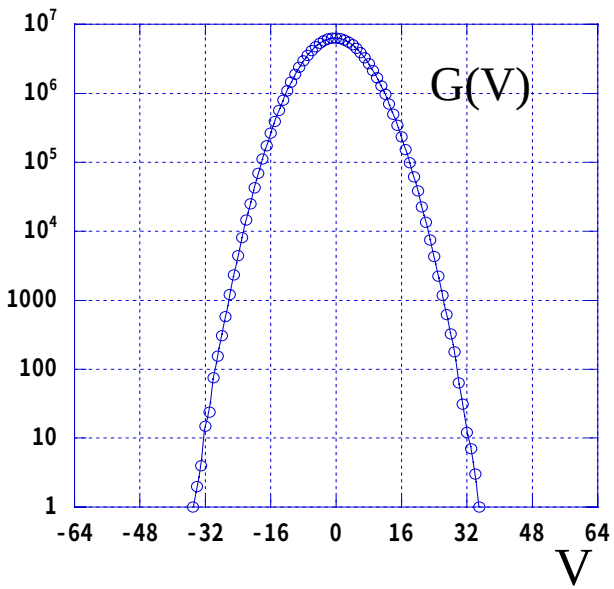


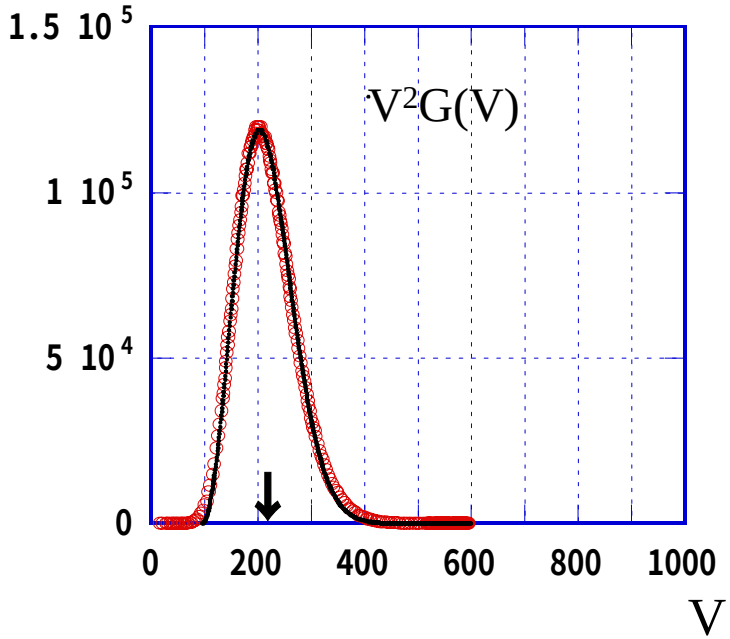


時間間隔tの計測値（図中◯）と
理論値（ポアッソン到達、exp[-t/T_0]）
とが常時比較されている。
データは1.6Gバイト(1秒間)。

故障や外的操作などにより、
計測値と期待値との差（偏差値）
が5σを超えた場合、乱数生成が
リセットされる。




G(V)
10^7
10^6
10^5
10^4
1000
100
10
1
-64 -48 -32 -16 0 16 32 48 64
V


$V^2G(V)$
1.5 10^5
1 10^5
5 10^4
0
0 200 400 600 800 1000
V