「RanSure(ランシュアー)」による乱数検定とトレーサブルな乱数(時刻)配信の新世代時刻認証への応用について

統計数理研究所　共同研究集会 物理乱数・擬似乱数の発生法・検定法とその周辺

独立行政法人　情報通信研究機構

梅野 健

2010年3月12日(金曜日)

Background

- 色々な物理乱数、カオス、暗号系が“乱数”として提案されている。

（例：本日午後の擬似乱数・物理乱数の講演）

- 課題：既存のカオスと乱数を区別する方法(例えば、リアプノフ指数、等)等は無力。参考：R. Takahashi, E. Nameda, K. Umeno, JSIAM Letters Vol. 2,pp.9-12 (2010).
- 目的：ランダム性の質を“計測”(Quantify)したい。
- 何か方法はあるのか？
- 応用：Traceable乱数の配信(NICT, NTP－＞NTRP標準時とともに)→標準乱数の探究

「RanSure」とは。

- ランダム性評価ソフトウェア
- できること：正しい乱数検定を誰もが
  簡単に実行可能。
- 製造メーカー：株式会社カオスウェア
  (NICT発ベンチャー,2003年設立）
- 国産ソフトウェア(販売開始:2005年)
- 2010.3.12現在のversion: 2.1（常に更新中）
- 適用OS：Windows 2000,XP,Vista,7(Soon)
- 内部(受託)評価用Linux版(本日リリース), LSI IP(2004)版もあり。

ランダム性の検定

- H_0：帰無仮説―
  テストする系列(データ）
  はランダムである。
- H_1：対立仮説―
  テストする系列(データ）
  はランダムでない。

2種類の検定エラー

- タイプIエラー：データがランダムである場合に、テストが帰無仮説H_0 を棄却する事象：（本当はランダムなのにランダムでないと判定される）

  ーその確率をα（有意水準:Significance Level)という。
- タイプIIエラー：データが非ランダムである場合に、テストが対立仮説H_1を棄却する事象：（本当は非ランダムなのにランダムだと判定される）ーその確率をβという。

乱数テストの設計

- β(タイプIIエラー確率)を小さくしたい。ただβの計算は非ランダムな事象は無限にあるので難しい。
- αは0.01もしくは0.001が使われる。

ランダム性検定テストのP-value (P-値）

- **完全な乱数生成器が、与えられたデータよりランダム性が低い系列を生成する確率**—P-value (P- **値**）

テスト結果の判定

- P-Value <α(=0.01 or 0.001)**の場合、データは非ランダムと判定。**
- P-Value ≧α(=0.01 or 0.001)**の場合、データはランダムと判定。**

P-value のP-value(P-値）

- P-valueも確率変数。適当な変換で
  任意のテストのP-valueが[0,1]に一様分布する。

P-Valueの一様性検定（x^2検定）

P-Value of P-Values <0.0001の場合、データは非ランダムと判定

The checking of the success rate

- The range of acceptable proportions:

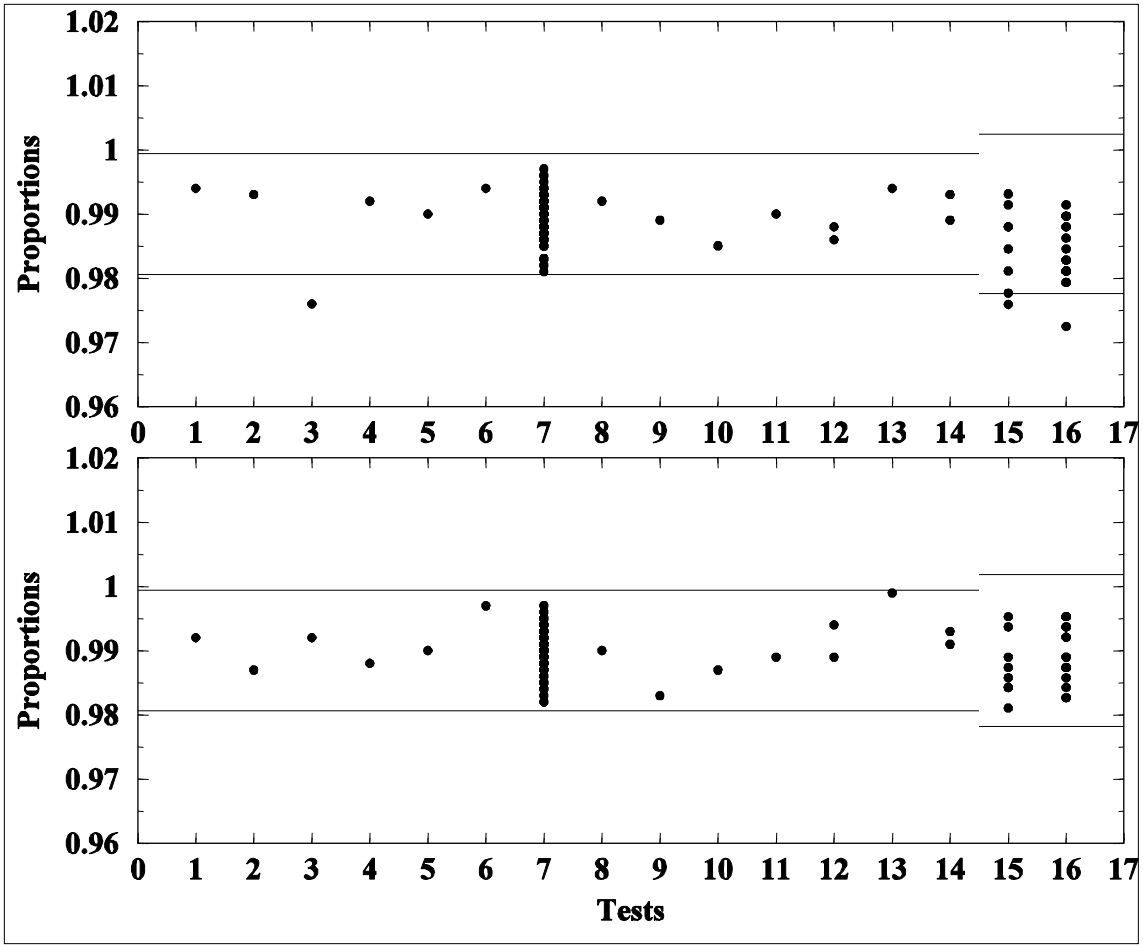
$$1-\alpha \pm 3\sqrt{\frac{\alpha(1-\alpha)}{m}}$$

※ (μ ±3σ)/m : 99.73% range of binomial distribution, where μ = m (1 − α) and σ = m α (1− α).
α =0.01: significance level

Success Rate (Example)

Key 1

Key 4



The checking of the uniformity of the P-values distribution

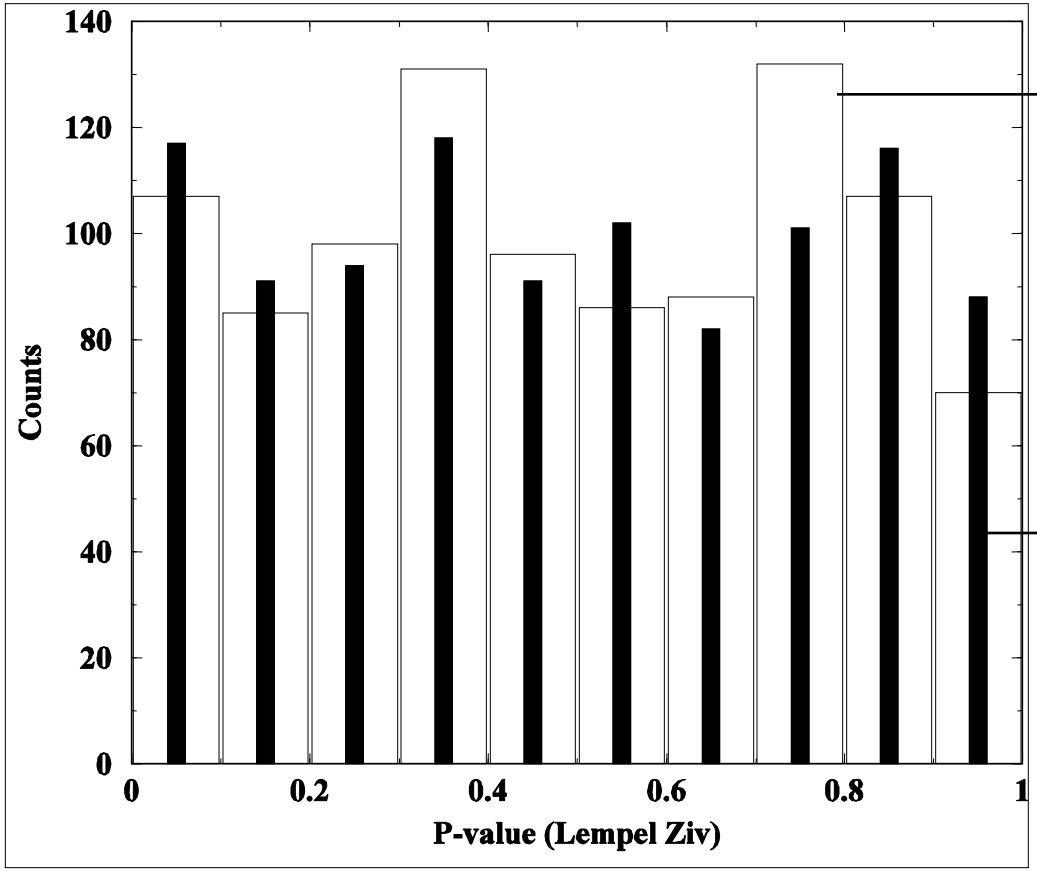
The interval [0,1] is divided into 10 sub intervals, and the p-values that lie within each sub-intervals are counted (F i).

p-value of p-values: IGMC(9 / 2, χ 2 / 2)

where IGMC(n, x) = $\frac{1}{\Gamma(n)} \int_x^\infty e^{-t} t^{n-1} dt$ and $\chi^2 = \sum_{i=1}^{10} \frac{(Fi - \frac{m}{10})^2}{\frac{m}{10}}$

The test passes if p-value of p-values ≥ 0.0001

Uniformity of p-values (Example)



Key 1 (fail)

Key 4 (pass)

The NIST Statistical Test Suite before 2004.12.9

"A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications"

National Institute of Standards and Technology (2001)

http://csrc.nist.gov/rng/

Number	Test Name
1	Frequency
2	Block Frequency
3	Runs
4	Longest Run
5	Binary Matrix Rank
6	Discrete Fourier Transform
7	Non-overlapping Template Matching
8	Overlapping Template 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

Summary of Our Revision to NIST SP 800-22 (2003.12) which affects NIST's revision on Dec. 9, 2004

- We corrected two points for DFT test.

  (1) the threshold T

$$\sqrt{3n} \longrightarrow \sqrt{2.995732274n}$$

  (2) the variance of the theoretical distribution

$$\sigma^2 = \frac{npq}{2} \longrightarrow \sigma^2 = \frac{npq}{4}$$

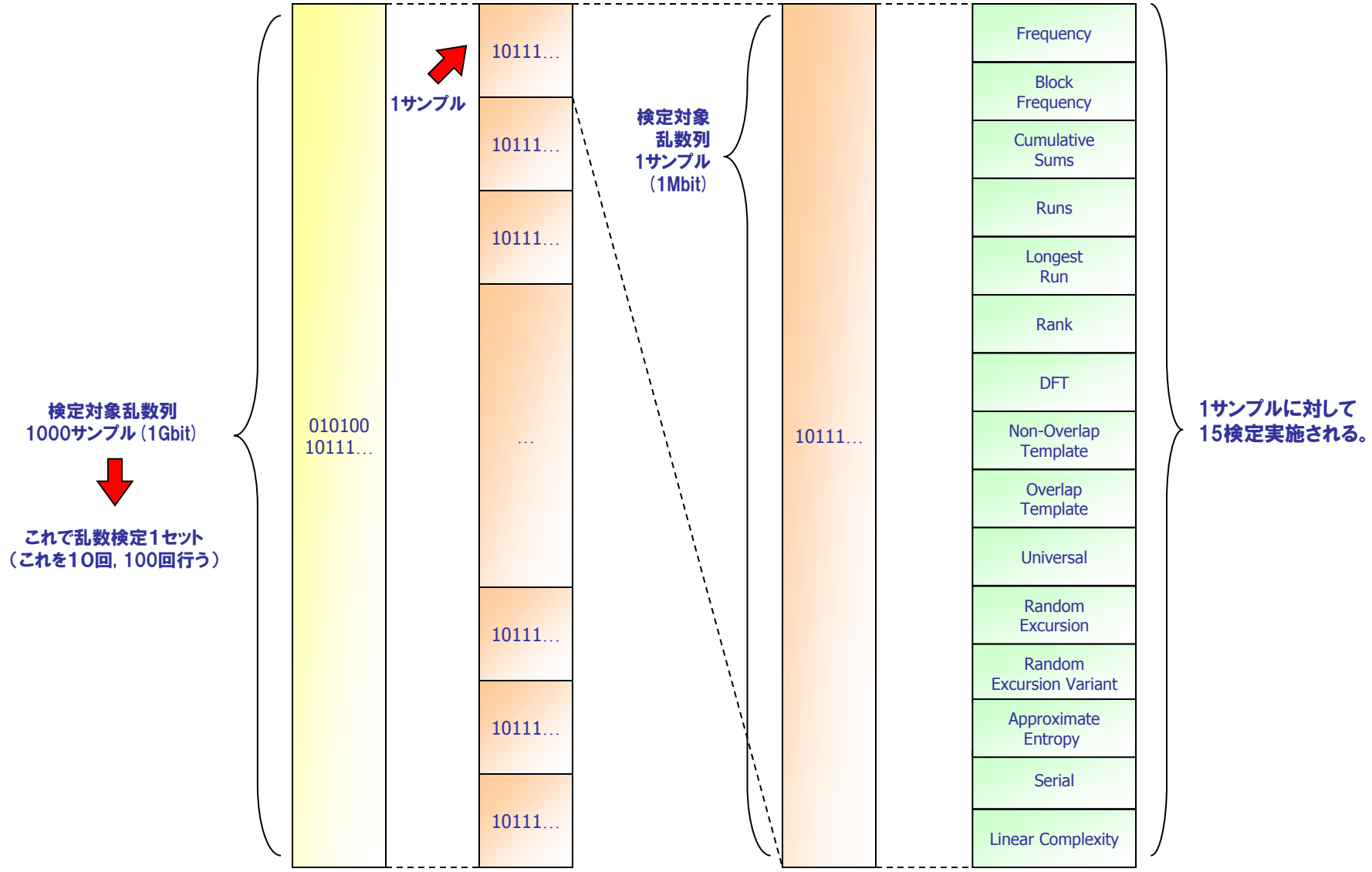
- We corrected two points for LZ test.

  (1) setting of standard distribution (asymmetric) which has no algorithm dependence.

  (2) re-definition of the uniformity of P-values.

Note: Kaneko(2004) also pointed out the incorrectness of the LZ test (CRYPTRET 2004 Report).

乱数検定概要(NIST SP 800-22 v.1.8 とRanSure v.2.1.)



The parameters we used

TEST NAME	BLOCK LENGTH
Block Frequency	20000
Template Matching	9
Universal	7
(Initialization Steps)	(1280)
Linear Complexity	500 (5000)
Serial	10
Approximate Entropy	10

$n=10^6$,

$\alpha=0.01$,

1000 samples

10 keysx1000 samplesx10^6 (sequence length)

total 10^10 bit

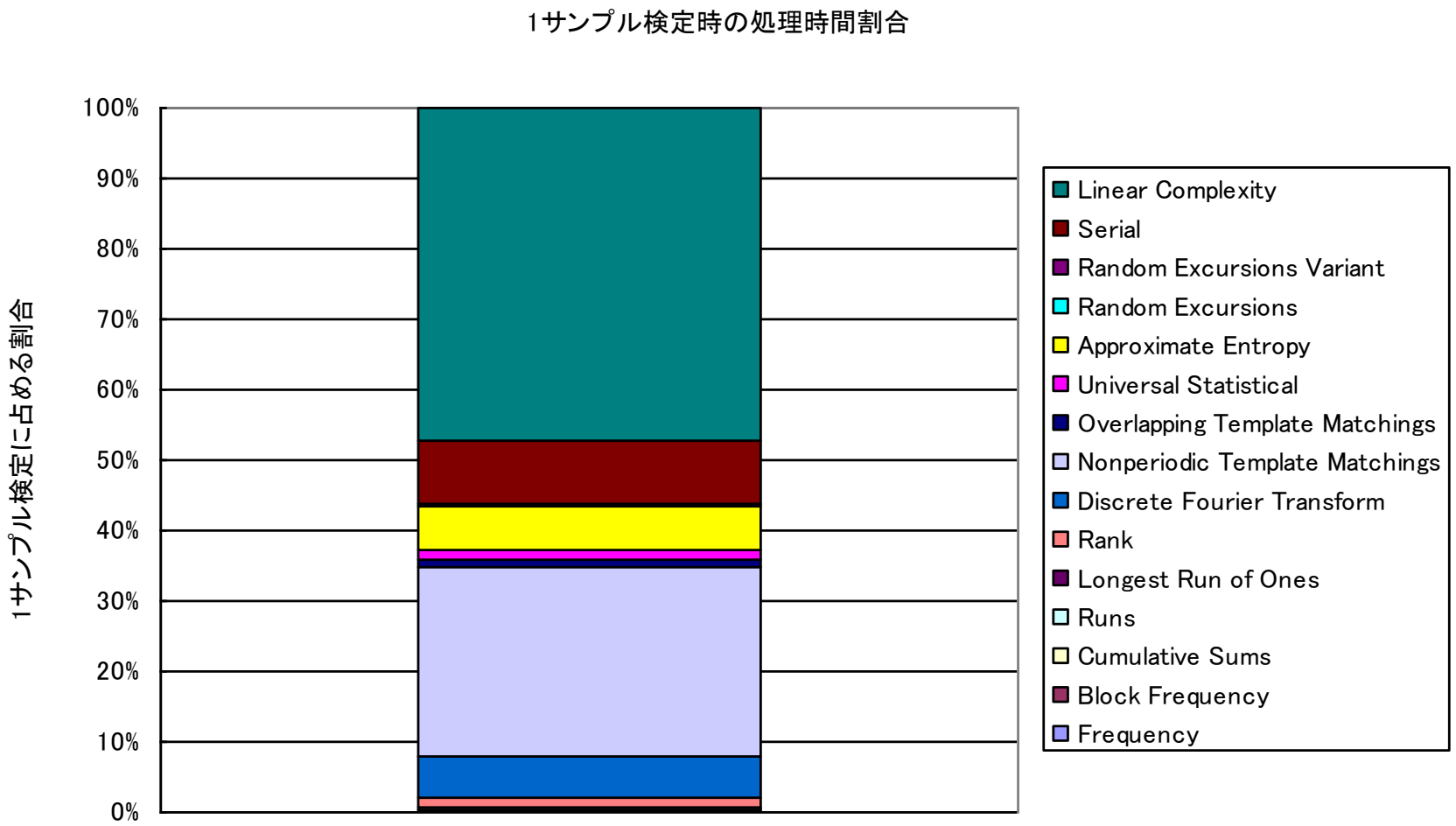
15検定それぞれに要する時間①

- 1サンプル(100万ビット)の乱数系列に対して15検定実施する際に要する検定時間を測定

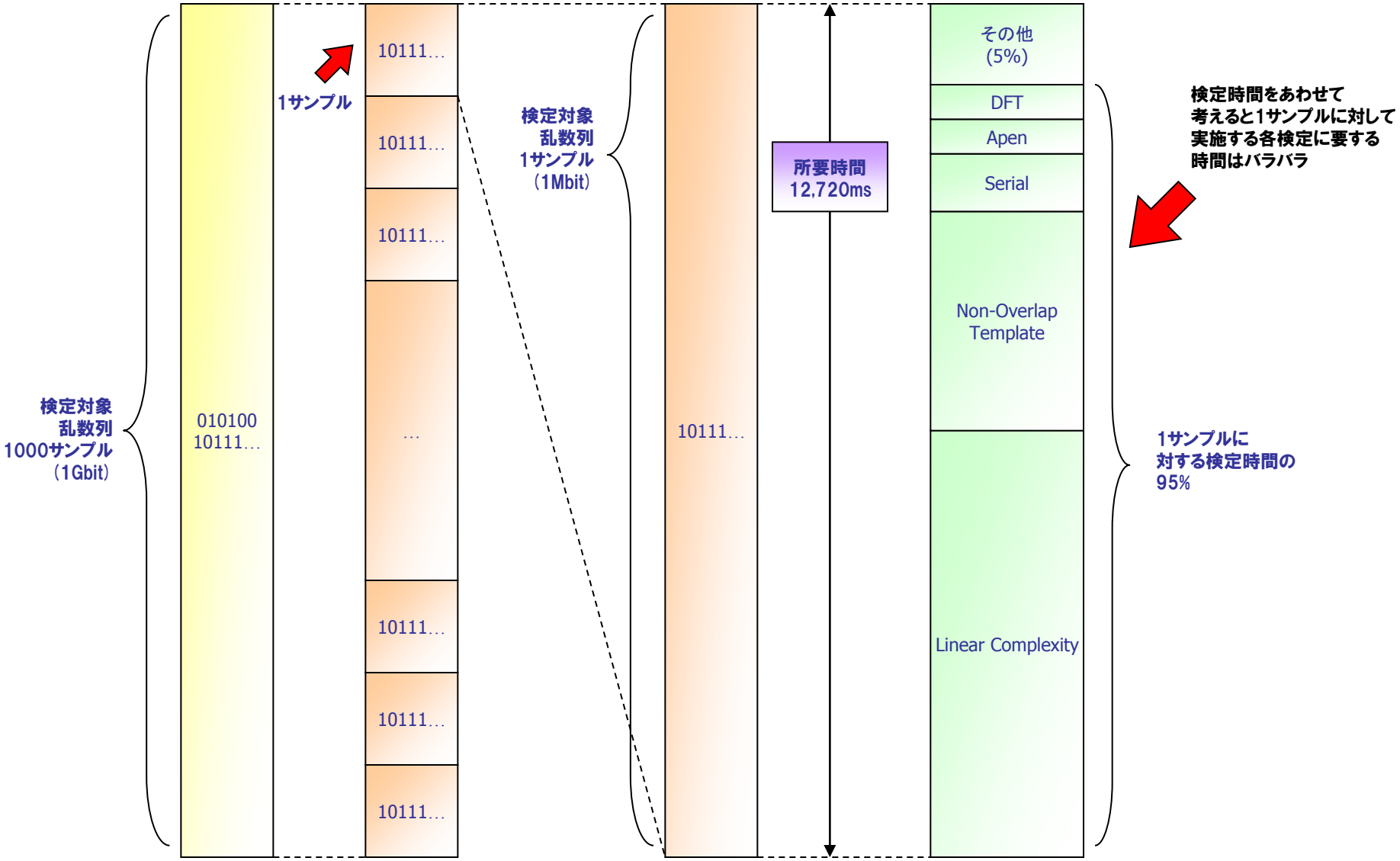
検定名	1サンプル検定時間 (ms)	検定時間割合
Frequency	10	0.08%
Block Frequency	10	0.08%
Cumulative Sums	30	0.24%
Runs	30	0.24%
Longest Run of Ones	10	0.08%
Rank	180	1.42%
Discrete Fourier Transform	740	5.82%
Nonperiodic Template Matchings	3430	26.97%
Overlapping Template Matchings	140	1.10%
Universal Statistical	140	1.10%
Approximate Entropy	810	6.37%
Random Excursions	10	0.08%
Random Excursions Variant	10	0.08%
Serial	1160	9.12%
Linear Complexity	**6010**	**47.25%**
合計	12720	100%

※ Linuxで実行
※ HP xw4300で稼動 (Intel(R) Pentium(R) 4 CPU 3.00GHz, Memory 512M)

15検定それぞれに要する時間②



乱数検定概要（検定に要する時間にあわせて図を修正）

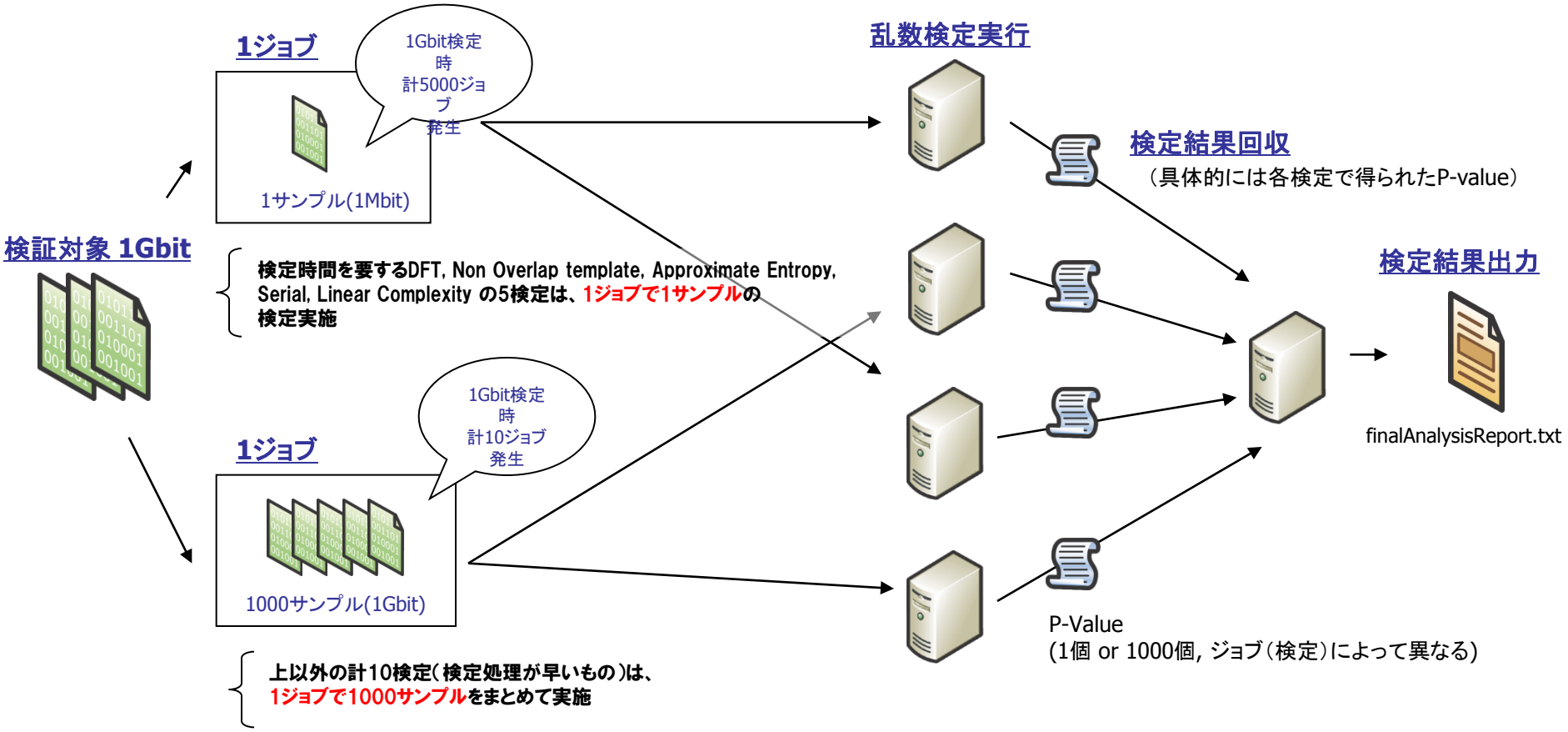


分散処理実装①-RanSure(ChaosWare)-

- **目標**
  - **1サンプル(1Mbit)に対して行う15検定に要する時間を短縮し、乱数検定1回分 1Gbit(1000サンプル, 1Gbit)の検定時間を可能な限り短くする**
    - **現状**
      - Pentium4 3.0GHz のPCで3時間程度

- **方法**
  - **検定対象の乱数列(1Gbit, 1000サンプル)を1000分割し、1サンプル毎に対して更に検定毎に処理を分割する。**
    (但し、特に検定時間を要するもののみ, 重くないものは1処理で1000サンプル分を処理する)

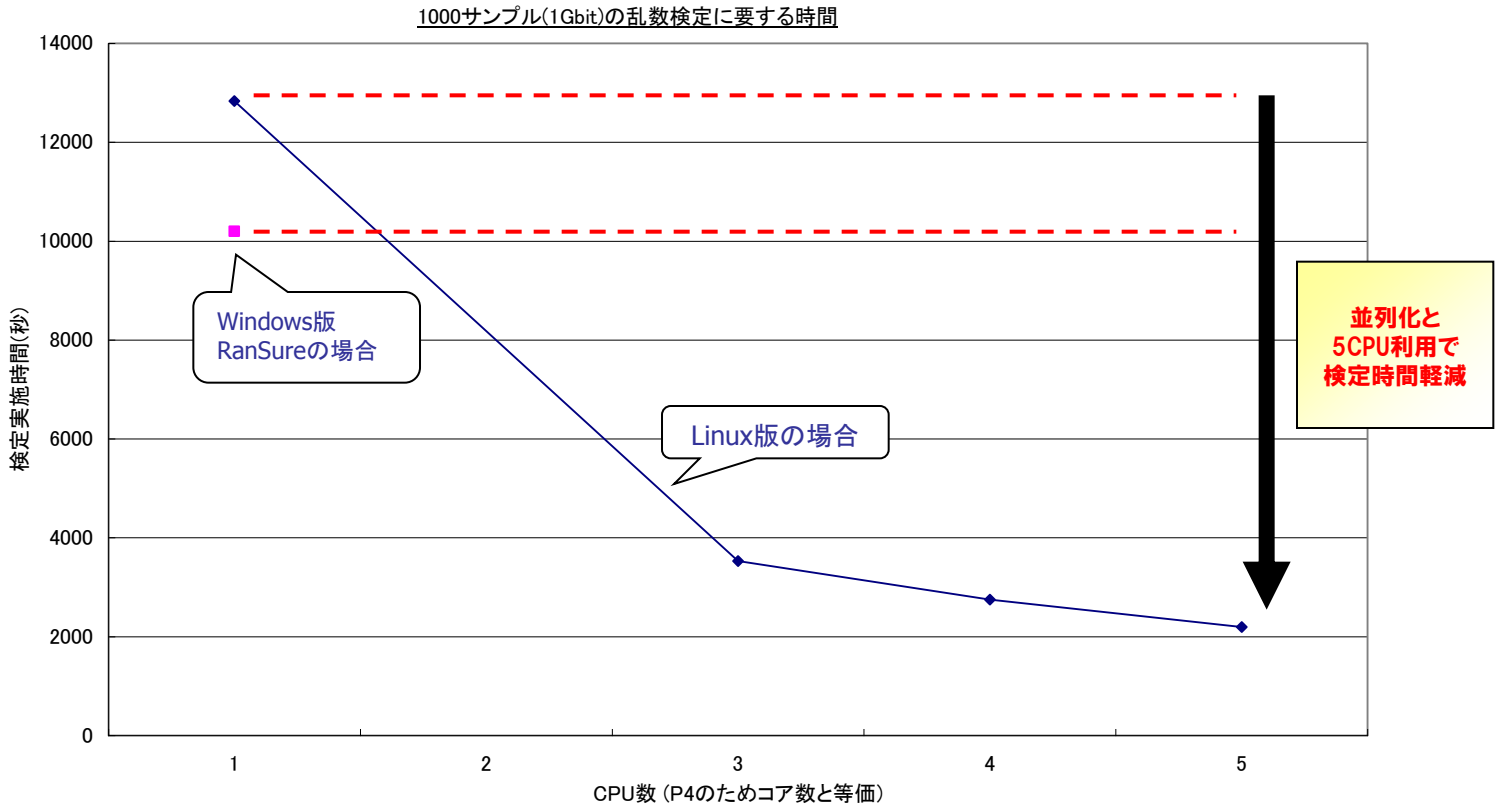
分散処理実装② -RanSure (ChaosWare)-



検定時間計測

- **条件**
  - 1000**サンプル**, 1Gbit**の乱数系列に対する乱数検定**(15**項目**)**に要する時間を測定**
- **条件**
  - **単体**
    - HP workstation xw4300 (Pentium4 3.0GHz)
  - **分散環境**
    - HP workstation xw4300 **を複数台でスケールさせる**(3～5CPU)

検定時間計測



- **実際はこれに更に20秒程度最終レポート出力時間が必要**
- **5CPU利用時で検定時間が**1/5
  → **36分で**1Gbit（**1000サンプル** × 100Mbit）**の検定完了**

各種暗号アルゴリズム別乱数検定

- **条件**
  - **独立した秘密鍵及びIVを100本準備し、1Gbit分の暗号化されたファイルを100ファイル用意**
  - 1Gbit(=1**ファイル**)を10**万ビット×1000サンプルとして**RanSure**を利用して乱数検定を実施する。**
- **検定対象アルゴリズム**
  - **カオス暗号**
    - VSC128S
  - eStream[*1]**推奨ソフトウェア向けストリーム暗号**
    - HC-128, Rabbit, Salsa20, SOSEMANUK
  - **ストリーム暗号, ブロック暗号**
    - blowfish, AES128, camellia, RC4, MUGI, KASUMI
  - **長周期擬似乱数生成機**
    - Mersenne twister
  - **物理乱数**
    - FDK**社製 高性能汎用物理乱数生成**ASIC RPG**シリーズ**

*1 eStreamについて
2004年2月に設立された欧州のEuropean Network of Excellence for Cryptology (ECRYPT) により立ち上げられたプロジェクト。
次世代ストリーム暗号の選定を目的としたストリーム暗号の評価プロジェクト。公募によって集まったアルゴリズムに対して
3年間にわたり評価及び選定が行われ、2008年3月に選定を終了。ソフトウェア用暗号4種類, ハードウェア用暗号3種類が選定された。

理想的な乱数をこのRanSureで評価すると、

- **1000回のRanSure評価で全てのテスト項目に合格する確率**

  （乱数性評価テストのメタテスト）＝51％

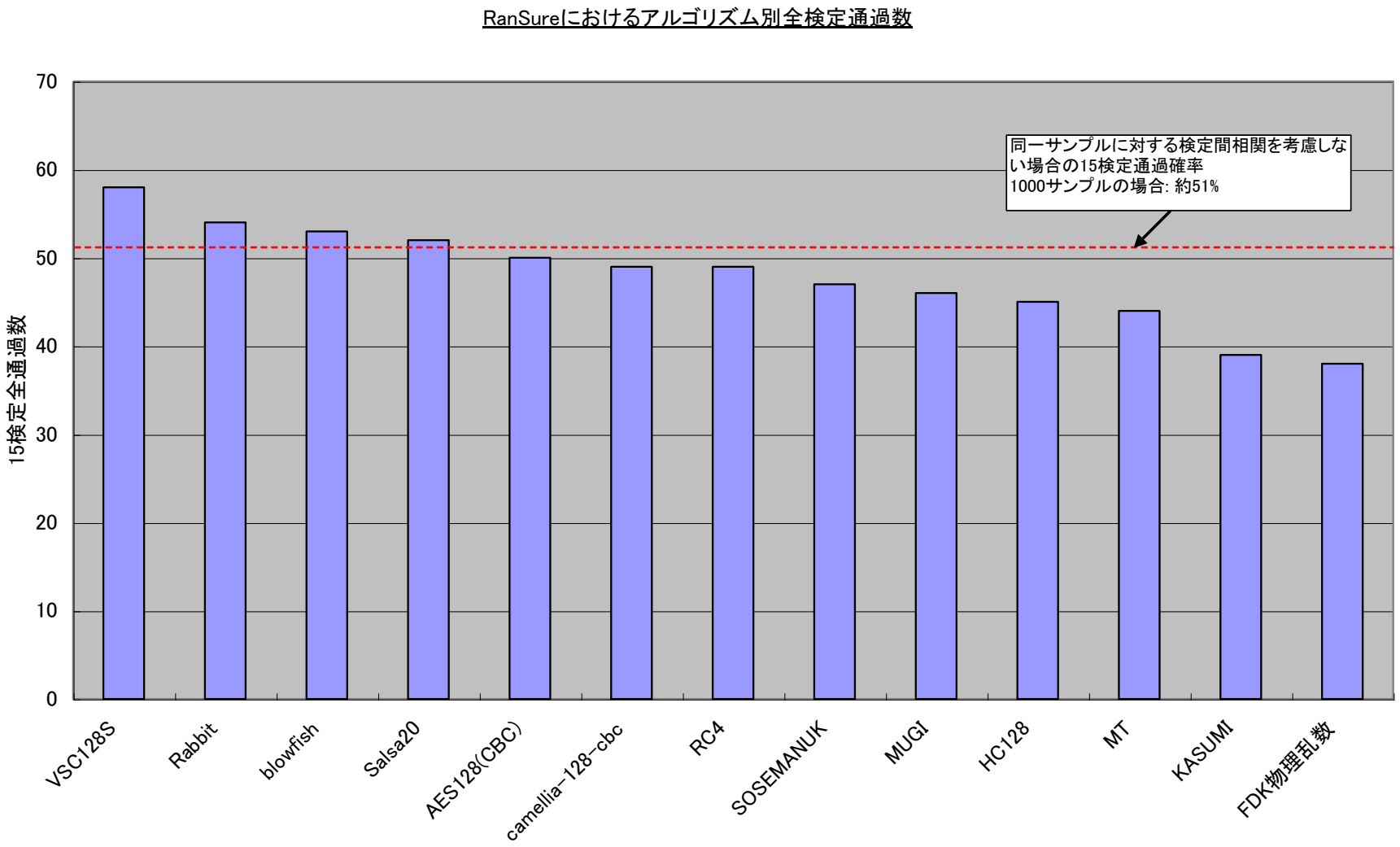
  （山口, 2009 応用数理学会年会)

仮定1：p-valueの分布の一様性

仮定2：各テストは独立。

51％という値は、仮定1及び仮定2の基でのモンテカルロシミュレーション結果

検定結果(100回の全パス回数)



示唆される結論：

- きちんと修正NIST SP 800-22とRanSureに理想化された乱数ビット(１回1Gbit)をかけると全パスする確率はコイン投げとほぼ同じで５１％。
- ー＞頑張ればいつかは全パスになってしまう。
- ー＞複数回テスト（メタ検定）の場合全パスする確率は、乱数・擬似乱数によって差がでる。ー＞質の評価に使えそうだ。

乱数性の3階層

1Gbit のRanSureテストで
１回は合格するが、１００回
以上(1000回推奨）のテストで５０％以上
合格する（合格率５０％以上の)クラス

1Gbit のRanSureテストで
１回は合格するが、１００回(1000回推奨)
以上のテストで５０％未満しか
合格しない（合格率０％より大きく
５０％未満の）クラス

1Gbit のRanSureテストで
一度も合格しないクラス

乱数性の3階層(テスト結果　2010.3.12現在)

VSC128S, Rabbit, Blowfish, Salsa20, AES128

Camellia 128, RC4, SOSEMANUK, MUGI, HC-128, MT, FDK ASIC-PRG(物理乱数), KASUMI(1000)

その他多くの擬似乱数・物理乱数

KASUMI暗号への集中検定

- KASUMI暗号（A5/3暗号）
  - 現在の3G携帯電話(W-CDMA)標準暗号
  - 基地局と移動局（携帯端末）間の電波の暗号化
    (LSIベースバンド処理で実装)

- 条件
  - 独立した秘密鍵及びIVを1000本準備し、1Gbit分の暗号化されたファイルを1000ファイル用意
  - 1Gbit（=1ファイル）を10万ビット×1000サンプルとしてRanSureを利用して乱数検定を実施する。

KASUMI暗号検定結果

- **テスト対象数** = 1000
  - 15**検定全パス数** = 470
  - 15**検定全パス率** = 47.00%
    - **分散** = 30.40
    - **標準偏差** = 5.51

今後ますます必要な乱数の研究

- 物理乱数・擬似乱数の乱数性(乱数Quality)の評価(特に大規模評価)
- 高速性(RanSureグリッド化)
- モンテカルロでモンテカルロを
- 良質な乱数生成メカニズムの研究
- 乱数のトレーサビリティ
- 乱数生成ビットレートの物理限界は？
- 乱数評価結果の共有.