国家密码管理局
商用密码检测中心

《随机性检测规范》概述

2013年5月

主要内容

一、制定规范的目的与意义

二、标准的制定与发布

三、标准的结构和主要内容

四、随机性检测技术概述

五、随机数样品的采集与检测

一、制定规范的目的与意义

- 随机数广泛应用于密钥生成、密码算法、安全协议等与信息安全密切相关的各个方面。
- 随机数发生器输出序列的随机性可保证系统结果的不可预测性，是保障信息保密性、完整性、可用性的基础。
- 随机性检测，是密码检测的一项基础性检测科目。其目的是检验密码模块或系统的随机数发生器是否能够产生符合密码学要求的随机数。密码产品、密码系统的检测，几乎都离不开对其随机数产生模块进行检测。

一、制定规范的目的与意义（续）

- 针对随机性检测，相关国际组织提供了尺度不一的随机数检测指标，例如：
  - FIPS140-1/2/3
  - SP800-22：NIST Statistical Test Suite
  - 欧洲新数字加密与签名计划NESSIE
  - 随机数软件包DIEHARD
  - 应用密码学手册 Handbook of Applied Cryptography
- 各类检测方法互不相同，缺乏对随机数检测的一致标准。
- 形成我国的随机性检测标准，形成统一的随机数检测项目及方法，是确保随机数发生器质量过关、服务随机数发生器设计与生产的重要举措。

主要内容

一、制定规范的目的与意义

二、标准的制定与发布

三、标准的结构和主要内容

四、随机性检测技术概述

五、随机数样品的采集与检测

二、标准的制定与发布

- 2005年3月14日，国家密码管理局和全国信息安全标准化技术委员会密码工作组（WG3）指定商用密码研究中心作为“随机性检测标准”的召集单位，组织完成随机性检测标准的起草工作。
- 为完成“随机性检测标准”的起草工作，商用密码研究中心联合信息安全国家重点实验室，成立课题组，课题组组长李大为，副组长冯登国，成员包括研究中心和实验室从事随机性检测方法研究和检测工作的主要人员，共同开展随机性检测标准的研究制定工作。

二、标准的制定与发布

- 2012年3月21日，国家密码管理局发布了第23号国家密码管理局公告，批准《随机性检测规范》在内的六项密码行业标准，自公布之日起实施。
- GM/T 0005-2012 《随机性检测规范》由国家密码管理局、中科院软件所合作起草。
- GM/T 0005-2012 《随机性检测规范》由国家密码管理局提出并归口。
- GM/T 0005-2012 《随机性检测规范》规定了商用密码应用中的随机性检测指标和检测方法，为随机性的评估提供科学依据，适用于对随机数发生器产生的二元序列的随机性检测。

主要内容

一、制定规范的目的与意义

二、标准的制定与发布

三、标准的结构和主要内容

四、随机性检测技术概述

五、随机数样品的采集与检测

三、规范的整体结构和主要内容

《随机性检测规范》按照GB/T1.1：2000标准的格式要求进行编写。整体结构包括：

前　言
引　言
1 范围
2 规范性引用文件
3 术语和定义
4 符号和缩略语
5 随机序列的检测
5.1 数据格式
5.2 显著性水平
5.3 参数设置
5.4 检测项目
5.5 结果分析
6 随机数发生器的检测
6.1 采样
6.2 存储
6.3 检测
6.4 分析
7 其它检测分析方法的应用
附录A （资料性附录） 概率统计基础知识
附录B （资料性附录） 随机性检测原理
附录C （资料性附录） 随机性检测参数设置表
附录D （资料性附录） 随机性检测结果分析表

三、规范的整体结构和主要内容

1) 单比特频数检测
Monobit Frequency test

2) 块内频数检测
Frequency test within a block

3) 扑克检测
Poker test

4) 重叠子序列检测
Serial test

5) 游程总数检测
Runs test

6) 游程分布检测
Runs distribution test

7) 块内最长游程检测
Test for the longest run of ones in a block

8) 二元推导检测
binary derivative test

9) 自相关检测
autocorrelation test

10) 矩阵秩检测
Binary matrix rank test

11) 累加和检测
Cumulative sums test

12) 近似熵检测
Approximate entropy test

13) 线性复杂性检测
Linear complexity test

14) Maurer通用统计检测
Maurer’s universal statiscal test

15) 离散傅里叶变换
Discrete fourier transform test

主要内容

一、制定规范的目的与意义

二、标准的制定与发布

三、标准的结构和主要内容

四、随机性检测技术概述

五、随机数样品的采集与检

理论基础
数据要求
检测项目原理
参数设置
合格判定

四、随机性检测方法概述

理论基础（一）

1、随机性检测的原假设

- 对二元序列做随机性检测时，首先假设该序列是随机的，这个假设称为原假设或零假设。与原假设相反的假设，即这个序列是不随机的，称为备择假设。
- 随机性检测的基础在于首先假设要进行随机性测试的序列均为随机序列。
- 对二元序列进行多种不同的随机性测试，若其中一项测试不通过，则原假设不成立，测试样本数据为非随机序列。
- 若在显著性水平为0.01的情况下通过测试，则有99%的把握认为该序列为随机序列。

五、随机性检测方法概述

理论基础（二）

2、概率统计

- 采用概率统计方式，针对不同的随机性特点进行统计，以统计值是否服从标准正态分布或已知自由度的χ2分布。测试统计值是为了计算P值（P值的大小体现了了源假设为假的可能性），即衡量样本随机性好坏的指标。
- If　P=1 → 良好的随机特性
- If　P=0 → 完全不是随机序列。
- If　P>=显著性水平a → 源假设是合理的
- If　P<a → 认为源假设不成立，序列非随机

四、随机性检测方法概述

理论基础（三）

3、显著性水平

- 显著性水平是指随机性检测中错误地判断某一个随机序列为非随机序列的概率 。
  - 显著性水平一般取0.05、0.01、0.005、0.001等。
  - 大量试验表明，当显著性水平取0.05时，许多随机性良好的数据也不能通过检验，从而使良好的随机数发生器也被判定为不合格。
  - 而取0.005或更低，将对样本的数量要求更高，不利于检测工作的开展。
  - 课题组经过权衡，选择取0.01。

四、随机性检测方法概述

数据要求

1、数据格式

- 待检数据以比特串的形式接受检测。

2、样本数量

- 用于随机性检测的二元序列，成为样本。
- 样本数量太小，则通过率的精度太低，容易错判结果。
- 样本数量太大，采集时间过长，也不利于检测工作的开展。
- 经过权衡，样本数量按照1/a来选择，即1000。

3、样本长度

- 样本长度是指一个样本的比特个数。
- 各检测项目均属统计项目，对样本长度均有一定要求。
- 样本长度太小，就可能会因为样本太少而产生较大的错判几率。
- 样本长度太大，采集时间过长，也不利于检测工作的开展。
- 经过权衡，样本长度要求统一为 10^6 比特。

四、随机性检测方法概述

检测方法及其原理（一）

- 对每一个样本按15项检测项目进行检测，分别得到每一个随机性检测项目的P值，记录这些结果。

	检测原理
矩阵秩检测	用序列构造矩阵，检测矩阵行列之间的线性独立性
累加和检测	最大累加和与随机序列应具有的最大偏移相比较
近似熵检测	比较m位与m+1位可重叠子序列模式的频数
线性复杂度检测	各等长子序列的线性复杂度分布应服从随机性要求
通用统计检测	检测待检序列是否可被无损压缩。
离散傅立叶检测	序列进行傅立叶变换后的尖峰高度是否超过门限值

四、随机性检测方法概述

检测方法及其原理（二）

	检测原理
单比特频数检测	检测待检序列中0和1的个数是否接近。
块内频数检测	m 位子序列中1的个数是否接近m/2 。
扑克检测	以m为长度划分序列，各类子序列的数量是否接近
重叠子序列检测	m位可重叠子序列的每一种模式的个数是否接近
游程总数检测	检测游程总数是否服从随机性要求。
游程分布检测	检测相同长度游程的数目是否接近一致。
块内最大“1”游程	N个等长子序列中最大1游程的分布是否规则。
二元推导检测	第K次二元推导序列中0和1的个数是否接近一致。
自相关检测	序列左移d位后所得新序列与原序列的关联程度。

四、随机性检测方法概述

■参数设置

	参数设置
块内频数检测	$m=100$
扑克检测	$m=4$ $m=8$
重叠子序列检测	$m=2$ $m=5$
块内最大1游程	$m=10000$
二元推导检测	$k=3$ $k=7$
自相关检测	$d=1$ $d=2$ $d=8$ $d=16$
矩阵秩检测	$M=Q=32$
近似熵检测	$m=5$
线性复杂度检测	$m=500$

四、随机性检测方法概述

- 合格判定
  - 对于每一个随机性检测项目，统计值P不小于显著性水平（表示该样本通过该项检测）的样本个数。
  - 按照公式 $p = 1 - \alpha \pm 3\sqrt{\frac{\alpha(1-\alpha)}{m}}$ ，当显著性水平取0.01时，通过率取0.98。
  - 当样本数量为1000个时，如果通过的样本个数不小于981，则随机数发生器通过此项检测；否则，未通过此项检测。

主要内容

一、制定规范的目的与意义

二、标准的制定与发布

三、标准的结构和主要内容

四、随机性检测技术概述

五、随机数样品的采集与

- 数据要求
- 采集方法
- 常见问题分析

随机数样品采集要求

随机数格式

- 生成的随机数以十六进制格式写入二进制文件中，如*.dat 或*. Bin等文件类型

名称	大小	类型	修改日期
1. dat	128 KB	DAT 文件	2013-3-5 12:48
2. dat	128 KB	DAT 文件	2013-3-5 12:48
3. dat	128 KB	DAT 文件	2013-3-5 12:48
4. dat	128 KB	DAT 文件	2013-3-5 12:48
5. dat	128 KB	DAT 文件	2013-3-5 12:48
6. dat	128 KB	DAT 文件	2013-3-5 12:48
7. dat	128 KB	DAT 文件	2013-3-5 12:48
8. dat	128 KB	DAT 文件	2013-3-5 12:48
9. dat	128 KB	DAT 文件	2013-3-5 12:48
10. dat	128 KB	DAT 文件	2013-3-5 12:48

随机数样品采集要求

随机数格式

- 生成的随机数以十六进制格式写入二进制文件中，如*.dat 或*. Bin等文件类型

```
00000000h: 43 31 20 FA 61 C7 45 88 1F 73 F9 55 0C F5 98 97 ; C1 鹞苔?s鹞.鳆?
00000010h: A2 F3 6E 29 43 F5 44 E9 DF 63 12 7E 2C D6 80 77 ; [lln)C鲀檬c.~,謤w
00000020h: E0 90 69 4F 14 AB 15 A7 61 F5 34 3B CA 17 6A D8 ; 鄯iO.?  ?;?j?
00000030h: A9 D6 80 90 AE 77 5C 77 EA DE C6 60 A9 F1 CB B0 ; ┰€悛w\w焚芙┐税
00000040h: 70 67 98 BC 63 D6 49 FF 82 C5 DC 40 B7 42 DA 00 ; pg椭c論  偭蹶稗?
00000050h: E5 1F 60 7F B5 1A D9 20 9F 1A B3 00 D0 A1 4D 22 ; ?` ????小M"
00000060h: F2 E7 D4 BA 27 E2 51 65 13 D4 7C EB 67 84 E2 F7 ; 蝉院'釷e.談雌勦?
00000070h: A5 C6 B4 70 10 FF EA D6 FB F2 8E 44 2C 0D FF E1 ; テ碘.  瞟  嶦,.
00000080h: 6F 94 A9 6E 07 BE 49 9F 15 78 85 BA CB F5 A8 3E ; o敍n.綱?x□缩?
00000090h: 1E 10 B4 87 96 82 7C 4D 7E 59 8F 1D F7 C5 35 11 ; ..碥松|M~Y?髓5.
000000a0h: 17 F9 27 3E 4D AB EF F9 08 7F C0 89 BA 58 7E 66 ; .?>M  ? 缘篠~f
000000b0h: BA 91 44 E7 0F E4 E5 95 E9 12 6F 91 DB 9C 31 6D ; 筷D?溴瞭.o慷?m
000000c0h: EF 37 22 48 AD 52 38 17 09 B4 C6 5D 68 49 40 5C ; ?"H瑒8..衅]hI@\
000000d0h: E8 54 E2 10 39 96 85 C5 0A 90 BD 20 C2 84 EE 5B ; 鑄?9粂?恍 閻糈
000000e0h: B8 AB 37 5B DD E9 49 40 BA EC C4 0C 11 2F A2 C5 ; 斧7[薯I@红?./(l)
000000f0h: FA 57 18 02 55 E3 67 1B BC 72 90 20 AE C8 EB 82 ; 鹘..U鉏.纫?  鼋
```

随机数样品采集要求

随机数格式

- 生成的随机数以十六进制格式写入二进制文件中，如*.dat 或*. Bin等文件类型

各类产品检测的随机数采样数据量：

	安全芯片	PCI、密码机	卡key	VPN	WAPI
样本数量	1000	1000	1000	1000	20
样本大小	128KB	128KB	64KB	128KB	64KB

随机数样本采集方法（一）

- （1）采用API接口采集随机数

代表产品：
PCI密码卡、密码机、芯片等

随机数样本采集方法（一）

- （1）采用

```
unsigned char *buff;

for (j=0;j<1000;j++)

{
    FILE *fp;
    CString file;
    z=j+1;
    file.Format("%d.dat",z);
    fp=fopen(file,"ab");

    for (k=0;k<1024;k++)

    {
        rv = SDF_GenerateRandom(hSessionHandle, 128, buff);

        if (rv != SDR_OK)
        {
            free(buff);
            err.Format("SDF_GenerateRandom Failed!!! Error: %#x!\r\n", rv);
            m_list.AddString(err);
            return ;
        }
        else
        {
            fwrite(buff,num1,1,fp);
            free(buff);
        }
    }
    fclose(fp);
}
```

1、新建二进制数据文件*.dat或*.bin，分别以数字顺序命名，如1.dat，2.dat，…

2、设置循环，每次调用API接口生成若干长度的随机数，依次写入文件中。最终形成一个大小为128KB的随机数样本文件。

随机数样本采集方法（一）

- （1）采用

```
unsigned char *buff;
for (j=0;j<1000;j++)
{
    FILE *fp;
    CString file;
    z=j+1;
    file.Format("%d.dat",z);
    fp=fopen(file,"ab");

    for (k=0;k<1024;k++)

    {

        rv = SDF_GenerateRandom(hSessionHandle, 128, buff);

        if (rv != SDR_OK)
        {
            free(buff);
            err.Format("SDF_GenerateRandom Failed!!! Error: %#x!\r\n", rv);
            m_list.AddString(err);
            return ;
        }
        else
        {
            fwrite(buff,num1,1,fp);
            free(buff);
        }
    }
    fclose(fp);
}
```

3、重复步骤1、2，循环生成1000个随机数样本文件

随机数样本采集方法（二）

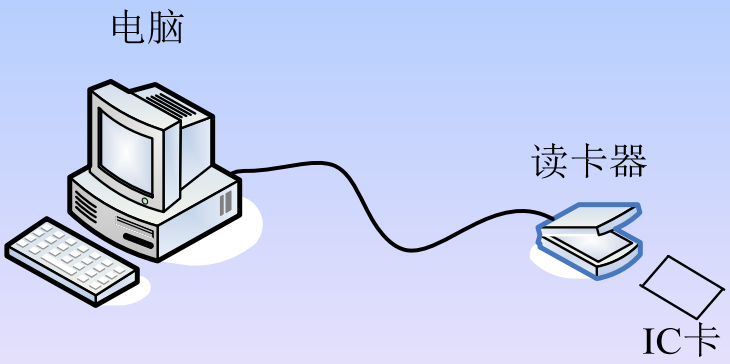
- （2）采用APDU指令采集随机数

代表产品：

安全芯片、智能IC卡、智能密码钥匙

随机数样本采集方法（二）

- （2）采用APDU指令采集随机数



读卡器与测试设备之间采用7816或14443协议通信，读卡器与电脑通过USB端口连接，数据采集平台对IC卡发送指令并采集被测样品返回的数据。

1）芯片上电复位，返回ATR，等待接受APDU指令；
2）采集平台发送取随机数APDU指令（如：00 84 00 00 10）；
3）测试设备接收取随机数指令，通过内部操作后返回16个字节随机数；
4）反复进行步骤2）和3），直至完成128M数据的采集；
5）过程2）、3）、4），直至生成1000个128M的随机数据。

随机数样本采集方法（三）

- （3）使用测试脚本采集随机数

代表实现：

- 智能密码钥匙/智能IC卡 COS检测

原理：

- 使用类VB语言发脚本组装、解析并发送APDU指令，在APDU指令的基础上增加了指令封装与解析的功能。

随机数样本采集方法（三）

```
For i= 0 To 999 Step 1
  fd = OpenFile(Random+i+".bin")
  For j=0 To File_size/once_write_File_len Step 1
    resp1 = ""
    For K=0 To once_write_File_len/once_get_Random_Len Step 1
      resp = CardTransmit("00840000"+AsHexString(2,once_get_Random_Len),"9000")
      Get_Random_Time=Get_Random_Time+GetTimeDiff(1)
      resp1 = resp1+Left(resp,len(resp)-4)
    Next
    offset=once_write_File_len*j
    WriteFileBin(fd,offset,resp1)
  Next
  CloseFile(fd)
```

1、依据样本数量要求设置循环数，用于生成所需数量的随机数文件

2、依据（所需样本大小÷每次可生成的随机数数量）设置二级循环次数。用于生成所需大小的各随机数样本文件

3、发送随机数生成指令，成果则返回9000

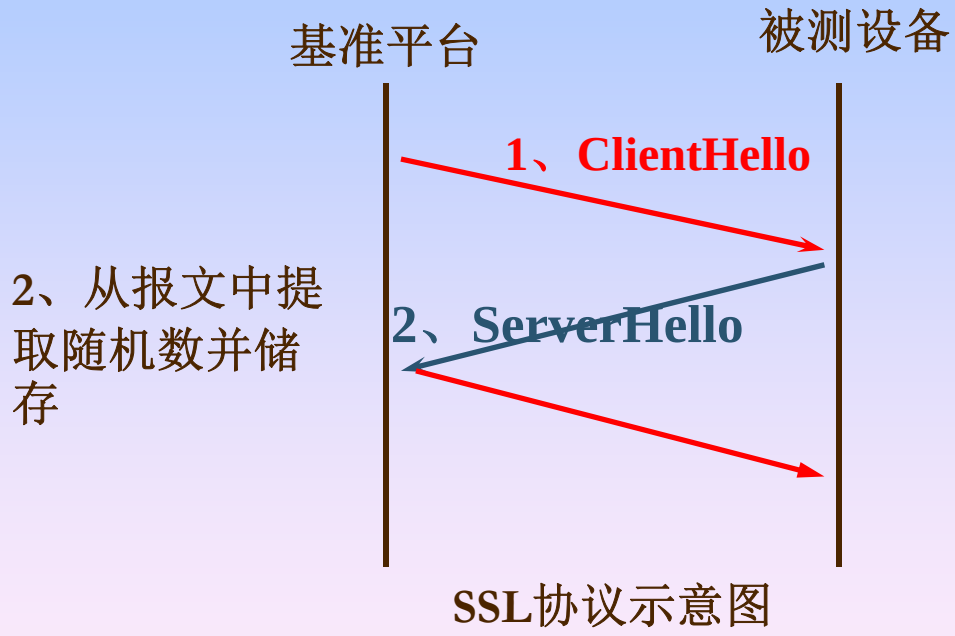
随机数样本采集方法（四）

- （4）通过网络协议过程采集随机数

代表产品：
WAPI、VPN、网卡、鉴别服务器等

随机数样本采集方法（四）

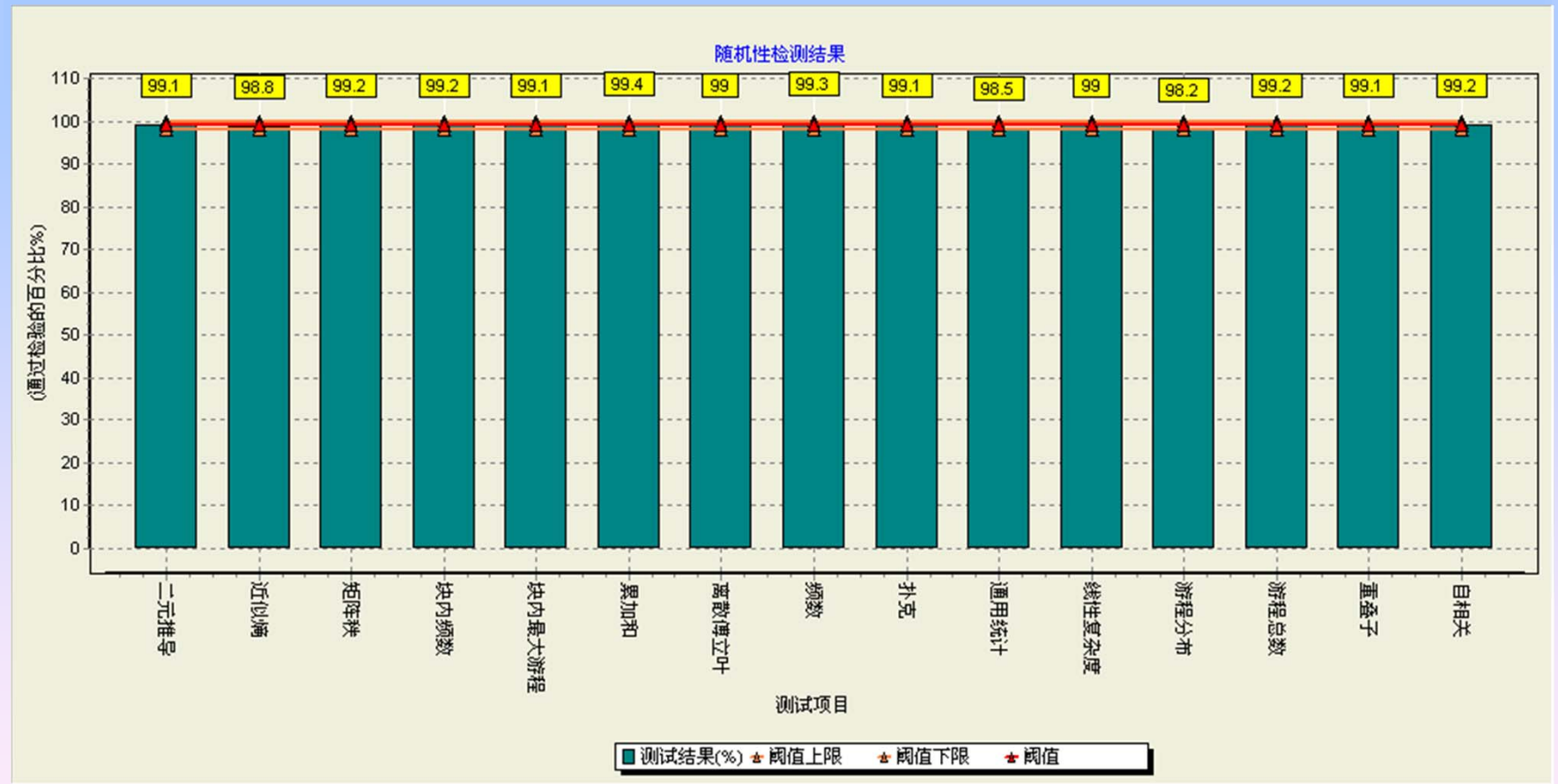
- （4）通过网络协议过程采集随机数



SSL协议示意图

3、关闭连接，再次建立SSL连接获取随机数，如此反复，直到接收到停止命令。集群控制服务器定时计算随机数的数量，发现达到需要的数量，则通知基准服务器的所有模拟客户端停止收集。

随机数检测结果与常见问题分析



随机数检测结果与常见问题分析

不通过分析

检测项目	不通过分析
单比特频数检测	说明0或1个数过小
块内频数检测	位子序列中0、1比例不均衡
扑克检测	有某个或者某几个子序列的个数过多或过少
重叠子序列检测	的可重叠子序列模式分布不均匀
游程总数检测	说明序列中元素变化过快或者过慢。
游程分布检测	相同长度的游程数目分配不均匀
块内最大“1”游程检测	待检序列中有很多成簇的1或者0
二元推导检测	序列中0、1变化得过慢
自相关检测	序列具有较强的自相关性
矩阵秩检测	秩分布差别比较大
累加和检测	说明待检序列头部有过多的0或1
近似熵检测	待检序列具有较强的规则性
线性复杂度检测	子序列线性复杂度分布不规则
通用统计检测	待检序列可大幅度地被压缩
离散傅立叶检测	太多傅立叶变换的尖峰高度超过门限值

随机数检测常见问题分析

随机数检测常见缺陷/故障：

（1）初始序列不随机

- 随机数发生器启动初期可能输出若干固定或有规律的数字序列。

（2）时序设计不合理

- 时钟频率过高或过低均可能引起输出序列不随机。

（3）器件故障

- 因电容、电阻等器件虚焊、击穿等引起的随机数样品不合格。

欢迎各位批评指正！