ICS 35.040
L 80
备案号:36832—2012

GM

中华人民共和国密码行业标准

GM/T 0005—2012

随机性检测规范

Randomness test specification

2012-03-21 发布　　2012-03-21 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅰ
1　范围 …… 1
2　术语和定义 …… 1
3　符号和缩略语 …… 3
4　二元序列的检测 …… 4
4.1　数据格式 …… 4
4.2　显著性水平 …… 4
4.3　样本长度 …… 4
4.4　检测项目 …… 4
4.5　结果分析 …… 8
5　随机数发生器的检测 …… 8
5.1　采样 …… 8
5.2　存储 …… 8
5.3　检测 …… 9
5.4　判定 …… 9
附录A（资料性附录）　随机性检测原理 …… 10
A.1　单比特频数检测 …… 10
A.2　块内频数检测 …… 10
A.3　扑克检测 …… 10
A.4　重叠子序列检测 …… 10
A.5　游程总数检测 …… 11
A.6　游程分布检测 …… 11
A.7　块内最大“1”游程检测 …… 11
A.8　二元推导检测 …… 12
A.9　自相关检测 …… 12
A.10　矩阵秩检测 …… 13
A.11　累加和检测 …… 13
A.12　近似熵检测 …… 13
A.13　线性复杂度检测 …… 14
A.14　Maurer通用统计检测 …… 14
A.15　离散傅立叶检测 …… 15
附录B（资料性附录）　随机性检测参数设置表 …… 16
附录C（资料性附录）　随机性检测结果分析表 …… 17

前　言

本标准依据 GB/T 1.1—2009 给出的规则起草。

本标准对随机性检测进行规范，为随机性的评估提供科学依据。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准的附录 A、附录 B 和附录 C 是资料性附录。

本标准由国家密码管理局提出并归口。

本标准起草单位：国家密码管理局商用密码检测中心、中国科学院软件研究所。

本标准主要起草人：李大为、冯登国、陈华、张超、周永彬、董芳、范丽敏、许囡囡。

随机性检测规范

1 范围

本标准规定了商用密码应用中的随机性检测指标和检测方法。

本标准适用于对随机数发生器产生的二元序列的随机性检测。

2 术语和定义

下列术语和定义适用于本文件。

2.1

二元序列 binary sequence

由“0”和“1”组成的比特串。

2.2

随机数发生器 random number generator

产生随机序列的设备或程序称为随机数发生器。

2.3

随机性假设 randomness hypothesis

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，记为 H_0。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，记为 H_α。

2.4

随机性检测 randomness test

用于二元序列检测的一个函数或过程，可以通过它来判断是否接受随机性原假设。

2.5

显著性水平 significance level

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，用 α 来表示。

2.6

样本 sample

用于随机性检测的二元序列，称为样本。

2.7

样本长度 sample length

一个样本的比特个数。

2.8

样本数量 sample size

随机性检测的样本的个数。

2.9

检测参数 test parameter

随机性检测需要设定的参数。

2.10

***P* 值 *P*-value**

一种衡量样本随机性好坏的度量指标。