ICS 35.040
L 80

中华人民共和国国家标准

GB/T 32915—2016

信息安全技术
二元序列随机性检测方法

Information security technology—Randomness test methods for binary sequence

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　术语和定义 …… 1
3　符号 …… 2
4　随机性检测 …… 3
4.1　单比特频数检测方法 …… 3
4.1.1　概述 …… 3
4.1.2　检测步骤 …… 3
4.1.3　结果判定 …… 3
4.2　块内频数检测方法 …… 3
4.2.1　概述 …… 3
4.2.2　检测步骤 …… 3
4.2.3　结果判定 …… 3
4.3　扑克检测方法 …… 4
4.3.1　概述 …… 4
4.3.2　检测步骤 …… 4
4.3.3　结果判定 …… 4
4.4　重叠子序列检测方法 …… 4
4.4.1　概述 …… 4
4.4.2　检测步骤 …… 4
4.4.3　结果判定 …… 5
4.5　游程总数检测方法 …… 5
4.5.1　概述 …… 5
4.5.2　检测步骤 …… 5
4.5.3　结果判定 …… 5
4.6　游程分布检测方法 …… 5
4.6.1　概述 …… 5
4.6.2　检测步骤 …… 5
4.6.3　结果判定 …… 6
4.7　块内最大“1”游程检测方法 …… 6
4.7.1　概述 …… 6
4.7.2　检测步骤 …… 6
4.7.3　结果判定 …… 6
4.8　二元推导检测方法 …… 6
4.8.1　概述 …… 6
4.8.2　检测步骤 …… 6
4.8.3　结果判定 …… 7

4.9 自相关检测方法 …… 7
4.9.1 概述 …… 7
4.9.2 检测步骤 …… 7
4.9.3 结果判定 …… 7
4.10 矩阵秩检测方法 …… 7
4.10.1 概述 …… 7
4.10.2 检测步骤 …… 7
4.10.3 结果判定 …… 8
4.11 累加和检测方法 …… 8
4.11.1 概述 …… 8
4.11.2 检测步骤 …… 8
4.11.3 结果判定 …… 8
4.12 近似熵检测方法 …… 8
4.12.1 概述 …… 8
4.12.2 检测步骤 …… 8
4.12.3 结果判定 …… 9
4.13 线性复杂度检测方法 …… 9
4.13.1 概述 …… 9
4.13.2 检测步骤 …… 9
4.13.3 结果判定 …… 10
4.14 Maurer 通用统计检测方法 …… 10
4.14.1 概述 …… 10
4.14.2 检测步骤 …… 10
4.14.3 结果判定 …… 10
4.15 离散傅立叶检测方法 …… 10
4.15.1 概述 …… 10
4.15.2 检测步骤 …… 10
4.15.3 结果判定 …… 11
5 随机数发生器检测 …… 11
5.1 随机数发生器检测概述 …… 11
5.2 采集 …… 11
5.3 检测 …… 11
5.4 判定 …… 11
附录 A（资料性附录） 随机性检测原理 …… 12
附录 B（资料性附录） 随机性检测参数设置表 …… 19

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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。

本标准由国家密码管理局提出。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)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、北京信息科学技术研究院。

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、邓开勇、罗鹏。

信息安全技术
二元序列随机性检测方法

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

产生随机二元序列的器件或程序。

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_a。

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。