ICS 35.040
CCS L 80

# 中华人民共和国国家标准

GB/T 32915—2026
代替 GB/T 32915—2016

# 网络安全技术
# 二元序列随机性检测方法

**Cybersecurity technology—Randomness test methods for binary sequence**

2026-05-25 发布　　2026-12-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

# 目　　次

# 前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 32915—2016《信息安全技术　二元序列随机性检测方法》，与 GB/T 32915—2016 相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了术语“样本集”及其定义（见 3.6），删除了术语“随机数发生器”及其定义（见 2016 年版的 2.2）；

b) 增加了符号 $\alpha_T$、$Q\_value$ 的说明（见第 4 章），删除了符号 $H_0$、$H_a$ 的说明（见 2016 年版的第 3 章），更改了符号 $\alpha$、$P\_value$ 的说明（见第 4 章，2016 年版的第 3 章）；

c) 增加了 $Q\_value$ 的计算步骤（见 5.2～5.16）；

d) 更改了游程分布检测的检测步骤（见 5.7.2，2016 年版的 4.6.2、附录 A 的 A.6）；

e) 增加了块内最大“0”游程检测模式（见 5.8）；

f) 增加了后向累加和检测模式（见 5.12）；

g) 更改了离散傅里叶检测方法在计算统计值 $V$ 时使用的参数（见 5.16.2，2016 年版的 4.15.2）；

h) 增加了对 $Q\_value$ 的样本分布均匀性判定要求（见第 6 章），将“随机数发生器的检测”更改为“随机性检测判定”（见第 6 章，2016 年版的第 5 章）；

i) 增加了“样本长度及检测设置”（见附录 A）。

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专利的责任。

本文件由全国网络安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：商用密码检测认证中心、中国科学院软件研究所、中国科学院信息工程研究所、兴唐通信科技有限公司、清华大学、北京海泰方圆科技股份有限公司、安徽问天量子科技股份有限公司、北京宏思电子技术有限责任公司、北京银联金卡科技有限公司、中电科网络安全科技股份有限公司、鼎铉商用密码测评技术（深圳）有限公司、中国电子信息产业集团有限公司第六研究所、智巡密码（上海）检测技术有限公司、北京中电华大电子设计有限责任公司、中电信量子信息科技集团有限公司、郑州信大捷安信息技术股份有限公司、华为技术有限公司、深圳市纽创信安科技开发有限公司。

本文件主要起草人：毛颖颖、雷银花、陈华、范丽敏、马原、孙晓峰、贾文义、罗鹏、曹伟琼、贾珂婷、罗影、凌杰、刘婧婧、张文婧、张贺、李亚威、李峥、牛路宏、邓开勇、张运理、吕娜、陈天宇、侯庆良、王提、李昆桦、黄佩达、纪爽、张雪、李寅霜、吕竹青、王紫涵、赵礼鹏、蓝建春、凌杭、胡之斐、王龙、王子涛、匡云、陈启明、刘戬、刘勇、朱迪、梁松涛、曾光、王宗岳、刘晨、邹超。

本文件及其所代替文件的历次版本发布情况为：

——2016 年首次发布为 GB/T 32915—2016；

——本次为第一次修订。

# 网络安全技术
# 二元序列随机性检测方法

## 1 范围

本文件描述了二元序列的随机性检测方法，包括检测目的、检测步骤、参数设置和结果判定。

本文件适用于网络安全领域二元序列随机性检测。

## 2 规范性引用文件

本文件没有规范性引用文件。

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**二元序列 binary sequence**

由“0”和“1”组成的比特串。

注：简称“序列”。

3.2

**随机性假设 randomness hypothesis**

关于待检二元序列随机性的假设，可基于随机性检测结果来选择接受或拒绝该假设。

注：本文件假设待测二元序列是随机的，称为原假设或零假设。

3.3

**随机性检测 randomness test**

用于二元序列检测的一个函数或过程，其结果用以判断是否接受原假设。

3.4

**显著性水平 significance level**

随机性检测中，当原假设为真时，错误地拒绝原假设的概率。

3.5

**样本 sample**

用于随机性检测的二元序列。

注：也称为“待检序列”。

3.6

**样本集 sample group**

多个样本的集合。

3.7

**样本长度 sample length**

样本的比特个数。