ICS 35.040
L 80
备案号:62997—2018

中华人民共和国密码行业标准

GM/T 0062—2018

密码产品随机数检测要求

Random number test requirements for cryptographic modules

2018-05-02 发布　　2018-05-02 实施

国家密码管理局　　发布

中华人民共和国密码
行业标准
密码产品随机数检测要求
GM/T 0062—2018
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2018年9月第一版
*
书号:155066·2-44885

版权专有　侵权必究

目　　次

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。

本标准由密码行业标准化技术委员会提出并归口。

本标准主要起草单位：北京宏思电子技术有限责任公司、国家密码管理局商用密码检测中心、中国科学院数据与通信保护研究教育中心、中国科学院软件研究所、北京中电华大电子设计有限责任公司、国民技术股份有限公司、北京三未信安科技发展有限公司、天地融科技股份有限公司。

本标准主要起草人：张文婧、罗鹏、郁群慧、范丽敏、夏鲁宁、陈华、李丹、杨贤伟、高志权、李国阳。

引　言

随机数在密码应用中发挥着极其重要的作用，例如密码算法里的密钥要求是随机数，另外许多密码协议的中间过程也需要随机数。

随机数发生器是指产生随机数的专用集成器件或者器件中的随机数生成部件。

使用随机数发生器产生随机数时，随机数的好坏对于保障整个系统的安全性举足轻重。本标准将随机数检测划分为A类、B类、C类、D类和E类五个不同产品形态，对每个产品形态的随机数检测划分为送样检测、出厂检测、上电检测、使用检测四个不同应用阶段，并对每种产品形态的各应用阶段提出了随机数检测要求。

密码产品随机数检测要求

1 范围

本标准规定了密码产品应用中，硬件实现随机数发生器产生随机数的随机性检测指标和检测要求。

本标准适用于随机数发生器的检测，亦可指导随机数发生器的研制。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 32915 信息安全技术 二元序列随机性检测方法

3 术语、定义和符号

3.1 术语和定义

GB/T 32915 界定的以及下列术语和定义适用于本文件。

3.1.1

送样检测 sample test

厂商产品样本交由第三方检测机构进行的产品随机性检测。

3.1.2

出厂检测 delivery test

由厂家在产品出厂前进行的产品随机数功能和质量检测。

3.1.3

上电检测 power on test

产品加电时自动进行的随机数功能检测。

3.1.4

使用检测 running test

产品工作过程中自动进行的随机数功能检测，使用检测分为周期检测和单次检测。

3.1.5

周期检测 cyclical test

产品工作过程中按照一定的时间间隔自动进行的随机数功能检测。

3.1.6

单次检测 single test

产品工作过程中随机数每次使用前自动进行的随机数功能检测。

3.2 符号

下列符号适用于本文件。

α 显著性水平

m 扑克检测的分组长度