ICS 35.040
L 80
备案号:62997—2018

GM

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.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 0.75 字数 16 千字
2018年9月第一版 2018年9月第一次印刷
*
书号:155066·2-44885 定价 18.00 元

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

4 随机数检测说明

4.1 产品形态划分

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类别。

A类产品的主要特征为不能独立作为功能产品使用；典型产品形态为随机数发生器芯片等。

B类产品的主要特征为用时上电，随机数检测处理能力有限，对上电响应速度有严格要求；典型产品形态为IC卡等。

C类产品的主要特征为用时上电，随机数检测处理能力有限，对上电响应速度没有严格要求；典型产品形态为USBKey等。

D类产品的主要特征为长期加电，随机数检测处理能力有限，对上电响应速度没有严格要求；典型产品形态为POS机等。

E类产品的主要特征为长期加电，具有较强的随机数检测处理能力，对上电响应速度没有要求；典型产品形态为服务器等。

本标准对每种产品形态提出了随机数检测要求。

4.2 应用阶段划分

本标准将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。

对上述四个应用阶段，本标准规范了相应的随机数检测方法。

4.3 数据格式

待检的数据以二元序列的形式接受检测。

4.4 检测项目

本标准采用的随机性检测项目涉及GB/T 32915规定的15项，分别为单比特频数检测、块内频数检测、扑克检测、重叠子序列检测、游程总数检测、游程分布检测、块内最大游程检测、二元推导检测、自相关检测、矩阵秩检测、累加和检测、近似熵检测、线性复杂度检测、通用统计检测、离散傅立叶检测。

4.5 显著性水平

本标准采用的显著性水平为$\alpha=0.01$。

4.6 参数设置

本标准针对不同产品形态的不同应用阶段，接受检测的二元序列的长度不同。

5 A类产品随机数检测

5.1 送样检测

依据GB/T 32915进行随机数检测。

5.2 出厂检测

随机数出厂检测包括以下要求：

a) 检测量：采集$1\ 000\times10^6$比特随机数，分成1 000组，每组10^6比特。

b) 检测项目：依据 GB/T 32915 中规定的检测项进行检测。

c) 检测判断标准：单项检测如果 20 组或者 20 组以上不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

5.3 上电检测

本标准不做要求。

5.4 使用检测

5.4.1 周期检测

本标准不做要求。

5.4.2 单次检测

本标准不做要求。

6 B 类产品随机数检测

6.1 送样检测

依据 GB/T 32915 进行随机数检测。

6.2 出厂检测

随机数出厂检测包括以下要求：

a) 检测量：样本长度不应低于 128 比特。

b) 检测项目：单比特频数检测或者扑克检测。扑克检测参数 $m=2$。

c) 检测判断标准：被测序列如果不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

6.3 上电检测

本标准不做要求。

6.4 使用检测

6.4.1 周期检测

本标准不做要求。

6.4.2 单次检测

随机数使用单次检测包括以下要求：

a) 检测量：根据实际应用时每次所采随机数大小确定，但长度不应低于 128 比特，且已通过检测的未用序列可继续用。

b) 检测项目：扑克检测，参数 $m=2$。

c) 检测判断标准：被测序列如果不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

7 C类产品随机数检测

7.1 送样检测

依据 GB/T 32915 进行随机数检测。

7.2 出厂检测

随机数出厂检测包括以下要求：

a) 检测量：样本长度不应低于 256 比特。

b) 检测项目：单比特频数检测或者扑克检测。扑克检测参数 $m=2$。

c) 检测判断标准：被测序列如果不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

7.3 上电检测

随机数上电检测包括以下要求：

a) 检测量：样本长度不应低于 256 比特。

b) 检测项目：扑克检测，参数 $m=2$。

c) 检测判断标准：被测序列如果不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

7.4 使用检测

7.4.1 周期检测

本标准不做要求。

7.4.2 单次检测

随机数使用单次检测包括以下要求：

a) 检测量：根据实际应用时每次所采随机数大小确定，但长度不应低于 256 比特，且已通过检测的未用序列继续使用。

b) 检测项目：扑克检测，参数 $m=2$。

c) 检测判断标准：被测序列如果不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

8 D类产品随机数检测

8.1 送样检测

依据 GB/T 32915 进行随机数检测。

8.2 出厂检测

随机数出厂检测包括以下要求：

a) 检测量：样本长度不应低于 256 比特。

b) 检测项目：单比特频数检测或者扑克检测。扑克检测参数 $m=2$。

c) 检测判断标准：被测序列如果不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

8.3 上电检测

随机数上电检测包括以下要求：

a) 检测量：采集 20×10^4 比特随机数，分成 20 组，每组 10^4 比特。

b) 检测项目：扑克检测，参数 $m=2$。

c) 检测判断标准：被测序列如果 2 组或者 2 组以上不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

8.4 使用检测

8.4.1 周期检测

随机数使用周期检测包括以下要求：

a) 检测量：采集 5×10^4 比特随机数，分成 5 组，每组 10^4 比特。

b) 检测项目：扑克检测，参数 $m=2$。

c) 检测判断标准：被测序列如果 1 组或者 1 组以上不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

d) 检测周期：可配置，建议检测间隔最长不超过 24 h。

8.4.2 单次检测

随机数使用单次检测包括以下要求：

a) 检测量：根据实际应用时每次所采随机数大小确定，但长度不应低于 256 比特，且已通过检测的未用序列可继续用。

b) 检测项目：扑克检测，参数 $m=2$。

c) 检测判断标准：被测序列如果不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

9 E 类产品随机数检测

9.1 送样检测

依据 GB/T 32915 进行随机数检测。

9.2 出厂检测

随机数出厂检测包括以下要求：

a) 检测量：采集 50×10^6 比特随机数，分成 50 组，每组 10^6 比特。

b) 检测项目：依据 GB/T 32915 中规定的检测项进行检测。

c) 检测判断标准：单项检测如果 3 组或者 3 组以上不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

9.3 上电检测

随机数上电检测包括以下要求：

a) 检测量：采集 20×10^6 比特随机数，分成 20 组，每组 10^6 比特。

b) 检测项目：依据 GB/T 32915 中规定的检测项进行检测。

c) 检测判断标准：单项检测如果 2 组或者 2 组以上不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

9.4 使用检测

9.4.1 周期检测

随机数使用周期检测包括以下要求：

a) 检测量：采集 4×10^5 比特随机数，分成 20 组，每组 2×10^4 比特。

b) 检测项目：对采集随机数按照 GB/T 32915 中除离散傅立叶检测、线性复杂度检测、通用统计检测外的 12 项项目检测。

c) 检测判断标准：单项检测如果 2 组或者 2 组以上不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

d) 检测周期：可配置，检测间隔最长不超过 12 h。

9.4.2 单次检测

随机数使用单次检测包括以下要求：

a) 检测量：根据实际应用时每次所采随机数大小确定，但长度不应低于 256 比特，且已通过检测的未用序列可继续用。

b) 检测项目：扑克检测，参数 $m=2$。

c) 检测判断标准：被测序列如果不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

GM/T 0062-2018

打印日期：2018年11月12日

*

书号：155066・2-44885

定价：　18.00 元