ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0105—2021

软件随机数发生器设计指南

Design guide for software-based random number generators

2021-10-18 发布　　2022-05-01 实施

国家密码管理局　　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。

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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：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、浙江大学、深圳技术大学、深圳市纽创信安科技开发有限公司、成都卫士通信息产业股份有限公司、中国科学技术大学网络空间安全学院、成都信息工程大学、中国金融认证中心、北京宏思电子技术有限公司、北京智芯微电子科技有限公司、智巡密码(上海)检测技术有限公司。

本文件主要起草人：马原、吕娜、陈华、沈海斌、郑昉昱、陈天宇、张翌维、樊俊锋、林璟锵、刘攀、吴鑫莹、张立廷、吴震、王飞宇、张文婧、胡晓波、范丽敏、韩玮。

引　言

随机数的质量直接影响到密钥生成、数字签名以及其他密码算法和协议的实际安全性。随着软件密码模块使用越来越广泛，其中的随机数发生器设计备受关注。

本文件为软件随机数发生器的设计提供了通用的基本模型，描述了其基本部件的设计指导和建议，以指导软件随机数发生器的设计者、开发者和测试者。

软件随机数发生器设计指南

1 范围

本文件给出了软件随机数发生器设计的基本模型、基本部件的设计指南以及安全分级方法，并在附录中给出了基于SM3算法和基于SM4算法的设计实例。

本文件适用于软件随机数发生器的设计、开发、检测和评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 15852.1 信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制

GB/T 17964 信息安全技术 分组密码算法的工作模式

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32915—2016 信息安全技术 二元序列随机性检测方法

GB/T 37092—2018 信息安全技术 密码模块安全要求

GM/Z 4001 密码术语

3 术语和定义

GB/T 32915—2016、GB/T 37092—2018和GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

熵 entropy

对一个封闭系统的无序性、随机性或变化性等状态的度量。

注：随机变量 X 的熵是对通过观测 X 所获得信息量的一个数学度量。

3.2

熵源 entropy source

产生输出的部件、设备或事件。当该输出以某种方法捕获和处理时，产生包含熵的比特串。

3.3

已知答案测试 known-answer test

一种测试确定性机制的方法，即通过该机制处理给定的输入，然后将所得到的输出与已知值进行比较。

3.4

熵池 entropy pool

临时保存熵的存储区域。