



# 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

行业标准信息服务平台

2021-10-18 发布

2022-05-01 实施

国家密码管理局 发布

## 目 次

前言 .....	III
引言 .....	IV
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	3
5 软件随机数发生器设计 .....	3
5.1 基本模型 .....	3
5.2 熵源 .....	4
5.3 熵池 .....	5
5.4 熵估计 .....	5
5.5 健康测试 .....	5
5.6 DRNG .....	6
6 安全分级方法 .....	7
6.1 概述 .....	7
6.2 GB/T 37092 安全等级一级 .....	8
6.3 GB/T 37092 安全等级二级 .....	8
7 实现 .....	8
7.1 通用 .....	8
7.2 关键安全参数定义 .....	8
7.3 熵源独占性 .....	8
附录 A (资料性) 熵源和熵池结构示例 .....	9
附录 B (规范性) 基于 SM3 算法的 RNG 设计 .....	11
附录 C (资料性) 熵估计方法 .....	16
附录 D (规范性) 连续健康测试方法 .....	20
附录 E (规范性) 基于 SM4 算法的 RNG 设计 .....	23
参考文献 .....	29

## 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、北京宏思信息技术有限公司、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。

行业标准信息服务平台