ICS 35.030
CCS L 80

# 中华人民共和国密码行业标准

GM/T 0103—2021

# 随机数发生器总体框架

**General framework of random number generator**

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：北京宏思电子技术有限责任公司、北京智芯微电子科技有限公司、中国科学院数据与通信保护研究教育中心、太原理工大学、科大国盾量子技术股份有限公司、安徽问天量子科技股份有限公司、中国电子科技集团公司第三十研究所、国家密码管理局商用密码检测中心。

本文件主要起草人：唐晓柯、甘杰、胡晓波、于艳艳、张文婧、马原、王云才、张建国、赵梅生、刘婧婧、徐兵杰、罗鹏、毛颖颖。

# 随机数发生器总体框架

## 1 范围

本文件是随机数发生器设计的总体上位标准，规定了随机数发生器设计总体框架。

本文件适用于随机数发生器的研制、开发、检测，亦可推动随机数发生器相关标准的制定。

## 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 25069 信息安全技术 术语

GB/T 32915 信息安全技术 二元序列随机性检测方法

GM/T 0062 密码产品随机数检测要求

GM/T 0078—2020 密码随机数生成模块设计指南

GM/T 0105 软件随机数发生器设计指南

GM/Z 4001 密码术语

## 3 术语和定义

GB/T 25069、GB/T 32915、GM/T 0062、GM/T 0078、GM/T 0105 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。

[来源：GB/T 25069—2010，2.1.31]

3.2

**热噪声 thermal noise**

在元器件(例如运算放大器、反向偏压二极管或电阻器)中，通常情况下不希望出现的，但却内在产生的杂散电子信号(又称“白噪声”)。

注：通常都会尽力将这一现象最小化，然而由此现象的不可预测性，在随机比特流生成中，可将其作为一种熵源加以利用。

[来源：GB/T 25069—2010，2.2.4.8]

3.3

**混沌振荡 chaotic oscillation**

非线性系统复杂、无序的振荡状态。

注：根源于系统的局部非稳定性，表现为初值敏感性和内在随机性。