ICS 35.030
CCS L 80

GM

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。

3.4

相位抖动　phase jitter

由时域不稳定引起的波相位的快速、短期且具有随机特性的波动。

3.5

量子随机过程　quantum random process

具有内秉量子随机性的随机现象/过程。

注：其随机性质由量子力学原理解释和保证。用于产生随机数的量子随机过程一般包括，单光子路径选择、光脉冲所包含的光子数、相邻光子间时间间隔、真空涨落、激光相位噪声、放大自发辐射噪声等。

3.6

随机数发生器　random number generator

产生随机二元序列的器件或程序。

[来源：GB/T 32915—2016，2.2]

3.7

软件随机数发生器　software-based RNG

软件密码模块(或混合密码模块的软件部件)中的随机数发生器部件，可以单独作为软件密码模块，也可以作为软件密码模块(或混合密码模块的软件部分)的一部分。

[来源：GM/T 0105—2021，3.13]

3.8

随机源序列　raw random number sequence

熵源输出经数字化得到的离散随机值序列。

3.9

随机数序列　random number sequence

数列中的每一项在已知其他项的情况下都无法被推断的一种数列。

[来源：GB/T 25069—2010，2.2.2.184]

4　随机数发生器设计总体框架

4.1　概述

随机数发生器设计框架如图1所示，随机数发生器通常包括熵源、后处理及检测。在设计阶段对熵源或随机源序列进行熵评估，在产品检测及使用阶段对随机源序列或随机数序列进行有效性检验或随机性检验。

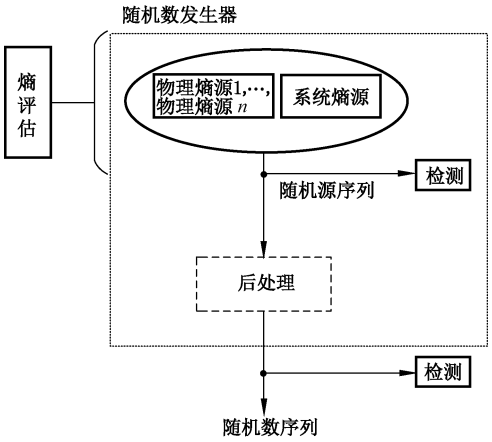

图 1　随机数发生器设计框架

a)　熵源是随机数发生器不确定性的源头，通过对不确定性进行采样量化，得到随机源序列。原则上能产生不确定性的任何方法都可以作为熵源。

b)　熵评估对熵源、随机源序列的熵进行估计，预测得到熵的估计值。

c)　后处理是可选的，通过后处理可以对随机源序列存在的偏差进行调整，生成符合统计检验的随机数序列。对于软件随机数发生器，后处理指初始化、种子更新、内部状态更新等部件。

d)　检测是通过对随机源序列或随机数序列进行有效性检验或随机性检验，以保证随机数发生器的功能正确性及质量安全性。

4.2　熵源

熵源通过对部件、设备或者事件中的不确定性进行采样量化，得到随机源序列。

熵源常用的设计原理包括相位抖动原理、热噪声直接放大原理、混沌振荡原理、量子随机过程和其他随机事件等。

熵源分为物理熵源和非物理熵源。

a)　物理熵源使用专用硬件来度量现实世界中不确定事件的物理特征，如测量热噪声电平值等。物理熵源的理论随机模型清晰合理，并能够通过采集的样本数据对声称随机模型的合理性进行验证。物理熵源输出的熵应当可以被从理论上估计，并且估计值要大于一定的阈值，以保证输出具有足够的熵。

b)　非物理熵源是指不属于物理熵源的非确定性熵源，如采集鼠标或键盘的动作等。非物理熵源由随机数发生器所在的运行环境（如操作系统、外接设备）提供，因此应当采取一定的防范措施以降低敌手破解非物理熵源（如预测到输出）的可能性。可通过建模或实验等方法论证非物理熵源输出的熵具有充足性和稳定性。

熵源是随机数发生器产生随机数的来源，当熵源失效时，需要能够快速被随机数发生器内部检测到，并根据检测输出做出相应处理，如产生报警信号等。

4.3　熵评估

熵评估通过理论建模分析、统计检测等方法对随机源序列进行预测评估，得到熵估值。

根据熵源的不同设计原理，选用适用的熵评估方法。熵评估方法应合理有效，估值应大于一定的阈值，如 0.997。

熵评估可不在随机数发生器内部实现。

4.4 后处理

后处理模块对随机源序列进行处理，通过后处理算法生成符合统计检验的随机数序列。后处理模块是可选的，实际中应根据随机源序列的统计特性决定是否选用。

后处理算法有很多，如基于分组密码、基于杂凑函数、基于 m 序列等的密码函数后处理方法和冯·诺依曼校正器、异或链、奇偶分组、m-LSB 等的轻量级后处理方法，实际中可根据熵源的特性进行设计。具体按 GM/T 0078—2020 第 9 章。

实际应用中应保证后处理的功能正确性。

4.5 检测

检测模块对随机源序列或随机数序列进行失效检验或随机性检验，以保证随机数发生器的功能正确性及质量安全性。

检测可分为自检测和产品使用时检测，自检测具体按 GM/T 0078—2020 第 7 章、第 8 章，产品使用时检测具体按 GM/T 0062 密码产品随机数检测要求。检测失败时，应根据检测输出做出相应处理，如产生报警信号等。

实际应用中应保证检测模块本身的安全性。

附 录 A
（资料性）
随机数发生器标准体系框架

本附录给出了随机数发生器标准体系框架，如图 A.1 所示，可分为框架类标准、设计类标准和检测类标准。

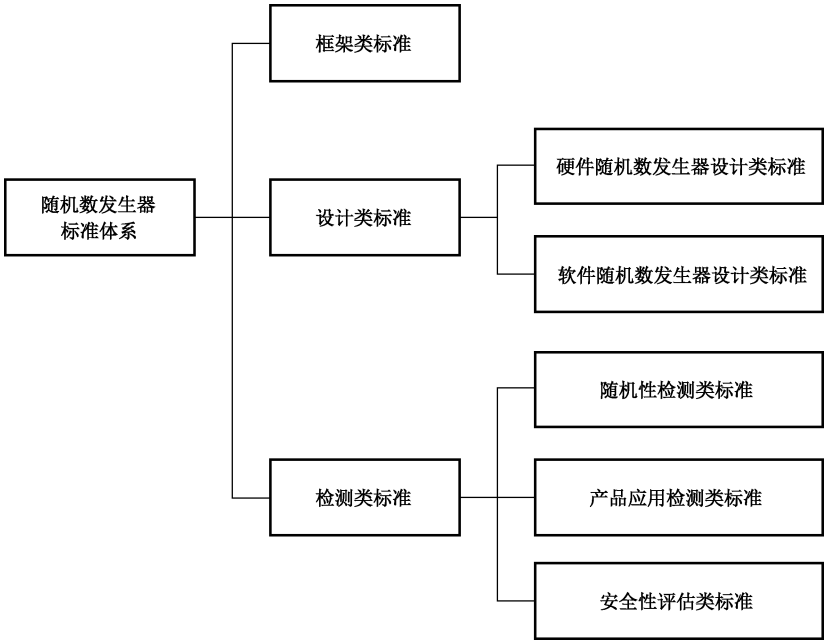

图 A.1 随机数发生器标准体系框架

——框架类标准用于指导随机数发生器设计框架、随机数发生器标准体系框架的建设。

——设计类标准用于指导随机数发生器的设计。根据设计原理不同又可分为：

- 硬件随机数发生器设计类标准，目前已经发布和正在制定的标准有 GM/T 0078《密码随机数生成模块设计指南》《物理混沌随机数发生器设计指南》《量子随机数发生器设计指南》等；
- 软件随机数发生器设计类标准，目前已经发布的标准有 GM/T 0105《软件随机数发生器设计指南》等。

——检测类标准又可分为随机性检测类标准、产品应用检测类标准和安全性评估类标准。

- 随机性检测类标准是对随机数进行的统计检测类标准，目前已经发布的标准有 GB/T 32915《信息安全技术 二元序列随机性检测方法》。
- 产品应用检测类标准是密码产品中随机数检测的标准，规定密码应用中的随机性检测指标和要求，目前已经发布的标准有 GM/T 0062《密码产品随机数检测要求》等。
- 安全性评估类标准是从安全性角度对随机数发生器进行评估的标准，如随机数发生器安全性测评要求（包括熵评估）等。

参 考 文 献

[1] AIS 20/AIS 31 Ver 2.0 A proposal for:Functionality classes for random number generators