ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0078—2020

密码随机数生成模块设计指南

The design guidelines for cryptographic random number generation module

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发 布

目　　次

前言 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 1
5　随机数生成模块一般模型 …… 2
6　物理随机源电路的设计原理 …… 2
6.1　混沌动力系统原理 …… 2
6.2　相位抖动原理 …… 3
6.3　热噪声直接放大原理 …… 4
6.4　多路物理随机源合成 …… 6
7　物理随机源的失效检测 …… 6
8　物理随机源的随机性检测 …… 6
9　后处理算法的设计方法 …… 6
9.1　后处理算法设计要求 …… 6
9.2　密码函数方法 …… 6
9.3　轻量级后处理方法 …… 7
附录 A（资料性）　物理随机源电路示例 …… 9

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、国家密码管理局商用密码检测中心、中国科学院软件研究所、中国科学院信息工程研究所、国民技术股份有限公司、北京中电华大电子设计有限责任公司、北京智芯微电子科技有限公司。

本文件主要起草人：张文婧、罗鹏、郁群慧、范丽敏、马原、杨贤伟、李丹、甘杰、夏鲁宁。

密码随机数生成模块设计指南

1 范围

本文件规定了密码硬件随机数生成模块的设计要求。

本文件适用于随机数生成模块的研制、开发和检测的指导。

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。

GM/T 0005 随机性检测规范

GM/T 0008 安全芯片密码检测准则

3 术语和定义

GM/T 0005 和 GM/T 0008 界定的以及下列术语和定义适用于本文件。

3.1

随机数生成模块 random number generation module

利用真实世界的自然随机性，从随机的物理过程中提取出随机量，并经过变换处理，输出随机数的电路。

3.2

热噪声 thermal noise

亦称白噪声，是由导体中电子的热震动引起的，它存在于所有电子器件和传输介质中。它是温度变化的结果，但不受频率变化的影响。热噪声在所有频谱中以相同的形态分布，它是不能够消除的。

3.3

混沌理论 chaos theory

一种复杂的系统演化理论，主要将系统数据从有序的状态下转变成无序的状态模式。混沌是确定性系统随机行为的总称，它的根源在于非线性的相互作用。混沌系统有如下几个基本特征：内在随机性、初值敏感性和非规则的有序。

3.4

相位抖动 phase jetter

电路中的噪声会随机改变周期信号的频率，它在信号的相位上表现为一种特殊的随机过程，这种随机现象就是相位抖动。

4 缩略语

下列缩略语适用于本文件。

CBC：密码分组链接(Cipher Block Chaining)