ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0083—2020

密码模块非入侵式攻击缓解技术指南

Guideline for the mitigation of non-invasive attacks against cryptographic modules

2020-12-28 发布　　2021-07-01 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、飞天诚信科技股份有限公司、格尔软件股份有限公司、北京中电华大电子设计有限责任公司、北京握奇智能科技有限公司、北京宏思电子技术有限责任公司。

本文件主要起草人：刘宗斌、刘泽艺、李敏、马存庆、高能、屠晨阳、彭佳、刘丽敏、马原、朱鹏飞、郑强、郑晓光、陈国、张文婧、陈钧莎。

密码模块非入侵式攻击缓解技术指南

1 范围

本文件给出了密码模块非入侵式攻击方法、缓解技术以及测试方法。

本文件适用于指导密码模块中部署非入侵式攻击缓解技术，指导技术人员在密码模块开发和使用过程中，根据具体的密码算法特点、密码模块特性、具体部署的实际场景，选择缓解技术来抵抗非入侵式攻击威胁。

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 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 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 37092—2018 信息安全技术 密码模块安全要求

GM/T 0001(所有部分) 祖冲之序列密码算法

GM/T 0044(所有部分) SM9 标识密码算法

3 术语和定义

GB/T 25069、GB/T 37092 界定的以及下列术语和定义适用于本文件。

3.1

高级侧信道分析 advanced side-channel attacks

对于信道泄露的高级利用。这些泄露主要依赖于密码设备处理的数据以及检索秘密参数时执行的操作。

3.2

关键安全参数 critical security parameter

与安全有关的信息(例如：秘密的和私有密码密钥，口令之类的鉴别数据，个人身份号、证书或其他可信锚)，其泄露或修改会危及密码模块的安全。

注：关键安全参数可能是明文或加密的。

[GB/T 25069—2010，定义 2.2.2.50]

3.3

关键安全参数类 CSP class

CSP 的分类，如密钥、鉴别数据(如口令、PINs 码、生物鉴别数据)。

3.4

差分电磁分析 differential electromagnetic analysis

对密码模块电磁辐射的变化进行分析。针对大量的电磁辐射测量值，使用统计方法来确定划分出