ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0084—2020

密码模块物理攻击缓解技术指南

Guideline for the mitigation of physical 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、屠晨阳、彭佳、高能、刘泽艺、李敏、马存庆、刘丽敏、马原、朱鹏飞、张勇、郑强、郑晓光、陈国、张文婧、陈钧莎。

密码模块物理攻击缓解技术指南

1 范围

本文件规定了密码模块的物理安全机制、物理攻击方法、用于防止或检测这些攻击的缓解技术、以及在开发、配送、运行等生命周期不同阶段的缓解措施。

本文件适用于指导密码模块中实现物理攻击缓解技术、验证所测评的密码模块达到最基本的安全保证。

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 37092 信息安全技术 密码模块安全要求

3 术语和定义

GB/T 37092 界定的以及下列术语和定义适用于本文件。

3.1

数据印痕攻击 data imprinting attack

采取措施(例如辐射、高温等)将内存电路或包含敏感信息的设备中的数据进行固化，使得在一段时间内，不能对数据进行写入、修改等操作。

3.2

物理攻击 physical attacks

导致密码模块发生物理修改或导致其运行异常的攻击。

3.3

能量攻击 power attack

通过对密码模块施加强能量场等方式，破坏密码模块内部电路的正常工作状态，获得密码模块中的敏感信息。

3.4

篡改检测 tamper detection

密码模块对企图破坏其物理安全的行为的自动判定。

3.5

篡改响应 tamper response

当企图破坏密码模块物理安全的行为被检测到时，密码模块自动采取的操作。

4 缩略语

GB/T 25069、GB/T 37092 中所使用的以及下列缩略语适用于本文件。