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。

CMOS:互补金属氧化物半导体(Complementary Metal Oxide Semiconductor)
DRAM:动态随机存取存储器(Dynamic Random Access Memory)
EEPROM:电可擦可编程只读存储器(Electrically Erasable Programmable Read Only Memory)
PROM:可编程只读存储器(Programmable Read-Only Memory)
RAM:随机存取存储器(Random Access Memory)
RFID:射频识别(Radio Frequency Identification)
ROM:读存储器(Read-Only Memory)
VCC:供电电压(Volt Current Condenser)

5 物理安全概述

在计算机安全领域,物理安全是指部署在计算系统周围,用于检测非授权的物理访问的屏障。物理安全是对逻辑安全和环境安全的补充。逻辑安全是指通过操作系统、安全协议以及其他软件防止非授权访问数据的机制;环境安全是指凭借诸如守卫、摄像机、围墙、建筑等设施,限制或防止对计算系统进行非授权物理访问的措施。

物理安全的有效性满足以下条件:遇到攻击时,在攻击开始或者后续的渗透破坏期间,应导致攻击成功的概率很低,并且导致检测出攻击的概率很高。

物理安全机制是指在遇到非授权物理访问时,用于保护敏感数据的防御措施,包括导致对数据的非授权物理访问很困难(篡改抵抗),具有用于阻止攻击的触发机制(篡改检测),能够保存一次攻击尝试的痕迹并在后续的检测中发现曾经出现的攻击尝试(篡改存迹)等。

对密码模块而言,物理攻击是指,导致密码模块发生物理修改或其运行异常,进而对密码模块进行非授权物理访问的攻击。物理攻击的缓解是指,阻碍或缓解物理攻击的防御措施。

密码模块不仅在使用时存在物理安全威胁,在开发、配送、运行等生命周期的不同阶段也可能遭受物理攻击,应在开发、配送等阶段具有缓解物理攻击的能力。

6 物理安全机制

6.1 概述

物理安全机制应适用于不同的技术实现、应用环境和攻击场景。常见的物理安全机制包括6.2～6.7列举的物理安全机制和影响系统安全性的物理安全因素。

6.2 防篡改

防篡改是指能够抵抗所有已知攻击和可能的突发攻击的物理安全机制。

6.3 篡改抵抗

篡改抵抗是指能够提供保护措施,阻止物理安全攻击对数据非授权的物理访问。对于只拥有篡改抵抗的密码模块而言,只有篡改发生时,密码模块所有者才知道篡改的发生。

6.4 篡改检测

篡改检测是指密码模块对企图破坏模块物理安全的行为的自动判定。密码模块在检测出入侵行为后,应紧接着自动做出响应。

6.5 篡改响应

篡改响应是指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。对于依赖外部响应的密码模块，可采用报警的操作。对于不能依赖外部响应的密码模块，可采用擦除或销毁秘密数据的操作。

6.6 篡改存迹

篡改存迹能够确保，篡改发生后，篡改留下的证据会被密码模块保留。这种机制由化学或化学与力学相结合的方法实现。密码模块中应存在长期有效的审计策略。

6.7 物理安全因素

6.7.1 体积和重量

应结合实际应用，在实现物理安全机制时考虑体积和重量的影响，增加攻击难度。

6.7.2 混合和分层的机制

可采用多层以及多种物理安全机制增加攻击难度。常见的混合机制包括（但不限于）篡改响应与篡改抵抗结合使用，在篡改抵抗或篡改响应机制的外围部署篡改存迹机制等。

——篡改响应与篡改抵抗结合使用。若攻击者提高技术可破坏具有篡改抵抗的密码模块，密码模块应能够做出响应，在被破坏之前，将内部敏感安全参数或数据置零。

——在篡改抵抗或篡改响应机制的外围部署篡改存迹机制，能够防止在一段时间内的攻击尝试。周期性的常规审计可能会在密码模块被完全破坏之前发现篡改的痕迹，并允许在攻击完成之前增加其他缓解措施。

7 物理攻击技术

7.1 概述

本章规定物理攻击技术。攻击技术分为五类：内部探针攻击技术、加工技术、聚能切割技术、能量攻击技术、以及环境条件改变技术。每一类攻击技术包含了多种攻击方法，并且随着技术的不断进步将产生新的攻击方法，本文件仅对常见的攻击方法进行规定。

本章所规定的攻击方法均有可能导致密码模块发生物理修改或运行异常，进而对密码模块进行非授权物理访问的攻击。每一种攻击方法是否能够成功实施，与密码模块的物理特性、物理安全机制强度、攻击参数的选取等因素密切相关，需要对具体场景进行具体分析，本文件不对攻击方法的可行性和有效性进行定量衡量。

7.2 内部探针攻击技术

7.2.1 概述

内部探针攻击是指通过探针直接接触电路中导体的方式，获得密码模块的信息和/或对密码模块进行修改。

7.2.2 被动式探针

被动式探针是指通过被动观测的方式，记录和观察包含在电路中的信息。常见的被动式探针包括（但不限于）示波器或逻辑分析仪探针。

7.2.3 主动式探针

主动式探针是指通过主动注入的方式对密码模块进行修改。常见的攻击方法是通过使用模式发生器或类似的装置，对一个运行的密码模块注入信号。

7.2.4 能量探针

能量探针是指通过电子束、离子束或者聚焦的光束对半导体存储器的内容进行读写，或改变控制信号。

7.3 加工技术

7.3.1 概述

加工技术是指通过对密码模块的外层包装、灌封或可卸封盖进行切削、钻孔等方式，移除外层包装、可卸封盖或灌封材料，访问到在外层包装、灌封或可卸封盖下的电路。上述材料被移除后，将能够进行探针攻击。

若密码模块受到物理安全机制保护，攻击者应具备在不触动传感器或留下证据的前提下执行加工操作的能力。灌封材料移除后，攻击者应具备禁用或绕过传感器，并进行探针攻击的能力。

若密码模块受到篡改存迹系统保护，攻击者在完成攻击后应具备能够覆盖掉证据的能力。

7.3.2 手工材料移除

手工材料移除是指通过使用小刀等工具，在不触发传感器的情况下，从灌封或密闭容器上移除材料。

7.3.3 机械加工

机械加工是指一种利用机械设备、可在短时间内完成的材料移除方法。

7.3.4 水刀加工

水刀加工是指利用高压水刀的材料移除方法。

7.3.5 激光加工

激光加工是指利用激光的材料移除方法，宜根据材料的特点对激光的波长、强度等进行调整。

7.3.6 化学加工

化学加工是指通过喷射腐蚀性溶剂，利用化学反应把涂层和灌封材料完全移除的方法。

7.3.7 喷沙处理

喷沙处理是指通过高速喷射的磨料，精确移除少量材料的方法，可实现微米级的切削。“沙”是指包括从沙子到碳化硅的各种磨料。

7.4 聚能切割技术

聚能切割技术是指通过高速精确地穿透外部封装，导致电路在响应之前就失效的材料移除技术。通过聚能切割技术解开外部包装后，攻击者应在内存所存储内容完全消失之前对内存恢复供电。

7.5 能量攻击技术

7.5.1 概述

能量攻击技术是指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。

7.5.2 辐射数据印痕攻击

辐射数据印痕攻击是指使用放射物对存储密钥或其他秘密数据的 CMOS RAM 进行 X 射线波段（可能还有其他波段）辐射，在不考虑掉电或复写机制的条件下对该 RAM 单元进行物理破坏，使该 RAM 单元中的内容被“固化”，该 RAM 单元可在空闲时被读取。

7.5.3 温度数据印痕攻击

温度数据印痕攻击是指使用较低的温度（在 0 ℃之下）对 CMOS RAM 进行数据印痕，使 RAM 在掉电后的几秒到几小时内保持其中的内容。温度越低，RAM 中内容所保持的时间越长。复写操作将擦除这些内容。

7.5.4 高电压数据印痕攻击

高电压数据印痕攻击是指通过对 CMOS RAM 注入一个短时间高电压脉冲信号，以一种类似于辐射数据印痕攻击的方式对 RAM 中的内容进行数据印痕。

7.5.5 高低电压异常

高低电压异常是指通过将 VCC 变更为异常的高值或低值，在电路中诱发异常行为。异常行为包括（但不限于）处理器曲解指令，擦除或复写电路失效，以及内存保留不需要的数据等。

7.5.6 时钟毛刺

时钟毛刺是指通过拉长或缩短诸如微处理器时钟电路的时钟脉冲，在电路中诱发异常行为。异常行为包括指令被跳过，或者其他不稳定的操作等。

7.5.7 电磁干扰

电磁干扰是指通过强烈的电磁场环境，对噪声二极管型随机数发生器和计算电路进行破坏。

7.5.8 电子束读/写

电子束读/写是指通过传统扫描电子显微镜的电子束对 EPROM，EEPROM 或 RAM 的各个位进行读/写操作。实施电子束读/写之前，宜通过化学加工方法将芯片表面暴露出来。

7.5.9 激光/放射线读/写

激光/放射线读/写是指通过使用激光/放射线直接穿透芯片的硅外壳部分，对计算设备的存储单元进行读写操作。穿透硅外壳不需要移除设备的钝化层。

7.5.10 成像方法

成像方法是指通过多种成像技术将密闭或灌封包装内部的内容显现出来，对脆弱部分准确定位，确定印制电路板卡的布局布线，显示不同部分的布局，并识别出特定的部分。

7.6 环境条件改变技术

7.6.1 概述

电子设备和电路被设计成在一个特定范围的环境条件下运行，当设备运行在正常运行范围之外，可导致不可预知的运行或失败。用于保护设备或提供篡改存迹的方法可能受到不同环境条件的影响。

7.6.2 设备电路失效攻击

设备电路失效攻击是指通过调整运行电压或温度，或扰乱时钟以改变频率，使设备电路超出正常运行范围的上界或下界，迫使设备进入不可预知的状态。在不可预知的状态下运行设备，可能破坏设备的安全性。

7.6.3 设备外部封装失效攻击

设备外部封装失效攻击是指调整运行温度可破坏某些保护机制，如篡改存迹封条的灌封材料或粘合剂。

8 物理攻击缓解技术

8.1 概述

本章规定物理安全所涉及的攻击缓解技术。攻击缓解技术分为四类：篡改抵抗类技术、篡改存迹类技术、篡改检测类技术、篡改响应类技术。每一类缓解技术包含了多种缓解方法，并且随着技术的不断进步将产生新的缓解方法，本文件仅对常见的缓解方法进行规定。

篡改抵抗类技术可阻止加工、聚能切割攻击，以及以加工、聚能切割为前置步骤的其他攻击。

篡改存迹类技术不能够阻止攻击或进入被保护的区域，而是对攻击或进入操作留下证据以供检测。

篡改检测类技术利用探测某一类物理信号或物理量的传感器对企图利用相应物理信号或物理量的破坏密码模块物理安全的行为进行自动检测和判定。例如，电压传感器对密码模块的电路供电电压进行检测。

篡改响应类技术是指当物理攻击行为被检测到时，密码模块自动采取的操作，使物理攻击难以达到窃取敏感安全参数等攻击目的，避免受到进一步攻击。

本章所规定的缓解技术均有可能导致一种或多种物理攻击难以达到预期的攻击目的。每一种缓解技术是否能够成功抵抗特定的物理攻击，与密码模块的物理特性、特定的物理攻击强度、缓解技术参数指标的选取等因素密切相关，需要对具体场景进行具体分析，本文件不对缓解技术的可行性和有效性进行定量衡量。

8.2 篡改抵抗类技术

8.2.1 概述

篡改抵抗类技术常采用两种方式实现。一种方式是通过选择难以被穿透的材料或者增加材料厚度的方式抵抗攻击，能够阻止加工、探针探测、能量或化学攻击。另一种方式是将设备牢牢地附着在篡改抵抗屏障上，使得不论是将设备从篡改抵抗屏障上分离开还是直接穿透屏障的尝试，都会导致被保护设备的损毁。

8.2.2 坚硬的外壳

坚硬的外壳是指采用硬质材料的外壳，可阻止加工、探针探测、能量或化学攻击。

8.2.3 保形涂料

保形涂料是指可应用于直接附着在电器部件或印制电路板上的各种厚度的保形涂层。保形涂料可保护印制电路板或部件免受潮湿、真菌、灰尘、腐蚀、磨损以及其他环境压力的损坏。宜采用坚硬的不透明保形涂料，用于阻止加工、探针探测、能量或化学攻击，以及阻止对实际实现细节的获取。

8.2.4 绝缘基板

绝缘基板是指使用不能让红外波段激光穿透的材料代替涂料中的硅材料。

8.2.5 特殊半导体拓扑

特殊半导体拓扑是指对芯片的布局布线进行扰乱，避免芯片的关键结构被暴露。

8.2.6 不透明

不透明是指使用不透明的外壳或保形涂料，阻止对设备结构的视觉检测。

8.3 篡改存迹类技术

8.3.1 概述

篡改存迹不能够阻止攻击或进入被保护的区域，而是对攻击或进入操作留下证据以供检测。

8.3.2 易碎包装

易碎包装是指将密码模块密封在由陶瓷、玻璃或其他易碎材料制成的包装内。若试图进入包装，包装将会产生裂缝或粉碎，留下证据。

8.3.3 铝制包装

铝制包装是指由铝或其他能够加热(高于 1 000 °F或 500 ℃)和淬火的类似材料制成的包装。这种热处理在包装表面出现无数网状的很浅的裂缝，并且每一块裂隙都是独一无二的。可对铝制包装进行拍照，通过采取周期性光学对比的方式，对破坏包装的行为进行检测。

8.3.4 抛光包装

抛光包装是一种类似于铝制包装的方法，对包装表面是否发生变化进行检测。包装表面的任何痕迹都代表试图破坏包装的行为。

8.3.5 变色油漆

变色油漆是指由一种颜色的油漆和另一种对比色的油漆的微气泡组成的包装表面涂层。若表面遭到破坏，另一种颜色会像“流血”一样出现在包装表面，表面的颜色特性可被检测。

8.3.6 全息和其他篡改检测的胶带和标签

全息和其他篡改检测的胶带和标签是指胶带或标签表面含有坚固的粘合剂、可印有全息图像、且难以被伪造。试图移除胶带的攻击会对胶带造成损毁。应通过检测上述胶带或标签是否损毁，对封盖是否被非法开启进行检测。

8.3.7 一次性应力形变测试仪

一次性应力形变测试仪是指用于测量物体曾受到外力发生形变的仪器。测试仪应通过适宜的粘合

剂与外壳相连，若外壳变形，测试仪中的金属薄片也发生不可逆形变，其电阻值变化将被测量出来。应通过检测外壳内部应力形变测试仪电阻值变化的方式，对外壳的形变进行检测。

8.3.8 一次性光敏材料

一次性光敏材料是指用于测量物理曾受到不同波长光波照射的仪器。测试仪应放置在密码模块的适当位置，若照射的光的波长发生变化，测试仪中的光敏材料也发生不可逆的外观变化。应通过录光敏材料外观变化的方式，对运行环境的光照变化进行检测。

8.3.9 气体分析

气体分析是指当外壳受到攻击而损坏时，可通过监测注入到外壳内部气体成分的变化，对外壳的损毁进行检测。常见的气体分析包括一次性气压测试和一次性成分变化。一次性气压测试通过检测外壳内部气压变化的方式，检测到外壳的损毁（气压下降或不再真空）。一次性成分变化通过检测外壳内部气体组成变化的方式，检测到外壳的损毁。

8.3.10 剂量传感器

剂量传感器是指通过检测剂量传感器中辐射总剂量变化的方式，对辐射数据印痕攻击进行检测。

8.3.11 RFID 轮询

RFID 轮询是指通过内嵌在设备或外壳中的 RFID 标签进行轮询的方式，对密码模块的物理位置是否改变或替换进行检测。

8.4 篡改检测类技术

8.4.1 电压传感器

电压传感器是指为保证电路的正常运行，应对电路的供电进行检测。任何超出正常运行范围的操作都应被视为攻击，并且应对其进行响应。电压监控器应不受供电变化的影响。

8.4.2 探针传感器

探针传感器是指由一组传感器对主动式物理攻击进行检测。探针传感器应足够敏感和/或足够小。

8.4.3 带有压电传感器的钢化玻璃

带有压电传感器的钢化玻璃是指通过检测压电传感器压电信号变化的方式，对钢化玻璃是否破损进行检测。打破玻璃所需的压力，应足以在附着在玻璃内侧的压电设备上引起一个明显的信号。

8.4.4 压电片

压电片是指通过检测压电片电压变化的方式，对压电片是否被探针探测或刺穿进行检测。

8.4.5 动作传感器

动作传感器是指通过检测动作传感器变化的方式，对密码模块是否被移动或打开进行检测。

8.4.6 超声波传感器

超声波传感器是指通过检测超声波传感器变化的方式，对被保护区域结构是否变化进行检测。

8.4.7 微波传感器

微波传感器是指通过检测微波传感器变化的方式，对被保护区域结构的变化进行检测。被保护区域的墙壁材料应具有不被微波穿透的能力。

8.4.8 红外线/可见光传感器

红外线/可见光传感器是指通过检测红外线/可见光传感器变化的方式，对被保护区域光（和热）的变化进行检测。

8.4.9 加速度传感器

加速度传感器是指通过检测加速度传感器变化的方式，对密码模块的移动或振动进行检测。

8.4.10 形变传感器

形变传感器是指通过检测附着于柔性底座或压电设备上的形变传感器通过镜面反射回来的光束是否偏移的方式，对柔性底座或压电设备是否发生形变进行检测。

8.4.11 微偏移动作传感器

微偏移动作传感器是指通过检测微偏移动作传感器变化的方式，对密码模块的移动进行检测。

8.4.12 磁通传感器

磁通传感器是指通过检测磁通传感器变化的方式，对实时辐射强度的变化进行检测。

8.4.13 温度传感器

温度传感器是指通过检测温度传感器变化的方式，对实时温度的变化进行检测。

8.5 篡改响应类技术

8.5.1 概述

检测出入侵行为后，密码模块应紧接着做出篡改响应。电压、温度、频率等环境变化引起密码模块失效时，可将密码模块复位或停止工作，避免受到进一步攻击。对于诸如探针攻击、能量攻击等攻击手段，常采取将敏感安全参数或敏感数据移除，或者利用 PUF、密钥擦除等方法将敏感安全参数进行加密，改变或擦除加密密钥的方式，避免数据被窃取。密码模块常将敏感安全参数或敏感数据存储于 RAM、DRAM、闪存、硬盘或其他易失性或非易失性的读/写介质中。篡改响应技术是指通过将敏感安全参数或敏感数据从内存电路或包含敏感信息的密码模块中移除的方式，阻止攻击者非授权地访问密码模块中的敏感信息。

8.5.2 RAM 掉电

对于已经采用数据印痕保护（温度检测和辐射检测）的设备而言，宜采用 RAM 掉电的篡改响应方法。长时间存储在 RAM 中的任何信息宜被周期性地打乱、翻转或以其他方式发生改变，以防止数据印痕攻击。

8.5.3 PUF 响应

对于已经采用 PUF 保护的设备而言，宜采用 PUF 响应的篡改响应方法。当密码模块受到物理攻

击时，PUF 所依赖的物理结构受到破坏，PUF 响应发生变化，由 PUF 响应所提供的敏感安全参数也将改变。

8.5.4 内存复写

内存复写是指通过对内存复写若干次全 0，再复写若干次全 1，消除内存痕迹特征。宜采用特殊的复写模式和较多的复写次数，例如 7 次复写模式依次填写 0xF6、0x00、0xFF、随机值、0x00、0xFF、随机值。

8.5.5 消磁

消磁是指通过用于抹去介质中数据的消磁器，消除或减弱磁盘或驱动器的磁场。对于磁性介质，消磁可快速并有效地清除整个介质中的数据。

8.5.6 物理破坏

物理破坏是一类不可逆的数据擦除方法。常见的物理破环方法包括（但不限于）化学反应、研磨和粉碎、焚化等：

——化学反应是指通过破坏剂对实体部件产生不可逆的化学变化，对实体部件进行物理破坏的方法。这种方法常用于敏感的环境。常见的破坏剂包括（但不限于）铝热剂、腐蚀剂等。

——研磨和粉碎是指通过物理方式，将实体部件分解成废料。例如通过硬件粉碎机粉碎的方式，能够将手机、PDA 等小型电子设备或电子部件进行粉碎。

——焚化是指通过能够将材料液化或汽化的高温对实体部件进行物理销毁的方法。对于磁性介质，当温度超过居里点时，铁磁材料或亚铁磁材料将变成顺磁物质，磁化被破坏。

9 开发、配送和运行

9.1 概述

本章将规定在开发、配送和运行的环节中，如何阻止或缓解物理攻击。

9.2 开发

9.2.1 功能测试和调试

在密码模块开发、测试和生产期间，密码模块中可能会包含测试探针接入点、逻辑或阵列中内置自测试管脚以及固件断点或其他诊断辅助工具。在密码模块发布之前，这些测试调试机制应被移除、禁用或不提供给攻击者使用。

9.2.2 安全测试

在密码模块测试期间，应进行足够的破坏性试验，验证所采用的安全特性。

9.2.3 出厂安装密钥

密码模块宜设计为在出厂时就将密钥或安全参数安装到密码模块内。在密码模块运抵至终端用户期间，应对密钥进行保护。在内部制造流程中，也应对秘密数据进行保护。应有适当的内部流程和机制，如定期审计、员工筛选以及将敏感信息放置在受控安全区域等，且确保这些流程和机制在制造和配送过程中被严格实施，以保证对密钥或安全参数的保护。

9.3 配送

9.3.1 文档

密码模块的开发包括生成并发布详细的文档以支持生产、提供用户支持、现场维修、维护或用户设置及操作。文档可提供设计规格、图表、内部图纸或插图以及物理安全机制信息。这些文档可与产品一同运送给用户，或者可从厂商网站上查阅或下载。厂商应设置文档的开发、出版或访问权限，包括对文档开发人员的权限管理，以及在文档发布出版之前对整个文档进行最终全面审查等。

9.3.2 打包

在配送或运输密码模块期间，厂商应提供适当的模块打包方法，以确保在配送期间密码模块未被修改或破坏。密码模块设计或制造时，应要求运行人员或收件人能够对密码模块进行装配和安全配置。在运输期间，密码模块尚未装配，可能以一种运行人员或收件人未知的方式被破坏。在对模块或其配件进行打包时，应采用一些机制防止上述未知的攻击或破坏，如装运在密封的坚固容器中，并在容器上设有篡改存迹封条或篡改检测机制。对于特别敏感的部分，宜采取可信快递、用户自提或安全运输协议等方式进行配送。

9.3.3 配送证明

运行人员或目标收信人接收了配送的密码模块，应采取一些流程以证明配送过程未受到破坏。例如，配送一个软件密码模块，发布代表制造信息的预设的杂凑值或数字签名，能够证明软件密码模块在配送期间是否被修改。

9.4 运行

9.4.1 概述

密码模块运行期间，提供反馈信息（如模块状态、错误报告或诊断信息）的机制，能被用于收集模块中的功能性信息，暴露模块的安全漏洞。反馈信息有两种形式：在被攻击时模块提供的实时反馈信息，或反馈给攻击者的关于设计和实现方面的信息。

9.4.2 攻击反馈

当检测到攻击时，密码模块可能即时进行显示，例如直接显示一条“检测到物理攻击”的消息。这种即时反馈可能允许攻击者识别哪些攻击方法未能被检测出，以及哪些被检测到的攻击方法有助于找出密码模块的安全漏洞。

密码模块宜被设计为不即时报告这些信息，并只对授权运行人员报告这些信息。

9.4.3 测试反馈

当采用特殊的方式测试密码模块服务时，测试反馈可能泄露独特的设计特点和内部敏感信息。

密码模块宜被设计为不提供这类测试反馈，或只对授权测试人员提供这类测试反馈。

参 考 文 献

[1] ISO/IEC TS 30104:2015 信息技术 安全技术 物理攻击及缓解技术和安全要求(Information technology—Security techniques—Physical security attacks,mitigation techniques and security requirements)

中华人民共和国密码
行业标准
密码模块物理攻击缓解技术指南
GM/T 0084—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.25 字数 31 千字
2021年5月第一版 2021年5月第一次印刷
*
书号:155066·2-35880 定价 18.00 元

GM/T 0084-2020

码上扫一扫 正版服务到