ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0098.2—2012

中国金融移动支付 检测规范 第2部分：安全芯片

China financial mobile payment—Test specifications—
Part 2: Security chip

2012-12-12 发布 2012-12-12 实施

中国人民银行 发布

目　　次

前　言

《中国金融移动支付 检测规范》标准由以下8部分构成：

——第1部分：移动终端非接触式接口；

——第2部分：安全芯片；

——第3部分：客户端软件；

——第4部分：安全单元（SE）应用管理终端；

——第5部分：安全单元(SE)嵌入式软件安全；

——第6部分：业务系统；

——第7部分：可信服务管理系统；

——第8部分：个人信息保护。

本部分为该标准的第2部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分负责起草单位：中国人民银行科技司、中国人民银行金融信息中心、中国金融电子化公司。

本部分参加起草单位：北京银联金卡科技有限公司（银行卡检测中心）、中金国盛认证中心、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、上海市信息安全测评认证中心、信息产业信息安全测评中心、北京软件产品质量检测检验中心、中钞信用卡产业发展有限公司、上海华虹集成电路有限责任公司、上海复旦微电子股份有限公司、东信和平智能卡股份有限公司、大唐微电子技术有限公司、武汉天喻信息产业股份有限公司、恩智浦半导体有限公司。

本部分主要起草人：李晓枫、陆书春、潘润红、杜宁、李兴锋、张雯华、刘力慷、刘志刚、聂丽琴、李晓、尚可、郭栋、熊文韬、宋铮、李宏达、王冠华、胡一鸣、张晓、平庆瑞、张志茂、陈君、彭美玲、李微、陈吉、程恒。

引　言

随着移动支付产业的发展和芯片在移动支付行业中的广泛应用,安全芯片在移动支付产业中的地位也越来越重要。采用安全芯片可以从根本上提升移动支付风险防范水平，能够有效地保护芯片中的用户敏感信息，抵御对芯片的非法访问和外部攻击，满足对移动支付安全的迫切需求。

移动支付安全芯片应用范围的扩大和应用环境复杂性的增加,对安全芯片保护数据的能力有了更强的要求。目前针对芯片的各种专用攻击技术也在迅猛发展，因此分析非入侵式、半入侵式和入侵式的攻击方式对芯片的威胁及其防御措施的有效性,编写相应的检测标准以规范安全芯片的设计和开发的安全需求,对于保证移动支付安全有着重大的意义。

中国金融移动支付　检测规范　第2部分：安全芯片

1　范围

本部分旨在对移动支付安全芯片的安全性评估测试进行定义。

本部分适用的对象主要为获得授权的从事移动支付安全芯片设计、制造、评估与检测单位。安全芯片卡的发卡机构也可参考本部分以获得对移动支付安全芯片安全风险的进一步了解，以协助风险控制过程。

有关安全功能检测和抗攻击能力检测要求在本部分中进行了定义。

2　术语和定义

下列术语和定义适用于本文件。

2.1

非易失性存储器（NVM）　non volatile memory (NVM)

断电后存储的数据不会消失的存储器。通常用来存放程序和数据。目前在安全芯片上采用的主要包括电可擦写存储器和闪存。

2.2

非易失性可编程存储器　non volatile programmable memory

断电后存储的数据不会消失的可编程存储器。

2.3

只读存储器（ROM）　read-only memory (ROM)

只能读出事先存入数据的存储器，该存储器一旦存入资料就无法再将其改变或删除。通常使用于不需经常变更资料的电子设备或计算机系统中，资料不会因为电源关闭而消失。

2.4

随机存储器（RAM）　random access memory (RAM)

随机存储器，存储单元的内容可随意读取或存入，且存取的速度与存储单元的位置无关。这种存储器在断电时将丢失其存储内容，主要用于存储短时间使用的数据。

2.5

侵入式攻击　invasive attack

是直接针对安全芯片上硅晶的攻击，封装材料被打开并且安全芯片表面被暴露。伴随着这类攻击，电路能够被直接物理触及，数据被窃听或者改动，并且硬件能够被物理修改。

2.6

半侵入式攻击　semi-invasive attack

此类攻击要求SE被打开并且安全芯片表面被暴露。攻击者将会尝试用从闪光灯操纵攻击到通过对靠近安全芯片表面电磁场的测量来窃听数据等非接触方法触及电路。

2.7

非侵入式攻击 non-invasive attack

此类攻击发生时SE不需要被打开。安全芯片仍然保持嵌入在封装材料中。非侵入式攻击利用所有安全芯片执行任务时在其周边所能够被获得的信息。

2.8

威胁 threats

任何强迫导致负面影响的行为。

2.9

攻击 attack

在所有威胁中，攻击者的攻击目标将会在秘密数据或物理平台中选择。为达到攻击目标，攻击者所进行的行为被称为攻击。

2.10

个人标识码（PIN） personal identification number (PIN)

用于保护安全芯片免受误用的秘密标识代码。PIN与密码类似，只有SE的所有者才知道该PIN。只有拥有该安全芯片并知道PIN的人才能使用该安全芯片。

2.11

倒装安全芯片 flip chip

一种无引脚结构，一般含有电路单元。设计用于通过适当数量的位于其表面上的锡球(导电性粘合剂所覆盖)，在电气上和机械上连接于电路。

2.12

高层设计（HLD） high level design (HLD)

顶层设计规范，将安全芯片的安全功能规范细化，主要包括安全芯片安全功能规范的基本结构和主要的硬件、固件和软件元素。

2.13

底层设计（LLD） low level design (LLD)

详细的设计规范，将高层设计细化成一定程度的细节，此细节可用作编程或硬件构造的基础。

2.14

标识信息 chip indicators

安全芯片生产完成后标识于表面的厂商名称和掩膜信息等。

2.15

反向工程 reverse engineering

通过技术手段对从公开渠道取得的安全芯片进行拆卸、测绘、分析等而获得有关敏感信息的行为。

2.16

旁路分析 side channel analysis

通过旁路的途径对安全芯片的敏感信息进行分析的非侵入式攻击的手段。

2.17

单粒子效应 single event effect

高能带电粒子在器件的灵敏区内产生大量带电粒子的现象。

2.18

测试模式 test mode

安全芯片出厂时，进行必要的功能验证所需的一种安全芯片状态，包括圆片测试模式或固件测试模式，在测试模式下可对安全芯片的关键参数和敏感信息访问。

2.19

形象化 visualize

通过相应技术手段对安全芯片表面和功耗等特征进行可视化的处理。

2.20

随机数发生器 random number generator

通过一些算法、物理信号、环境噪音等来产生没有关联性的数列的模块。

3 符号和缩略语

以下符号和缩略语表示适用于本部分。

IC	Integrated Circuit	集成电路
ROM	Read-Only Memory	只读存储器
RAM	Random Access Memory	随机存储器
EEPROM	Electrically Erasable Programmable Read-Only Memory	电可擦可编程只读存储器
SPA	Simple Power Analysis	简单功耗分析
DPA	Differential Power Analysis	差分功耗分析
DFA	Differential Fault Analysis	差分错误分析
EMA	Electro-Magnetic Analysis	电磁分析
FIB	Focused Ion Beam	聚焦离子束
CEM	Common Evaluation Methodology	通用评估方法

4 安全要求概述

4.1 安全功能要求

为保证安全芯片具备移动支付的相应的安全功能，典型安全芯片包括处理器单元、安全算法模块、I/O接口、易失性和非易失性存储器等，整体共同构成了安全芯片安全功能基础。在表1中定义了移动支付安全芯片安全功能。

表1 安全功能要求

名称	描述
要求 1	安全芯片应提供对称和非对称的国密算法或国际密码算法的专用计算模块。
要求 2	安全芯片应提供真随机数发生模块，以产生真随机数辅助移动支付安全芯片实现其安全应用。
要求 3	安全芯片应具备环境异常检测处理机制，如温度检测、电压检测、时钟频率检测等，安全芯片应能够发现并识别异常；安全芯片应提供程序的正常运行和有效的监视管理器，如看门狗电路等，如果程序执行时出现异常，安全芯片应能够发现异常；安全芯片应具备逻辑模块异常情况的检测处理机制，如算法模块溢出，寻址空间越界等情况的处理，如果逻辑模块出现异常，安全芯片应能够发现异常；并按照安全芯片的容错机制进行相应的处理。
要求 4	存储器应提供相应的访问控制策略，对存储器的访问应遵循该机制，以防止对存储器的非法越权操作。
要求 5	芯片的敏感数据在使用后如需立即删除应按照相应的删除机制立即从存储器中删除。
要求 6	存储器中应有相应的只读区域存放PAMID。

安全功能要求和检测项的映射关系见附录B中表B.1。

4.2 抗攻击能力要求

为防范针对移动支付安全芯片的非入侵式、半入侵式和入侵式攻击等威胁，在表2定义了移动支付芯片抗攻击能力的安全要求，详见附录A。

表2 抗攻击能力要求

名称	描述
要求 1	应保证将安全芯片模块从安全芯片上移除会导致可见的损坏，如果在无可见损坏的情况下，应保证将安全芯片模块装回或替换，整个安全芯片无法工作。
要求 2	应保证触及IC表面或将安全芯片表面的覆盖层剥离，如环氧树脂或聚酰胺等，有较高概率破坏安全芯片，使安全芯片无法使用。
要求 3	应保证安全芯片具有抵抗物理测定储存器单元逻辑内容的保护能力。
要求 4	应保证存储器单元逻辑或安全芯片内部布线已暴露时，安全芯片具有抵抗根据存储器单元逻辑恢复有用代码或信息的能力。
要求 5	应保证安全芯片具有抵抗通过旁路分析导致存储器敏感信息暴露的保护能力，如分析运行安全芯片功耗图，电磁场辐射或者主要处理功能的时序等。
要求 6	应保证侵入安全芯片进行机械探测攻击难以暴露存储器代码和信息。

名称	描述
要求 7	应保证以电压对比和电子束探测等攻击方式难以暴露存储器信息。
要求 8	应保证安全芯片应用不受操作环境变化干扰的影响。如果探测到内部变化或时钟频率、电压、复位脉冲宽度以及温度等规范外的赋值，使其无效。
要求 9	应保证安全芯片应用的执行不受探测攻击的影响。
要求 10	应保证安全芯片存储器单元和保护系统不易被修改。如果修改需要由具有全面安全芯片设计知识人员使用高端专门工具才能实现。
要求 11	应保证安全芯片能够抵抗具有全面的安全芯片设计知识的人员使用高端专门工具通过FIB系统或激光切割机对安全芯片修改的能力。
要求 12	应保证安全芯片受到的光学错误攻击、电磁场和放射线干扰，不会影响应用程序的正确运行或进入一个安全的状态。
要求 13	应保证安全芯片的设计具有一定的难度性，攻击者必须通过大量的努力和使用高端专业工具才能对逻辑建立模块进行反向工程提取。

抗攻击能力要求和检测项的映射关系见附录B中表B.2。

5 安全功能要求检测

5.1 检测条件

安全芯片应包括处理器单元、安全算法模块、I/O接口、易失性和非易失性存储器等，整体共同构成了安全芯片安全功能硬件基础。

5.2 检测内容

5.2.1 密码算法

检测目的：验证安全芯片的对称密码算法、非对称密码算法是否符合相应的国密算法或国际密码算法标准。

检测方法：若安全芯片包含对称或非对称国密算法，查看是否具备相应的国密证书。

对于国际密码算法，验证安全芯片的对称密码或非对称密码算法是否符合相应的国际密码算法标准；

结果判定：对称算法或非对称算法符合相应标准。

5.2.2 随机数发生器

检测目的：验证安全芯片中的随机数产生器产生的随机数是否具备足够的随机性。

检测方法：验证安全芯片产生随机数的质量，进行 AIS 20、AIS 31、NIS SP800-22 或 FIPS 140-2 标准化的测试。

结果判定：满足标准化测试的要求。

5.2.3 异常检测机制

检测目的：验证安全芯片是否具备足够的异常检测机制，且能按照安全芯片的容错机制进行相应的处理。

检测方法：验证安全芯片产生异常时是否有相应的检测机制，包括环境异常检测、程序执行异常检测和逻辑模块异常检测，并按照安全芯片的容错机制进行相应的处理。

结果判定：能够对常见的异常进行检测，并按照安全芯片的容错机制进行相应的处理。

5.2.4 存储器访问控制机制

检测目的：验证对存储器进行访问时是否具备且遵循其相应的访问控制策略。
检测方法：查看对存储器是否具备相应访问控制策略且遵循其访问控制策略。
结果判定：具备存储器访问控制机制。

5.2.5 残余信息保护机制

检测目的：验证安全芯片是否采用相应的残余信息保护机制，即敏感数据在使用后如需立即删除应按照相应的删除机制立即从存储器中删除。
检测方法：查看安全芯片的残余的敏感数据在使用后是否立即从存储器中删除。
结果判定：具备相应的残余信息保护机制。

5.2.6 PAMID

检测目的：验证安全芯片存储 PAMID 的区域仅限一次写入，在写入后只可读取 PAMID，不可修改或覆盖。
检测方法：检查存储 PAMID 区域的保护措施和权限控制。
结果判定：存储 PAMID 区域满足规范要求。

6 抗攻击能力要求检测

6.1 检测条件

默认环境条件（温度、湿度等）是指常温20±3℃，相对湿度在20%-80%RH之间。如无特殊说明，后续案例均采用此环境条件。

6.2 检测内容

6.2.1 安全芯片表面准备

检测目的：验证安全芯片是否具备足够的保护能力以防止安全芯片表面覆盖层被移除。
检测方法：尝试在不损坏安全芯片的前提下使安全芯片表面暴露。
结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.2 安全芯片背部准备

检测目的：验证安全芯片是否具备足够的保护能力以防止安全芯片背部覆盖层被移除。
检测方法：尝试在不损坏安全芯片的前提下使安全芯片背部暴露。
结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.3 安全芯片表面简要分析

检测目的：验证安全芯片硬件设计是否具备相应的复杂性。
检测方法：参考公开性的文档尝试分析安全芯片标识信息、表面构造和设计规则等。
结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.4 安全芯片表面详细分析

检测目的：验证安全芯片硬件设计是否具备足够的复杂性。
检测方法：参考设计文档尝试分析安全芯片功能模块和安全敏感区域等。
结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.5 传输系统的物理位置探测

检测目的：验证安全芯片是否具备足够的保护能力以防止其传输系统的物理位置被探测。
检测方法：参考设计文档尝试通过反向工程定位传输系统的位置。
结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.6 传输系统的 FIB 修改

检测目的：验证安全芯片是否具备足够的保护能力以防止通过 FIB 修改传输系统。
检测方法：尝试使用 FIB 系统对传输系统进行连线或修改。
结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.7 逻辑建立模块的干扰

检测目的：验证安全芯片是否具备足够的保护能力以防止逻辑建立模块被干扰。
检测方法：参考详细设计文档尝试旁路或使逻辑模块的功能或安全性暂时失准或失效。
结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.8 逻辑建立模块的修改

检测目的：验证安全芯片是否具备足够的保护能力以防止逻辑建立模块被修改。
检测方法：参考详细设计文档尝试对逻辑模块的功能或安全性进行永久的修改。
结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.9 测试模式的重激活

检测目的：验证安全芯片是否具备足够的保护能力以防止测试模式被重激活或被旁路。
检测方法：参考详细设计文档尝试使安全芯片在测试模式下运行。
结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.10 利用安全芯片的测试特性

检测目的：验证安全芯片是否具备足够的保护能力以防止滥用测试特性以获取及修改相关敏感信息。
检测方法：参考详细设计文档尝试滥用测试特性以获取及修改相关敏感信息。
结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.11 非易失性 ROM 信息的泄露

检测目的：验证安全芯片是否具备足够的保护能力以防止通过形象化获取非易失性 ROM 的内容。
检测方法：参考详细设计文档尝试利用在工艺上的差异形象化 ROM，并恢复出 ROM 中的数据。
结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.12 被动探测

检测目的：验证安全芯片是否具备足够的保护能力以防止通过被动探测获取安全芯片中敏感信息。
检测方法：尝试对安全芯片进行被动探测，窃听数据总线和控制线，并记录数据。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.13 主动探测

检测目的：验证安全芯片是否具备足够的保护能力以防止通过主动探测来改变安全芯片的程序流程、实现功能或敏感信息。

检测方法：参考详细设计文档尝试对安全芯片进行主动探测，观察安全芯片运行状况。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.14 非易失性 ROM 信息的获取

检测目的：验证安全芯片是否具备足够的保护能力以防止通过主动及被动探测来获取非易失性 ROM 内容。

检测方法：参考详细设计文档，通过反向工程定位 ROM 的控制和地址总线，进而实施恶意操作。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.15 非易失性可编程存储器的直接读取

检测目的：验证安全芯片是否具备足够的保护能力以防止通过主动及被动探测直接读取 EEPROM 或 Flash 的内容。

检测方法：参考详细设计文档尝试通过主动及被动探测直接读取 EEPROM 或 Flash 单元的内容。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.16 非易失性可编程存储器信息的获取

检测目的：验证安全芯片是否具备足够的保护能力以防止通过探测获取 EEPROM 或 Flash 的内容。

检测方法：参考详细设计文档尝试通过反向工程定位 EEPROM 或 Flash 控制和地址总线，进而进行恶意操作。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.17 电压对比/电子束探测

检测目的：验证安全芯片是否具备足够的保护能力以防止通过形象化安全芯片表面电压以恢复存储器中敏感信息及其位置。

检测方法：参考设计文档尝试通过形象化安全芯片表面的电压恢复存储器中的秘密信息的位置及内容。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.18 供电电源操纵

检测目的：验证安全芯片是否具备足够的保护能力以防止通过供电电源操纵改变安全芯片程序流程，或导致安全芯片进入一个非预期或未定义的状态。

检测方法：参考设计文档尝试操纵安全芯片供电电源，观察安全芯片运行状态。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.19 其他非侵入式操纵

检测目的：验证安全芯片是否具备足够的保护能力以防止通过外部参数操纵改变安全芯片程序流程或导致安全芯片进入一个非预期或未定义的状态。

检测方法：参考设计文档尝试改变安全芯片各类参数（比如时钟、复位或 I/O 信号），观察并记录

安全芯片运行情况。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.20 电磁操纵

检测目的：验证安全芯片是否具备足够的保护能力以防止通过电磁操纵改变安全芯片程序流程或导致安全芯片进入一个非预期或者未定义的状态。

检测方法：参考设计文档尝试使用高压在安全芯片表面产生一个电场，观察并记录安全芯片运行情况。参考设计文档尝试使用强磁场在安全芯片的连线中引起电流，观察并记录安全芯片运行情况。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.21 光注入

检测目的：验证安全芯片是否具备足够的保护能力以防止通过光注入引起安全芯片运行中的错误、改变安全芯片程序流程或导致安全芯片进入一个非预期或者未定义的状态。

检测方法：参考设计文档尝试对安全芯片表面进行光注入，干扰安全芯片运行，观察并记录安全芯片运行情况。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.22 放射线注入

检测目的：验证安全芯片是否具备足够的保护能力以防止通过放射线注入而导致单粒子效应对安全芯片的影响。

检测方法：参考设计文档尝试通过放射线注入干扰安全芯片运行，观察并记录安全芯片运行情况。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.23 形象化重现功耗中隐含的信息

检测目的：验证安全芯片是否具备足够的保护能力以防止通过形象化重现功耗中隐含的信息，来获取安全芯片上运行的程序信息。

检测方法：参考设计文档尝试通过形象化功率消耗中隐藏的重复信息获取安全芯片上运行的程序信息。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.24 简单功耗分析（SPA）

检测目的：验证安全芯片是否具备足够的保护能力以防止通过简单功耗分析获取密钥信息。

检测方法：参考设计文档尝试对安全芯片进行简单功耗分析。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.25 差分功耗分析（DPA）

检测目的：验证安全芯片是否具备足够的保护能力以防止通过差分功耗分析获取密钥信息。

检测方法：参考设计文档尝试对安全芯片进行差分功耗分析。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.26 电磁辐射（EMA）

检测目的：验证安全芯片是否具备足够的保护能力以防止通过电磁辐射分析获取密钥信息或程序信

息。

检测方法：参考设计文档尝试对安全芯片进行电磁辐射分析。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.27 差分错误分析（DFA）

检测目的：验证安全芯片是否具备足够的保护能力以防止通过差分错误分析获取密钥信息。

检测方法：参考设计文档尝试对安全芯片进行错误注入并进行密钥获取分析。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.28 过程中断

检测目的：验证安全芯片是否具备足够的保护能力以防止强制中断导致安全芯片进入非预期或未定义状态。

检测方法：参考设计文档尝试在敏感操作过程中，执行各类中断，观察并记录安全芯片运行情况。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.29 传输信息分析

检测目的：验证安全芯片是否具备足够的能力以防止安全芯片中的传输信息被反向工程或分析。

检测方法：参考设计文档尝试对安全芯片中的传输信息进行反向工程或分析。

结果判定：根据附录 C 中的判定方法给出具体分值。

6.2.30 随机数发生器攻击

检测目的：验证安全芯片是否具备足够的保护能力以防止对真随机数发生器的攻击。

检测方法：参考详细设计文档尝试分析随机数发生器原理，并找出可利用的漏洞。

结果判定：根据附录 C 中的判定方法给出具体分值。

附 录 A
（规范性附录）
芯片抗攻击安全要求详细描述

A.1 芯片各部分抗攻击安全要求

本附录对安全芯片安全的要求划分为非易失性只读存储器、非易失性可编程存储器、易失性存储器、传输系统和IC建立模块几部分。针对这几部分易受到的泄露、干扰和修改威胁，本附录定义了每部分受到不同威胁时应具备的安全要求以及可采用的应对措施。由于本附录提出的防攻击可采取应对措施的目的是作为安全要求描述的理解说明使用，因此不是全部的防攻击措施。

芯片的各个部分对攻击者具有不同的意义，因此，面对潜在的泄露、干扰以及修改等多种威胁各部分应具备相应的抗攻击能力，应满足本附录所规定的不同安全要求。表A.1定义了各部分在受到不同攻击时应分别符合的安全要求，其中安全要求1-13为第5章第2节所定义的芯片安全要求。

表A.1 芯片各部分抗攻击安全要求

名称	应符合的安全要求
芯片封装安全要求	应符合安全要求 1、要求 2
只读存储器 ROM 防泄露	应符合安全要求 3、要求 4、要求 5、要求 6、要求 7
只读存储器 ROM 防干扰	应符合安全要求 8、要求 9
只读存储器 ROM 防修改	应符合安全要求 10、要求 11
非易失性可编程存储器防泄露	应符合安全要求 4、要求 5、要求 6、要求 7
非易失性可编程存储器防干扰	应符合安全要求 8、要求 9、要求 12
非易失性可编程存储器防修改	应符合安全要求 10、要求 11
易失性存储器防泄露	应符合安全要求 4、要求 5、要求 6、要求 7
易失性存储器防干扰	应符合安全要求 6、要求 7、要求 12
易失性存储器防修改	应符合安全要求 6、要求 11
传输信息防泄露	应符合安全要求 5、要求 6、要求 7
传输信息防干扰	应符合安全要求 6、要求 9、要求 12
IC 建立模块防泄露	应符合安全要求 13
IC 建立模块防干扰	应符合安全要求 6、8、9、12
IC 建立模块防修改	应符合安全要求 6、要求 11
测试模式安全要求	应符合安全要求 11

A.2 芯片封装安全要求

A.2.1 具有抵抗芯片剥离的保护能力

安全芯片的表面有一层保护层，通常由环氧树脂或聚酰胺等组成，因此，对安全芯片进行侵入式或半侵入式攻击时，须将芯片与塑料封装分离开，并将芯片表面的保护层移除。在具备了一定的化学方面经验后，采用热酸刻蚀除去这层保护。

安全要求：

——应保证将芯片模块从芯片封装中移除会导致可见的损坏。应保证装回或替换芯片模块容易导致可见的损坏；

——应确保触及IC表面或将芯片表面的覆盖层剥离时，有较高概率破坏芯片，使芯片无法使用。

A.3 只读存储器ROM安全要求

A.3.1 只读存储器ROM的安全需求

只读存储器ROM中通常包含操作系统和一些额外的测试应用程序代码。对ROM的攻击方式有物理侵入式、半侵入式和非侵入式攻击。攻击者利用操作系统和应用程序代码对芯片进行攻击，如克隆芯片或利用程序结构漏洞进行攻击。

A.3.2 具有抵抗只读存储器ROM信息泄露的保护能力

此部分要求主要为防止ROM中所储存信息受到攻击泄漏。ROM单元中存储的逻辑值以不同的物理形式实现，攻击者可通过使用带有高倍放大率显微镜和图象处理软件的分析设备，分析物理性质，以获取各个单元的逻辑状态，建立起整个芯片逻辑的反向工程。

对于程序执行过程中的信息可通过侵入ROM中数据存储模块内部进行窃听，如机械探测等。也可通过半侵入式窃听，如电压对比、电子束探测等。利用这些方法，攻击者就可以从输出总线端窃听存储器的信息数据。攻击者也会通过非侵入式攻击对执行的代码进行窃听，如功耗分析（SPA/DPA），时序分析或电磁泄露分析（EMA）等，利用分析的功耗数据或芯片运行时的一些电磁特征就可恢复芯片执行敏感功能的代码。

安全要求：

——应保证芯片具有抵抗物理测定储存器单元逻辑内容的保护能力；

——应保证存储器单元逻辑值或芯片内部布线已暴露时，芯片具有抵抗根据存储器单元逻辑值恢复有用代码或信息的能力；

——应保证芯片具有抵抗通过旁路分析导致存储器敏感信息暴露的保护能力，如分析运行芯片功耗图，电磁场辐射或者主要处理功能的时序等；

——应保证侵入芯片进行机械探测攻击难以暴露存储器代码和信息；

——应保证以电压对比和电子束探测等攻击方式难以暴露存储器信息。

A.3.3 具有抵抗只读存储器ROM受干扰的保护能力

芯片工作过程按照非易失性ROM中包含的操作系统及应用程序代码执行，因此保证ROM数据完整性、应用软件正确执行对安全芯片的安全有很重要作用。

攻击者通过侵入式、半侵入式和非侵入式攻击，在芯片应用在进行敏感功能特殊处理时，对软件运行指令正确性进行干扰。例如，主动机械探测干扰、光学错误攻击和电压控制等。目前，安全芯片存储器大都采用预充电原理工作的，此类存储器容易受到电压控制攻击。

安全要求：

——应保证芯片应用不受操作环境变化干扰的影响。芯片应能够探测到时钟频率、电压、复位脉冲宽度以及温度等规范外的值；

——应保证芯片应用的执行不受探测攻击的影响。

A.3.4 具有抵抗只读存储器ROM被修改的保护能力

运用聚焦离子束系统攻击ROM，可修改ROM单元逻辑值，但同时对多个单元作修改比较困难，成功率不高，因此攻击者为改变程序功能，对ROM修改的目的不是对ROM数据内容的修改，而是修改ROM的控制功能。如使存储器防火墙失效或关闭ROM功能模块的输出驱动等。关闭ROM功能模块的输出驱动，会迫使输出数据都归零导致CPU无操作指令（NOP）状态，导致地址总线上的数据被总线探测器窃听。对于一个熟练的攻击者来说，可以通过聚焦离子束实现对ROM逻辑的修改。

安全要求：

——应保证芯片存储器单元和保护系统不易被修改。如果修改需要由具有全面芯片设计知识人员使用高端专门工具才能实现；

——应保证芯片能够抵抗具有全面的芯片设计知识的人员使用高端专门工具通过FIB系统或激光切割机对芯片修改。

A.4 非易失性可编程存储器安全要求

A.4.1 非易失性可编程存储器的安全需求

非易失性可编程存储器包含的数据多为敏感数据，如每张SE唯一的信息，包括密钥，PAMID号码和PIN值，同时存储器中也包含一部分操作系统程序代码、应用程序代码和应用使用数据等。EEPROM、闪存都属于非易失性可编程存储器。

A.4.2 具有抵抗非易失性可编程存储器信息泄露的保护能力

可编程存储器中的信息可通过侵入式，半侵入式和非侵入式攻击遭到泄露。侵入式和半侵入式攻击需要对芯片逻辑建立反向工程。因为利用电子束探测的尖端设备探测时会损坏在浮栅上储存的单元内容，目前无法直接暴露出EEPROM单元逻辑。通过在存储器程序执行期间利用机械探测对总线进行窃听，可获取总线上的数据。

安全芯片被执行的代码也会受到非侵入式攻击而泄露信息，如功耗分析（SPA/DPA），时序分析或电磁分析（EMA）。通过分析芯片功耗情况或芯片运行中的电磁特性恢复出敏感代码。

安全要求：

——应保证存储器单元逻辑值或芯片内部布线已暴露时，芯片具有抵抗根据存储器单元逻辑值恢复有用代码或信息的能力；

——应保证芯片具有抵抗通过旁路分析导致存储器敏感信息暴露的保护能力，如分析运行芯片功耗图，电磁场辐射或者主要处理功能的时序等；

——应具有抵抗通过机械探测侵入芯片泄露存储器代码和信息的能力；

——应保证以电压对比和电子束探测等攻击方式难以暴露存储器信息。

A.4.3 具有抵抗非易失性可编程存储器被干扰的保护能力

非易失性可编程存储器内容的完整性对安全芯片应用的安全性有重要的影响。如果非易失性可编程存储器中存放了程序代码，那么对存储器的干扰就可能导致程序工作异常。如果储存器中存储数据被干扰而改变，应用就丧失了完整性。

对非易失性可编程存储器上的攻击，可采用侵入式，半侵入式还是非侵入式的，其目的均为修改存储器数据或程序代码输出值。攻击方法包括机械探测干扰、光学错误攻击和电压操控等。目前安全芯片中所使用的非易失性可编程存储器主要采用预充电原理的存储器，这种存储器易受到电压操控攻击。

安全要求：

——应保证芯片应用不受操作环境变化干扰的影响。芯片应能够探测到时钟频率、电压、复位脉冲宽度以及温度等规范外的值；

——应保证芯片应用的执行不受探测攻击的影响；

——应保证芯片受到的光学错误攻击、电磁场和放射线干扰，不会影响应用程序的正确运行或进入一个安全的状态。

A.4.4 具有抵抗非易失性可编程存储器被修改的保护能力

非易失性可编程存储器内容的完整性保证了安全芯片应用的安全性，如电子钱包，非易失性存储器上的数值是独特，因此其完整性至关重要。攻击者对EEPROM的修改通常不采用直接修改EEPROM中的数据。

采用主动机械探测，通过改变应用执行期间的某些数据修改其他应用数据。这些攻击不直接接触修改存储器单元，而是通过传输系统进行修改。

有些非易失性存储器在编程之后，能够变成只读的OTP存储器。该种存储器的闭锁机制即成为被攻击的目标。这些机制能够通过机械探测、激光切割或FIB修改的方式与一些软件结合使用被攻击。

安全要求：

——应保证芯片存储器单元和保护系统不易被修改。如果修改需要由具有全面芯片设计知识人员使用高端专门工具才能实现；

——应保证芯片能够抵抗具有全面的芯片设计知识的人员使用高端专门工具通过FIB系统或激光切割机对芯片修改。

A.5 易失性存储器安全要求

A.5.1 易失性存储器的安全需求

易失性存储器（RAM）是处理器的临时存储区域，当掉电的时候，它的内容会被擦除。攻击者对存储器进行攻击，目的是获取中间密码结果，如过程密钥或密码运算的子密钥。

A.5.2 具有抵抗易失性存储器信息泄露的保护能力

采用侵入式、半侵入式以及非侵入式攻击可实现RAM信息的窃听获取。侵入式攻击可通过机械探测存储器输出总线窃听数据。半侵入式攻击可通过电压比较或电子束探测窃听。利用电压对比进行半侵入式窃听需要长时间获取电压信息，并且要求密码运算结束后信息不被立即清除。电子束探测攻击存储器，监视全速处理时RAM内部位线的逻辑状态，一次监视一条总线，获取有限的数据量。非侵入式攻击可通过功耗分析（SPA/DPA）、时序分析或电磁分析（EMA）获取信息。例如利用非侵入式进行时序分析，可获取RAM的读写周期。

安全要求：

——应保证存储器单元逻辑值或芯片内部布线已暴露时，芯片具有抵抗根据存储器单元逻辑值恢复有用代码或信息的能力；

——应保证芯片具有抵抗通过旁路分析导致存储器敏感信息暴露的保护能力，如分析运行芯片功耗图，电磁场辐射或者主要处理功能的时序等；

——应具有抵抗通过机械探测侵入芯片泄露存储器代码和信息的能力；

——应保证以电压对比和电子束探测等攻击方式难以暴露存储器信息。

A.5.3 具有抵抗易失性存储器受干扰的保护能力

易失性存储器RAM中存储的数据中包含密码计算的中间结果，因此保证RAM的完整性对应用的安全性至关重要。对于RAM的干扰攻击可采用侵入式和半侵入式攻击，这些攻击在RAM读写数据时，对存储器的输出数值临时改变。如通过主动机械探测，临时拉低或抬高位线逻辑来改变RAM单元输出的内容。或利用光、电磁场或放射线的半侵入方式进行干扰攻击。

安全要求：

——应保证侵入芯片进行机械探测攻击难以暴露存储器代码和信息；

——应保证以电压对比和电子束探测等攻击方式难以暴露存储器信息；

——应保证芯片受到的光学错误攻击、电磁场和放射线干扰，不会影响应用程序的正确运行或进入一个安全的状态。

A.5.4 具有抵抗易失性存储器被修改的保护能力

随机存取存储器RAM存储的只是暂时信息，因此，对RAM内容永久性修改不适用，但通过对RAM功能修改与其它攻击方式联合可实现对RAM内容的获取。对RAM的修改攻击常采用侵入式攻击，如采用机械探测、激光切割或FIB修改等侵入式攻击实现对硬件RAM清空控制线的修改。

对RAM的半侵入式攻击可通过使用激光或电子束实现对RAM单元的晶体管的攻击，阻止单元的正当的操作。但是，目前利用RAM数据永久性修改进行攻击不常见，因此目前此类攻击不包含在RAM修改威胁中。

安全要求：

——应保证侵入芯片进行机械探测攻击难以暴露存储器代码和信息；

——应保证芯片能够抵抗具有全面的芯片设计知识的人员使用高端专门工具通过FIB系统或激光切割机对芯片修改。

A.6 信息传输安全要求

A.6.1 信息传输的安全需求

所有芯片处理的信息，包括操作系统、应用代码和应用数据都将会在存储器和处理器之间传输，传输通过各功能模块间的金属连线实现，如数据总线。由于总线的顺序传输承载了芯片处理的所有相关信息，因此极易受到攻击者的攻击。

A.6.2 具有抵抗传输信息泄露的保护能力

信息传输中可遭到侵入式、半侵入式或非侵入式的攻击导致信息泄露。其中最为常见的是侵入式机械探测，探针被放在数据总线上，对经过的信息进行监视。机械探测通过对数据总线进行连续窃听，可获得处理器运行代码的每个指令和字节数据，然后把窃听到的数据转换成存储器中的代码和数据。如果总线采用加密，则需要通过其他反向工程和数据分析恢复总线信息。

非接触探测是一种使用电子束探测的半侵入式攻击。电子束探测能够通过单独总线结点窃听获取该条总线数据流。因此8位总线的非侵入式攻击需要8个运行程序收集总线数据。芯片内部传输的信息通过非侵入式攻击也会遭到泄露，由于总线的驱动产生功耗，功耗的大小由数据决定，因此通过差分功耗分析或电磁分析能够推测传输信息的内容并获得总线上的数据。

安全要求：

——应保证芯片具有抵抗通过旁路分析导致存储器敏感信息暴露的保护能力，如分析运行芯片功耗图，电磁场辐射或者主要处理功能的时序等；

——应保证侵入芯片进行机械探测攻击难以暴露存储器代码和信息；

——应保证以电压对比和电子束探测等攻击方式难以暴露存储器信息。

A.6.3 具有抵抗传输信息被干扰的保护能力

传输系统（数据总线）传输的数据完整性对应用的安全十分重要。干扰会导致数据的丢失，破坏数据的完整性，从而导致应用的不安全。对传输系统的干扰可通过侵入式、半侵入式和非侵入式攻击来实现。

主动探测是干扰传输系统最通常使用的技术。一个或多个探针被放置在传输结点上并对经过的数据在适当的时刻进行改变。被改变的信息，可以是程序指令、跳转地址或数据，根据不同的应用和时机对数据进行不同干扰。通常通过干扰不直接获取秘密信息，而是将此类干扰与其它攻击技术结合起来以获取攻击者想要的信息。半侵入式攻击可通过改变总线驱动器的状态或在芯片的结点注入峰值电流和涡旋电流进行攻击。

安全要求：

——应保证侵入芯片进行机械探测攻击难以暴露存储器代码和信息；

——应保证芯片应用的执行不受探测攻击的影响；

——应保证芯片受到的光学错误攻击、电磁场和放射线干扰，不会影响应用程序的正确运行或进入一个安全的状态。

A.7 IC建立模块安全要求

A.7.1 IC建立模块的安全需求

芯片中有许多IC建立模块，这些建立模块对于攻击者来说很重要。如要想在ROM单元中恢复代码，攻击者必须知道每个独立单元的状况（逻辑“1”或者逻辑“0”），同时也要知道该单元如何与程序相关联的。这个关系是由一个叫做ROM解码器的硬件单元所决定的。要重新建立ROM代码，攻击者必须知道该建立模块的功能。攻击者关注的模块还包括中央处理器和协处理器、数据总线的位置和布线、测试逻辑和（模拟）传感器逻辑等。

A.7.2 具有抵抗IC建立模块信息泄露的保护能力

IC建立模块够使用反相设计被恢复，如通过化学刻蚀将设备的保护层逐层的剥离，重建芯片逻辑的电路图，根据电路图攻击者可找出与安全相关的结点，判断设计的薄弱之处。

安全要求：

——应保证芯片的设计具有一定的难度性，攻击者必须通过大量的努力和使用高端专业工具才能对IC建立模块进行反向工程提取。

A.7.3 具有抵抗IC建立模块受干扰的能力

芯片中除存储器和传输系统以外还包含了许多功能模块，如CPU、协处理器模块、安全模块、输入输出模块、中断处理模块、时钟产生和复位处理管理模块等。对这些模块的干扰，目的是使某些功能暂时性失效。常用的攻击方法有侵入式、半侵入式以及非侵入式的攻击。

通过主动机械探测攻击来实现侵入式干扰。例如在内部供电电压线上执行电压操控攻击。

采用半侵入式干扰攻击扰乱模块逻辑的正确性，如在CPU或者密码协处理器的模块上进行光注入，导致差分错误并进行分析获取密钥，通过电磁场也可以实现对功能模块的攻击。

非侵入式干扰攻击IC建立模块，例如在存储器上进行电压操控，对IC建立模块进行电磁场干扰以影响其正常工作。芯片可通过使用内部电压调节器来防止触点处使用的非侵入式电压操控。

安全要求：

——应保证侵入芯片进行机械探测攻击难以暴露存储器代码和信息；

——应保证芯片应用不受操作环境变化干扰的影响。芯片应能够探测到时钟频率、电压、复位脉冲宽度以及温度等规范外的值；

——应保证芯片应用的执行不受探测攻击的影响；

——应保证芯片受到的光学错误攻击、电磁场和放射线干扰，不会影响应用程序的正确运行或进入一个安全的状态。

A.7.4 具有抵抗IC建立模块被修改的保护能力

可利用FIB或激光切割器对芯片进行修改。例如通过在膨胀熔丝处的导电材料的沉积来进行膨胀测试熔丝的修复，用激光切割器除去保护层或切割线等。利用这些方法可实现一些模块的激活、失效或传感器功能失效等等。

安全要求：

——应保证侵入芯片进行机械探测攻击难以暴露存储器代码和信息；

——应保证芯片能够抵抗具有全面的芯片设计知识的人员使用高端专门工具通过FIB系统或激光切割机对芯片修改。

A.8 测试模式安全要求

A.8.1 芯片测试模式应保证不能被非法利用

测试模式是芯片出厂时，进行必要的功能验证所需的一种芯片状态。芯片在测试模式下，存储器中的数据不受保护，传感器等模块可以人为的激活和失效。如果攻击者能够将芯片从用户模式返回到测试模式，将会产生安全威胁。芯片应防止通过利用FIB或改写软件等方式使芯片从用户模式返回到测试模式，从而激活或失效一些模块，并利用测试模式的一些特性，完全读取存储器中的敏感信息。应保证芯片测试模式的特性不被非法利用。

安全要求：

——应保证芯片能够抵抗具有全面的芯片设计知识的人员使用高端专门工具通过FIB系统或激光切割机对芯片修改。

附 录 B
（规范性附录）
检测项和安全功能要求、抗攻击能力要求的映射

表B.1 检测项和安全功能要求的映射

安全功能要求 / 检测项	要求 1	要求 2	要求 3	要求 4	要求 5	要求 6
6．2．1	●					
6．2．2		●				
6．2．3			●			
6．2．4				●		
6．2．5					●	
6．2．6						●

表B.2　检测项和抗攻击能力要求的映射

抗攻击能力要求 / 检测项	要求1	要求2	要求3	要求4	要求5	要求6	要求7	要求8	要求9	要求10	要求11	要求12	要求13
7.2.1	●	●											
7.2.2	●	●											
7.2.3													●
7.2.4													●
7.2.5													●
7.2.6											●		
7.2.7									●		●		●
7.2.8										●	●		●
7.2.9								●	●	●	●	●	●
7.2.10				●				●				●	●
7.2.11			●	●									●
7.2.12						●				●			●
7.2.13						●			●	●			●
7.2.14				●		●			●		●		●
7.2.15				●		●					●		●
7.2.16				●		●			●		●		●
7.2.17				●			●						
7.2.18								●					
7.2.19								●					
7.2.20												●	
7.2.21												●	
7.2.22												●	
7.2.23					●								
7.2.24					●								
7.2.25					●								
7.2.26					●								
7.2.27								●				●	
7.2.28													
7.2.29				●									
7.2.30										●	●		

附 录 C
（规范性附录）
检测结果判定方法

C.1 计算攻击分值

本部分着重于分析攻击分值的因素，提供攻击分值的计算方法，并给出示例说明，为安全芯片安全测试评估提供理论依据。

C.2 标识和攻击

C.2.1 概述

攻击者在准备攻击已存在的威胁时必须首先识别出威胁。因此将攻击划分为标识和攻击两个阶段。

C.2.2 标识阶段

标识阶段主要是创建各种攻击思路，并论证攻击思路的可行性，包括设计攻击用测试设备。

C.2.3 攻击阶段

攻击阶段主要是通过分析以及利用标识阶段设计的测试设备来完成某项攻击。

C.3 需要考虑的因素

C.3.1 概述

在标识阶段和攻击阶段的分析和测试可以映射到以下 6 个具体因素：攻击时间、技术水平、安全芯片知识、安全芯片样本数、攻击设备以及开放样本/带有已知秘密信息的样本。通过对上述因素进行综合评分，可以量化安全芯片安全等级。下面将就这些因素进行讨论。

C.3.2 消耗时间

这里对于CEM中消耗时间进一步细化。尤其是，对于一周和几周进行了区分。对时间区间进行了如下划分：

表C.1 消耗时间的分级

消耗时间	标识阶段	攻击阶段
＜1小时	0	0
＜1天	1	3
＜1周	2	4
＜1个月	3	6
＞1个月	5	8
不可实施	*	*

CEM把“不可实施”定义为：在攻击者可用的时间范围内，攻击路径是不可利用的。

事实上，评估者也不大可能花三个月的时间攻击安全芯片。在评估结束时，评估者必须评定实施最小攻击路径所用的时间。这将计算进行攻击的时间，但不一定是评估者构建整个攻击所用的时间。

当攻击建立在先前的评估结果时，就必须要考虑消耗时间和专业技能，比如已经开发了一个类似安全芯片的SE产品的特定攻击。当然，不可能给出一个通用的指南。

“不可实施”可能取决于特定的攻击场景，比如下面的两个例子：

a) 假设 SE 用于一个在线系统，当 SE 只包含个人密钥或 PIN，并进一步假设这些密钥或 PIN 在 SE 挂失后几天之内就去激活。在这种情况下，如果攻击者需要一周时间获取密钥，那么这个攻击就是不实际的。

b) 假设一个 SE 包含系统级的密钥，即使个人的 SE 丢失后被锁死，还是可能用于欺诈。这种情况下，即使攻击者需要一年的时间，还是可以成功进行攻击。

因此，如果需要为“不可实施”的时间给出一个通用假设，那么 3-5 年是一个较好的源于时间的最坏情况（在这个时间之后，SE 的生成通常发生了改变，系统级的密钥也可能改变了）。然而，最好的规则似乎只能在特定的攻击场景下定义“不可实施”。

C.3.3 技术水平

指在应用领域或者产品类型等方面的通用知识等级。技术水平包括外行、精通、专家和多领域专家 4 等级，具体等级说明参见表 C.2。

表C.2 技术水平等级说明

专业级别	等级说明
外行	是指和专家和精通人员相比是外行，不具备专业技术的人员。
精通	熟悉安全特性以及典型攻击的人员。
专家	对安全芯片相关的算法、协议、硬件、安全的概念及原理等方面非常熟悉的人员，以及对新的攻击的定义、技术及工具非常熟悉的人员。
多领域专家	具有不同领域的专业知识的人员，且这些领域应严格不同，比如硬件和加密算法。

C.3.4 安全芯片知识

指获取特定的和安全芯片的专门技术。安全芯片知识包括公开、受限、敏感、关键和非常危及硬件设计 5 个等级，具体等级说明参见表 C.3。

表C.3 安全芯片知识等级说明

专业级别	等级说明
公开	和安全芯片相关的信息，每个人都很容易获取到（如，从互联网获取）的信息，或者可由厂商提供给任何客户的信息，这些都被认为是公开的。
受限	和安全芯片有关的信息（例如，从厂商技术规格说明书中获取的信息）；如果它是先申请后发放，并且发放需要注册，则此类信息也被认为是受限制的信息。
敏感	高层设计和低层设计资料。
关键	安全芯片设计实现相关资料和源代码。
非常关键硬件设计	这些知识不仅能够区分高级设计和低级设计，同时还包括产品的原理图和源代码。

C.3.5 安全芯片样本数

攻击场景可能需要多个安全芯片样本，根据攻击者需要获取安全芯片的样本数，将其分为以下 4 个等级， ≤10 个样本，≤100 个样本，>100 个样本，以及不可实施。

表C.4 安全芯片样本数的分级

	标识阶段	攻击阶段
<10样品	0	0
<100样品	2	4
>100样品	3	6
不可实施	*	*

对“不可实施”做如下解释：

- 对于标识：“不可实施”表示所需样品数大于 2000 个，或者大于一个整数，这个整数是小于或等于 $\frac{n}{1+(\log n)^2}$ 的最大整数，这里 n 是估计产品生产数。
- 对于利用：“不可实施”表示所需样品数大于 500 个，或者大于一个整数，这个整数是小于或等于 $\frac{n}{1+(\log n)^3}$ 的最大整数，这里 n 是估计产品生产数。

C.3.6 攻击设备

指那些用来分析或攻击漏洞的设备，需要的攻击设备等级分为无、标准、专业、定制及多个定制共 5 个等级。具体等级说明如表 C.5 所示。

表C.5 攻击设备等级说明

攻击所需设备	等级说明
无	不需要攻击设备。
标准	指用于分析漏洞或者进行攻击的，对攻击者来说可以快速使用设备。这类设备很容易获取，例如，已经在市面上公开销售或者从互联网下载下来的。这类设备可能包含简单的攻击脚本，个人计算机，读卡器，模式发生器，简单光学显微镜，供电电源或者简单的机械装备。
专业	攻击者不能马上获取，但是可以经过正当途径获得的设备。这包括购买中等数量的设备，（例如，专门的电子卡片，专用的测试平台，协议分析器，示波器，微探针工作站，化学工作台，精确铣床设备等等）或者开发更多的攻击脚本或程序。
定制	指对公众来说还没有的设备，可能需要专门的定制，（例如，非常专业的软件）或者因为设备太专业，控制发放，甚至是严格限制。也有可能是这个设备非常昂贵（例如：离子聚焦光束、扫描式电子显微镜以及激光打磨器）可以租用到的定制设备可以视为专门设备，在分析阶段开发的软件也可认为是定制设备。
多个定制	不同攻击步骤需要不同类型的定制设备。

C.3.7 开放样本/带有可调参数的样本

开放样本是指评估员加载了带有目的性的软件到硬件平台上的样本，或是硬件平台上开放了可调

的参数。此操作的目的是使用不具有软件抗攻击手段的测试软件进行评估，且不会使 IC 内部抗攻击机制失效，另一种可能性是评估员能够自主定义一个或多个可调的参数，如一些安全机制的开关。

开放样本包括带有可调参数的样本，即评估员知道或者能够定义一个或多个可调参数的、的样本，比如用于旁路一些安全措施。

开放样本/带有可调参数的样本主要用于复杂评估，而不是重复的硬件评估。只有当不使用开放样本/带有已知可调参数的样本进行攻击不可实施时，才会使用开放样本/带有可调参数的样本进行攻击。

开放样本/带有可调参数的样本包括公开、受限、敏感和关键 4 个等级，具体等级说明如表 C.6。

表C.6　开放样本/带有已知秘密信息的样本等级说明

开放样本	等级说明
公开	开放样本：样本无保护，无发布控制，或 IC 用于非安全应用。 带有可调参数的样本：相关的安全参数没有可调节的外部接口。
受限	开放样本：受到 SE 的说明书、IC 的数据手册等典型保护，或发布没有额外的控制，IC 用于非安全应用。 带有可调参数的样本：提供可调节的安全参数，已知可调节参数对于攻击者可用。
敏感	开放样本：高层设计/低层设计受保护。 带有可调参数的样本：除关键安全参数之外的安全参数全部可调，已知可调节参数对于攻击者可用。
关键	开放样本：实现级受保护，这要求非常少的开放样本被生产，并且有非常严格的发布控制，确保接收机构能被设置相同级别的控制。 带有可调参数的样本：关键安全参数可调，已知可调节参数对于攻击者可用。

C.4　攻击分值计算方法

上一节分析了决定攻击分值的因素。表 C.7 给出了各个因素的评分规则。当某个因素接近一个边界时，评估员应当考虑表格中相关两个数值的中间值。

针对一个既定的攻击，提出多种攻击场景的分值计算是必要的。(例如：替换专业人员的攻击时间和设备)。保留这些方案的最低分值。当分析出一个威胁，并且这个是在公用域中，则标识分值应该选用攻击者在公用域中提出攻击方案的分值，而不是最初来标识它的分值。

设计出一个攻击场景后，首先对标识阶段和攻击阶段分别进行6个因素的等级评估，然后依据表C.7查表分别计算出标识阶段和攻击阶段的攻击分值，总攻击分值＝分析阶段攻击分值＋攻击阶段攻击分值，当针对某测试案例设计的攻击场景的总攻击分值超过该测试案例规定要求的最小攻击分值，表示该测试案例符合安全要求。

只有当不使用开放样本/带有已知秘密数据的样本进行攻击不可实施时，方才使用开放样本/带有已知秘密数据的样本进行攻击，然后分别计算两者的攻击分值，该测试案例的最终攻击分值由两者中较小的一个决定。

表C.7　攻击分值汇总表

因素	范围	标识阶段分值	攻击阶段分值
攻击时间	≤小时	0	0
	≤1 天	1	3
	≤1 星期	2	4
	≤1 月	3	6

因素	范围	标识阶段分值	攻击阶段分值
	>1 月	5	8
	不可实施	*	*
技术水平	外行	0	0
	精通	2	2
	专家	5	4
	多位专家	7	6
安全芯片知识	公开	0	0
	限制	2	2
	私有	4	3
	危及	6	5
	非常危及硬件设计	9	N/A
安全芯片样本数	≤10 个	0	0
	≤100 个	2	4
	> 100 个	3	6
	不可实施	*	*
攻击所需设备	无	0	0
	标准	1	2
	专用	3	4
	定做	5	6
	多个定做	7	8
开放样本	公开	0	N/A
	受限	2	N/A
	敏感	4	N/A
	危及	6	N/A

注：*的具体分值可根据C.3.5的描述进行定义，*的具体分值参考C.3.5中的公式进行计算，N/A为不适用。

C.5 攻击示例

C.5.1 概述

本攻击目标在于使用 SPA 获取 DES 加密密钥。

攻击分为标识阶段和攻击阶段。

C.5.2 标识阶段

标识阶段主要工作是通过形象化功率消耗中隐藏的重复信息来获取安全芯片上加密算法时序信息。

标识阶段所需攻击时间约 1 天。

标识阶段所需技术水平包括自相关技术、编程知识、中等的密码学知识、信号分析、中等级别的电子工程知识，属于多领域专家等级。

标识阶段所需安全芯片知识包括数据手册和其它由制造商在严格的保密协议框架下给 SE 制造商和买家提供的信息，属于受限等级。

标识阶段所需安全芯片样本数小于 10 个。

标识阶段所需攻击设备包括个人计算机和 SE 读卡器等属于标准设备，示波器属于专业设备。

C.5.3 攻击阶段

攻击阶段主要工作是通过简单功耗分析获取密钥信息。

攻击阶段所需攻击时间≤1 月。

攻击阶段所需技术水平包括编程知识、中等的密码学知识、信号分析、中等级别的电子工程知识，属于多领域专家等级。

攻击阶段所需安全芯片知识包括数据手册和其它由制造商在严格的保密协议框架下给 SE 制造商和买家提供的信息，属于受限等级。

攻击阶段所需安全芯片样本数小于 10 个。

攻击阶段所需攻击设备包括个人计算机和 SE 读卡器等，属于标准设备，示波器属于专业设备。

查表得出本次攻击分值的计算示例如下表：

表C.8 攻击分值计算示例

因素	标识值		攻击值	
攻击时间	≤1 天	1	≤1 月	6
技术水平	多领域专家等级	7	多领域专家等级	6
安全芯片知识	受限	2	受限	2
安全芯片样本数	≤10 个	0	≤10 个	0
攻击设备	专业	3	专业	4
开放样本	无	0	无	0
每个阶段攻击分值		13		18
总共攻击分值		31		

参 考 文 献

[1] Security Guidelines for Smart Card Integrated Circuits
[2] Q/CUP 040.1-2011　银联卡芯片安全规范 第1部分：芯片集成电路安全规范