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

的秘密参数子集合的假设值是否正确。以此来提取安全功能运算中的相关信息。

3.5

差分能量分析　differential power analysis

为提取与加密操作相关的信息，对密码模块的用电功耗的变化所作的分析。

[GB/T 25069—2010，定义 2.2.2.11]

3.6

电磁分析　electromagnetic analysis

对密码模块中由于逻辑电路转换所造成的电磁辐射的分析。用来提取对应于安全功能操作的信息以及后续提取秘密参数，例如密钥。

3.7

水平攻击　horizontal attack

从单条能量迹中的不同部分提取敏感信息的方法。

3.8

能量分析　power analysis

密码模块的能耗分析。用来提取对应于安全功能操作的信息以及后续提取秘密信息，例如密钥。

3.9

矩形攻击　rectangle attack

在观察采集阶段混合了水平和垂直攻击的方法。

3.10

侧信道分析　side-channel attacks

对密码设备的瞬时侧信道泄露的利用。这些泄露依赖于设备所处理的数据以及检索秘密参数时所执行的操作。

3.11

简单电磁分析　simple electromagnetic analysis

对指令执行模式和逻辑电路活动模式的直接（主要是可视化的）分析。这些模式主要来源于监视密码模块的电磁辐射变化，用以揭示密码算法的特征和实现，并后续揭示秘密参数的值。

3.12

简单能量分析　simple power analysis

对指令执行（或单个指令的执行）模式的直接（主要是可视化的）分析，它与密码模块的能耗有关，并用以获取密码操作相关的信息。

3.13

计时分析　timing analysis

对安全功能中某个操作的响应或执行时间变化进行分析，这种时间变化可能揭露出与诸如密钥或PIN等安全参数有关的信息。

3.14

垂直攻击　vertical attack

从多次不同的算法执行过程中提取敏感信息的方法。

4　符号和缩略语

4.1　符号

GB/T 37092 中所使用的以及下面给出的符号适用于本文件。

A：密码运算

C:观测量处理函数,默认为恒等变换
d_C:观测量处理函数的多项式次数
d_D:统计测量函数的多项式次数
d_o:观测量维度
F:函数,即操作
i:索引
K:密钥
k1:子密钥 1
k2:子密钥 2
M:泄露模型
N:观测量的数量
o_i:观测量
(o_i)_i:第 i 次观测值
pred_i:预测值
x1_i:x1 的第 i 次循环值
x2_i:x2 的第 i 次循环值
X:输入文本
*:乘法符号

4.2 缩略语

GB/T 37092 中所使用的以及下面给出的缩略语适用于本文件。
ASIC:专用集成电路(Application Specific Integrated Circuit)
CSP:关键安全参数(Critical Security Parameter)
DEMA:差分电磁分析(Differential Electro Magnetic Analysis)
DPA:差分能量分析(Differential Power Analysis)
EM:电磁(Electro-Magnetic)
EMA:电磁分析(Electro Magnetic Analysis)
FPGA:现场可编程门阵列(Field-Programmable Gate Array)
HD:汉明距离(Hamming Distance)
HW:汉明重量(Hamming Weight)
PA:能量分析(Power Analysis)
PIN:个人识别码(Personal Identification Number)
RNG:随机数发生器(Random Number Generator)

5 非入侵式攻击方法

5.1 概述

非入侵式攻击利用的密码模块中产生的侧信道信息(从密码系统的物理实现中获得的信息)主要包括:

——计算时间;
——能量消耗;
——电磁辐射。

对应的攻击为:

——计时分析攻击，主要通过密码模块固有接口（包括但不限于）对密码运算的总体计算时间进行记录；

——能量分析攻击，一般从电源供电端或者电路接地端对密码模块的整体能量消耗进行采集；

——电磁分析攻击，主要利用电磁探头对密码模块的密码运算模块进行更为精确的电磁辐射采集。

5.2 命名及分类

本文件规定了一种形式化的命名方法（见图1），以突显不同攻击之间的关系。当需要对新的攻击命名时，可参考该命名方法。

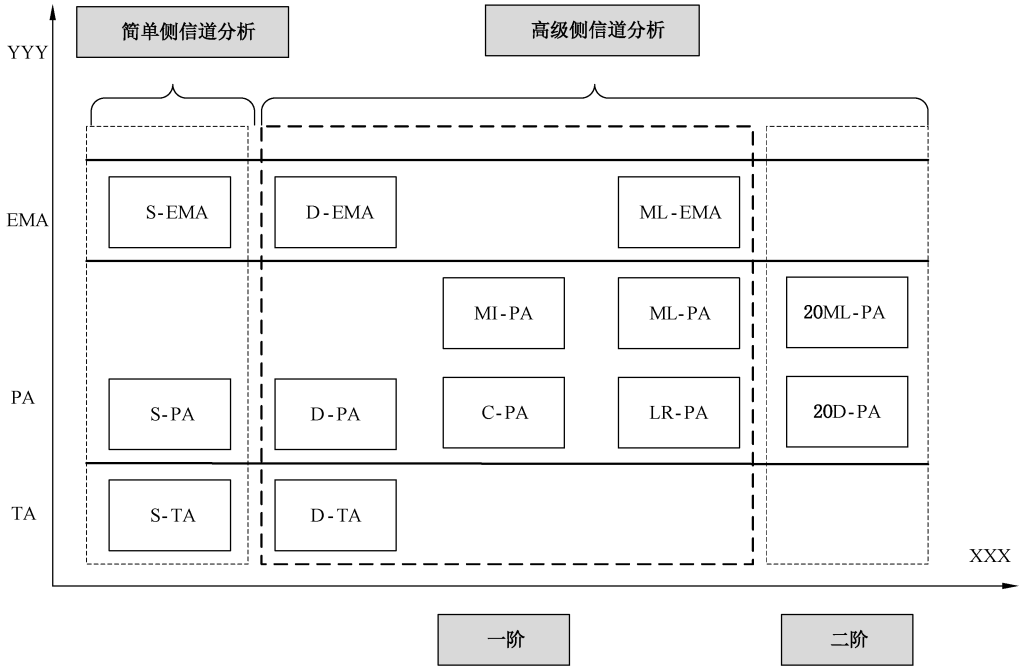

图1 形式化的侧信道命名方法

应按照如下的方式描述一个攻击：〈XXX〉-〈YYY〉-〈ZZZ〉。

XXX（见图1横轴）代表在攻击中使用的统计学方法，如〈S〉代表Simple，即简单分析，〈C〉代表Correlation，即相关性统计，〈MI〉代表Mutual Information，即极大似然统计，〈ML〉代表Maximum Likelihood，即互信息统计，〈D〉代表Difference of Means，即均值差分统计，〈LR〉代表Linear Regression，即线性回归方法等。若需表示一种产生d阶能量的预处理方法，可采用〈dO〉方式表达，如〈dOC〉、〈dOML〉，表示d阶相关性攻击以及d阶极大似然攻击（这种方式既可表示将能量迹中单个目标时刻的能量消耗自乘为d次方，也可表示对每条能量迹上d个点的能量消耗进行结合）。

YYY（见图1纵轴）代表观测到的侧信道类型，如〈PA〉代表能量分析，〈EMA〉代表电磁分析，〈TA〉代表计时分析等。

ZZZ代表攻击方法的特点，如〈P〉代表刻画攻击，〈UP〉代表非刻画攻击，其中刻画攻击是指攻击人员能够事先对目标设备的真实侧信道泄露模型进行精准建模的一种攻击方式，非刻画攻击反之。该项为可选项，默认的值为〈UP〉。在整体攻击名称前可附加一个形容词用以指明攻击的工作方式。该工作方式可为“垂直的”（默认模式），“水平的”或者“矩形的”。

5.3 分析流程

本文件根据是否使用统计分析方法，将非入侵式侧信道分析流程分为简单侧信道分析流程和高级

侧信道分析流程。

简单侧信道分析流程通常为:通过直接(主要是可视化的)或是肉眼识别的分析方法对密码模块的运行时间、能量消耗或是电磁泄露进行检测分析,从而揭示密码算法的秘密参数。

高级侧信道分析通常包括如下步骤:

a) 对观测量(o_i)进行 N 次测量,每次测量对应一次以已知输入 X 和密钥 K 为参数的密码运算 A;

b) 为设备选择泄露模型 M;

c) 选择观测量处理函数 C(默认情况下,C 被设置为恒等变换);

d) 对密钥 K 或者其子密钥的可能值进行假设,记为 h;

e) 从 A,h,(o_i)_i 以及可能的 M 中推测出 N 个预测值 pred_i(每个预测值对应一个明文,且该明文对应的观测量已被获取);

f) 选择统计测试函数 D,并计算 D[pred_i,C(o_i)];

g) 如果 D[pred_i,C(o_i)]大于某一阈值,则认为假设值 h 正确。否则,认为假设值错误,回到步骤 d)并重新选择假设值 h。

其中,步骤 b)和步骤 c)是可选项。步骤 g)中的阈值应根据实际的攻击方法进行选取。一种经典的方法是选取与所有密钥假设对应的 D[pred_i,C(o_i)]中的最大值作为阈值。观测量 o_i 可是单变量也可是多变量。当 o_i 为多变量时,o_i 中的每一个变量对应于不同的时刻的测量量。o_i 的维度可用 d_o 表示。观测量处理函数 C(.)是一个多项式函数,定义在 d_o 维的实数向量集合上,下文用 R^{d_o} 表示,多项式的次数用 d_C 表示。函数 D(pred_i,.): X→D(pred_i,X)表示一个包含 X 的多项式,多项式次数为 d_D,值 d_C * d_D 为攻击的阶数 d。

碰撞攻击是一种特殊的高级侧信道分析方法,其分析流程主要包括:

a) 对观测量(o_i)进行 N 次测量,每次测量对应一次以已知输入 X 和密钥 K 为参数的密码运算 A;

b) 从能量迹 o_i 中的不同运算时刻提取特征点;

c) 对差分值(k1−k2)的可能值进行假设,假设值记为 h,其中 k1、k2 分别是目标密钥 K 的两部分(即分组密码实现中的两个子密钥);

d) 根据差分假设值 h 对每个观测量(o_i)_i 进行分组;

e) 如果假设差分值 h 与真实的子密钥差分值相同,则该差分值所对应的观测量 o_i 分组在选取的不同特征点上存在强关联。

例如,攻击以 F(x1_i+k1)的操作为目标,则攻击将从观测量 o_i 中提取出与 F(x1_i+k1)及另一个 F(x2_i+k2)操作相关的特征点,并且这些观测量将会根据 h 进行重新分组,每组中的观测量满足性质 x2_i−x1_i=h。为了证实这个假设 h,通常采用相关系数作为测试函数 D,当 h 正确预测了 k1−k2 的差值,则第 h 组中的观测量在 F(x1_i+k1)与 F(x2_i+k2)对应的两部分特征点上存在高相关性。

本节中描述的所有攻击包括垂直攻击、水平攻击以及矩形攻击(即水平和垂直攻击):

——垂直攻击方法中,每个观测量 o_i 对应于一次不同的算法运算;

——水平攻击方法中,所有的 o_i 对应于同一次算法运算;

——矩形攻击方法中,o_i 中的一部分对应于同一次算法运算而另一部分对应于不同的算法运算。

在本文件中,垂直攻击是默认的攻击方法。

5.4 与安全功能的关联性

本节所述的非入侵式攻击方法与 GB/T 37092 中涉及的非入侵式安全的安全功能相关联,安全功能见 GB/T 37092—2018 中附录 C,非入侵式攻击方法与安全功能的关联性见表 1。实际使用中本文件可与 GB/T 37092—2018 配合使用。

表 1　非入侵式攻击方法与安全功能的关联性

核准的安全功能		非入侵式攻击方法		
		计时分析攻击	能量分析攻击	电磁分析攻击
分组密码	GB/T 32907 SM4 分组密码算法	适用	适用	适用
流密码	GM/T 0001 祖冲之序列密码算法	适用	适用	适用
非对称密码算法	GB/T 32918 SM2 椭圆曲线公钥密码算法	适用	适用	适用
	GM/T 0044 SM9 标识密码算法	适用	适用	适用
杂凑函数	GB/T 32905 SM3 密码杂凑算法	适用	适用	适用

表 1 中“适用”指的是存在针对该安全功能的攻击。计时分析攻击对 SM4 适用指的是存在缓存计时分析攻击可恢复 SM4 中的关键安全参数。计时分析攻击、能量分析攻击、电磁分析攻击对 SM3 密码杂凑算法适用指的是在利用 SM3 进行密钥流或其他关键安全参数生成的应用场景下存在相应的攻击技术。

6　非入侵式攻击缓解技术

6.1　概述

本文件针对计时分析攻击、能量分析攻击以及电磁分析攻击，分别提出相应的缓解技术以减轻上述攻击可能给密码模块带来的安全威胁。应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，选择有针对性的缓解技术来抵抗已知的非入侵式攻击威胁。

计时分析攻击主要利用与密钥相关的指令操作间存在的时间差异来展开攻击。本文件列举了几种通用缓解技术，包括平衡指令分支技术、随机延时插入技术、盲化操作技术等。

能量分析攻击主要分为简单能量攻击和差分能量攻击两大类。前者需要直接（例如通过视觉）分析密码模块在执行过程中出现的与关键安全参数相关的指令能量消耗模式，而后者则通过使用统计方法（例如均值差、相关系数）对收集到的大量能量消耗进行统计分析，以获取关键安全参数。为了抵抗此类攻击进而有效引导密码算法实现人员在其实现的密码算法中添加相应的能量分析抵抗力，本文件列举了一些常见的能量分析攻击缓解技术（主要分为隐藏技术和掩码/盲化技术两大类），以及一些在最新的研究成果中提出的其他缓解技术。

电磁分析攻击主要利用密码模块在运行过程中产生的电磁辐射能量消耗来恢复密码模块在运算过程中使用的关键安全参数。与能量分析攻击中主要对密码模块的整体能量消耗值进行测量不同，电磁分析攻击能更精确的探测密码模块中局部模块产生的电磁辐射消耗，拥有更高的攻击精度。由于电磁辐射泄露的主要来源是密码模块中与指令操作和数据操作相关的电流波动，本章涉及的针对能量分析攻击的缓解技术也有助于缓解电磁分析攻击，此外，针对电磁分析攻击的特有缓解技术见 6.4。

附录 A 列举了几种针对 SM2/SM9 和 SM4 密码算法的非入侵式攻击缓解技术。

6.2 计时分析攻击缓解技术

6.2.1 平衡指令分支技术

平衡指令分支技术通过检查密码模块中出现的所有与关键安全参数相关的指令分支，在密码模块特性允许的情况下尽可能的降低不同分支的指令执行总时间方差，从而平衡指令分支，利用固定时间的指令执行特性来对抗计时分析攻击。

6.2.2 随机延时插入技术

随机延时插入技术通过在密码算法的实现过程中插入随机延时操作来对抗计时分析攻击。该方法可有效降低攻击者对与关键安全参数相关的指令执行时间的测量精确度。从攻击者所需的计时次数来讲，攻击者实施一次成功的攻击所需的计时次数与引入的时间噪声的平方成正比。例如，一个模幂运算器的自身运算时间标准差为 n 毫秒，且使用计时分析攻击可在 x 次计时测量中恢复其使用的关键安全参数，当引入随机延时使模幂运算器的自身运算时间标准差变为 m 毫秒，攻击者所需的计时测量次数将变为 $y=(m/n)^2*(x)$。

6.2.3 盲化技术

盲化技术通过将密码运算所需的时间完全随机化，使得计算过程中产生的计算中间值不可预测，以抵抗计时分析攻击。该技术主要用在签名过程中。在每次签名开始之前，利用随机数发生器(RNG)生成两个随机数(vi,vf)，此后随机数 vi 与待签明文消息进行结合，使得后续的签名过程中所有操作均无法预测。为最终获得正确的签名结果，vf 可由 vi 推导得到，对由盲化消息产生的签名结果进行补偿，得到正确的明文消息签名结果。

6.3 能量分析攻击缓解技术

6.3.1 隐藏技术

常见的隐藏技术分为时间维度的隐藏技术和振幅维度的隐藏技术两种。时间维度的隐藏技术主要针对差分能量分析攻击需要收集能量曲线上固定时刻点的能量消耗来进行统计分析。若该条件不能满足，则攻击难度大幅提高。振幅维度的隐藏技术中，可通过使用双轨预充电逻辑以及引入额外噪声等方式来产生恒定电压幅值或随机化测量电压幅值，进而隐藏包含关键安全参数的中间值的能量消耗。

a) 时间维度隐藏技术

1) 随机插入伪指令技术

随机插入伪指令技术通过随机插入空指令或一些无效指令来改变密码算法指令序列，降低由敏感中间值产生的真实能量消耗在固定时刻点的出现概率，增加能量分析攻击的难度。该技术易于在密码模块部署，且不会增加额外计算开销。但是，该技术存在指令模式易被识别、算法加密总时间不一致等问题，使得该缓解技术仍会被一些常见的攻击技术破解，如简单能量分析。随机插入伪指令的缓解技术宜作为最低安全级别的缓解技术来使用。

2) 伪轮运算技术

伪轮运算技术主要通过在密码算法轮函数的各模块之间随机插入伪轮运算来随机化算法执行流程。伪轮运算可采用同时插入正向与逆向轮函数对的方式实现，而伪轮函数对的轮密钥为固定值，与密码算法自身设置的密钥相互独立，且正向加密轮运算和逆向解密轮运算的轮密钥相同，轮顺序相反。攻击者难以确定算法内部运算数据与电路运行功耗时间点之间的对应关系，继而有效隐藏与关键安全参数相关的能量消耗。

3） 时钟随机化技术

时钟随机化技术主要在硬件电路层面而非算法逻辑层面实现。该技术通过对电路时钟频率的随机改变(例如多种时间频率间的随机切换)来扰乱硬件电路的能量功耗,使攻击者无法准确同步时钟信号和能量功耗曲线,进而隐藏密码算法内部信息。

4） 乱序操作技术

乱序操作技术通过随机化密码算法的指令执行序列来缓解能量分析攻击。为保证密码算法安全实现的同时避免过大的额外性能开销,乱序操作所针对的指令对象应根据密码模块期望达到的安全等级有针对性的部署。以 SM4 密码算法为例,为抵抗攻击者仅通过穷举 8 比特的子密钥空间可开展的统计分析,在实际的乱序操作中,应对首轮 F 函数中的每个 S 盒非线性变换进行乱序保护。为达到更高级别的安全性,如抵抗攻击者通过穷举 32 比特的子密钥空间所开展的统计分析攻击(如选择 SM4 第一轮加密中的 F 函数输出值作为攻击中间值),算法中所有包含少于 32 比特密钥值的中间值操作指令都应采用乱序防御方案进行保护。

b） 振幅维度隐藏技术

1） 双轨预充电逻辑技术

当密码模块采用硬件方式(如 ASIC 和 FPGA)实现时,可采用双轨预充电逻辑技术来抵抗能量分析攻击。其中,双轨电路是指在正向的逻辑运算电路的基础上另外添加一条传输反向信号的逻辑电路,如图 2 所示。理论上,该技术可使整个逻辑电路在运行过程中各个时刻的汉明重量能量消耗保持恒定。在实际部署中,逻辑电路的布线方式对密码模块的整体能量消耗存在影响,双轨电路中所有导线的布线方式应以一种平衡的方式进行,以保证正向和反向逻辑电路之间产生的能量消耗总和保持恒定。

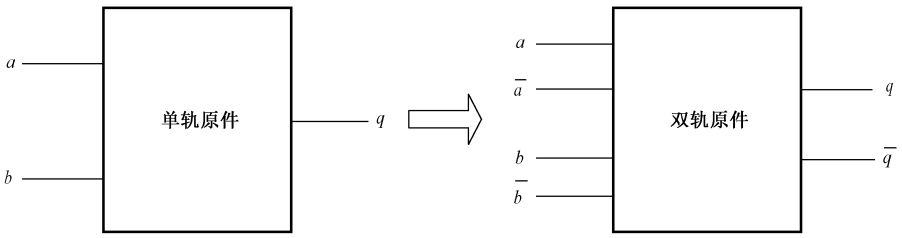

图 2 单轨元件和双轨元件

预充电机制应与双轨逻辑同时使用,以补偿另一种常见的电路能量消耗模式,即汉明距离泄露。汉明距离能量消耗对应于数字逻辑电路中逻辑元件的输出值在相邻的时钟周期上产生变化的比特位数总和,预充电机制为了保证各元件在每个时钟周期上的汉明距离值保持恒定,将整个电路的工作模式分为计算阶段和预充电阶段。在计算阶段中,各互补元件对产生完全相反的输出信号,而在预充电阶段中,所有元件的输出值被设置为预充电值,全 0 或者全 1。整个电路在计算阶段和预充电阶段之间切换,以保证任意阶段中各互补元件对之间产生的汉明距离能量消耗均保持恒定。

由于预充电阶段的存在,与组合逻辑元件输出端相连的时序元件部分需要进行特殊处理。以寄存器为例,为保证存储正反电路逻辑信号的互补寄存器对之间的值在预充电阶段之后依然有效,互补寄存器对应由前后共两级的寄存器组所替代。当第一级寄存器组 R1、R2 处在预充电阶段时,第二级寄存器组 R3、R4 与其后相连的逻辑电路处于计算阶段。而当第二级寄存器组处于预充电阶段时,第一级寄存器组则保存了与其输入端相

连的逻辑电路在上一个计算阶段中产生的电路正确运行中间值。双轨预充电逻辑寄存器组 R1、R2、R3、R4 时序图见图 3。通过这种方式，整个双轨预充电逻辑可保证计算电路的计算逻辑与单轨情况下完全相同，在抵抗能量分析攻击的同时确保输出正确的电路运算结果。

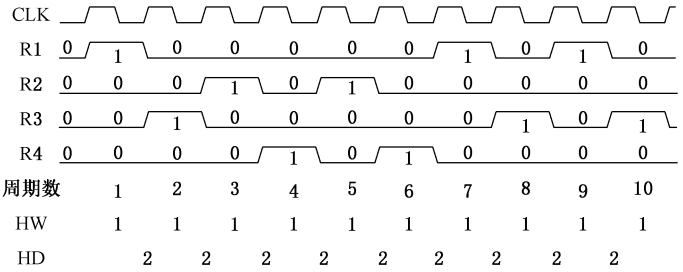

图 3　双轨预充电逻辑寄存器组时序图

2）　信号滤波与噪声叠加技术

能量分析攻击主要利用密码模块能量消耗中的信号分量进行统计分析，可通过降低信噪比的方式隐藏实际的信号分量。其中，降低信号噪声的方法包括引入恒流电源、使用双电容进行周期性切换供电，或在电源或接地端引脚插入滤波器等方式；增加噪声分量的方法包括但不限于将随机数发生器与大电容构成的网络相连，以进行随机充放电操作，从而增加噪声分量等。

3）　低功耗设计技术

集成电路的低功耗设计主要通过动态电压调节，并行结构设计，低功耗单元库启用以及低功耗状态即编码等方式来有效降低电路的总体能量消耗，进而相对应的大幅降低整体电路的信噪比，达到有效隐藏与关键安全参数相关联的能量消耗的目的。

4）　复合寄存器技术

密码模块的能量消耗大部分来自电路寄存器。为隐藏这部分与敏感中间值相关的寄存器能量消耗，复合寄存器系统使用一组共 4 个寄存器取代原有电路中使用的工作寄存器(F_R1)，新添加的三个寄存器分别称为汉明重量补偿寄存器(F_R1_HW)，汉明距离补偿寄存器(F_R1_HD)以及双补偿寄存器(F_R1_DC)。寄存器之间的连接方式如图 4 中代码所示，其中 F_R1_w 和 F_R1_wHW 分别表示 F_R1 和 F_R1_HW 寄存器的输入信号。通过这种连接方式，F_R1 和 F_R1_HW，F_R1_HD 和 F_R1_DC 寄存器组形成汉明重量互补寄存器对，F_R1 和 F_R1_HD，F_R1_HW 和 F_R1_DC 寄存器组形成汉明距离互补寄存器对，整个复合寄存器系统在任意时钟周期上的汉明重量能量消耗与汉明距离能量消耗均保持恒定，可有效隐藏实际敏感中间值产生的能量消耗。

```
begin
    F_R1 <= F_R1_w;
    F_R1_HW <= F_R1_wHW;
    F_R1_HD <= F_R1_w⊕F_R1⊕F_R1_DC;
    F_R1_DC <= F_R1_wHW⊕F_R1_HW⊕F_R1_HD;
end
```

图 4　复合寄存器系统代码

6.3.2 掩码/盲化技术

掩码缓解技术主要用在对称密码算法中，对密码算法计算过程中产生的所有中间值进行随机化处理，切断密码模块的能量消耗与可预测的敏感中间值之间的直接联系。掩码方案可按照掩码阶数划分。N 阶掩码方案指的是将运算过程中产生的所有中间值用随机数进行保护，并可表示为如下形式：M0＝X∘M1∘M2∘…∘Mn，其中 M0 称为掩码型中间值，X 表示敏感中间值（其中包含关键安全参数），Mi，i∈[1，n]表示随机产生的 n 个掩码随机数，“∘”表示一种运算操作，如异或操作。通常情况下，高阶掩码方案要比低阶掩码方案安全性更强，但会导致更多随机数生成开销、存储开销，以及在实际的运算过程中引入的计算开销。

盲化缓解技术主要用在非对称密码算法中，同 6.2.3 中介绍的一样，该技术通过随机化非对称密码算法计算中间值的方式来避免攻击者对中间值的有效预测，进而防范能量分析攻击。因此，盲化技术不仅能够有效抵抗计时分析攻击，对于能量分析攻击同样具有缓解效果。

6.3.3 其他缓解技术

为了在密码模块中部署更高安全性的缓解技术，同时兼顾密码模块的资源开销，宜使用混合防御缓解技术。

混合防御缓解技术采用低阶掩码方案加上指令乱序的混合缓解技术，可有效提高能量分析攻击的门槛，为密码模块提供高安全性保护。以一阶掩码为例，尽管一阶掩码方案可抵抗常见的统计分析技术，但容易遭受二阶攻击的威胁。例如，由于一阶掩码将敏感中间值划分为两个随机变量 M0＝X∘M1 和 M1，若攻击者可在能量迹中的特定时刻提取出与这两个随机变量相对应的能量消耗，则这两部分能量消耗的联合能量消耗将再次与敏感中间值 X 之间存在相关性。为避免此类能量分析攻击的威胁，可进一步采用指令乱序技术，将由敏感中间值划分出的两个随机变量的出现位置进行随机化处理。这种乱序处理使得攻击者不能轻易在能量曲线上定位出被划分中间值中各个子部分的计算位置，提高了将相关位置的能量消耗进行联合处理的难度，进而为密码模块提供更高安全性的保护。

6.4 电磁分析攻击缓解技术

6.4.1 低功耗技术

低功耗技术通过降低密码模块的能量消耗来抑制可利用的密码模块电磁辐射。

6.4.2 屏蔽套件技术

屏蔽套件技术通过在所有可能产生关键安全参数相关的电磁泄露的组件外部安装电磁屏蔽套件（如法拉第笼），抑制或者有效减少可利用的电磁辐射，从根源上消除电磁分析攻击，即消除密码模块在操作密码运算中间值时产生的电磁辐射。

6.4.3 扩展频谱时钟技术

扩展频谱时钟技术主要利用低频调制信号对周期性窄带时钟进行频率调制，将其扩展为宽带时钟信号。该方法可有效减小所有由该调制时钟驱动的数字信号的基频以及谐波的振幅，将信号的能量均匀的扩散在整个频带内，获得较大的电磁辐射衰减。这种采用扩展频谱时钟来降低峰值辐射能量的方法在电磁兼容领域较为常见。

6.4.4 交错的双轨逻辑技术

交错的双轨逻辑技术是双轨预充电逻辑技术(见 6.3.1)的一种改进的布局布线形式,即交错原始逻辑电路和补偿逻辑电路的一种布线实现方式。该缓解技术首先将包含关键安全参数运算的电路部分与无需保护的逻辑电路部分进行合理划分,同时在敏感电路上实现双轨预充电逻辑电路,并且在最大限度上将局部的真实电路和补偿电路布局在邻近的空间位置。该缓解可将双轨逻辑电路任意局部的电磁能量消耗保持恒定,有效隐藏电路实际运行中操作中间值时产生的能量消耗,抵抗后续采用统计分析方法进行密钥恢复的电磁分析攻击。

6.4.5 分布式电路架构技术

分布式电路架构技术通过将与关键安全参数计算相关的模块拆分成并行化的分布式计算子模块,使得针对单一探测位置的电磁分析攻击无法收集到完整的泄露信息,进而有效缓解依赖于电磁探头对目标计算模块准确定位的电磁分析攻击威胁。

7 非入侵式攻击测试方法

7.1 概述

本章针对第 5 章中指定的非入侵式攻击方法给出对应的测试方法。

7.2 测试策略

非入侵式攻击测试目标是评估使用了非入侵式攻击缓解技术的密码模块能否提供抵抗非入侵式攻击的能力。测试程序不能保证密码模块可完全抵抗攻击,但有效的测试可表明密码模块中充分考虑了非入侵式攻击缓解技术的设计和实现。

非入侵式攻击测试的基本原理是首先以非入侵的方法从密码模块中或密码模块周围提取物理量,随后利用隐藏在物理量中的有偏性展开攻击。这种有偏性来源于或者依赖于攻击者作为目标的秘密信息。在本文件中,这种依赖于秘密信息的有偏量被称为泄露。若实验结果表明泄露的信息超过了允许的泄露阈值,则认为密码模块不能通过非入侵式攻击测试。相反,若未观察到该泄露,攻击将会失效,则认为密码模块通过了非入侵式攻击测试。这种测试泄露存在与否的方法在本文件中被称为泄露分析。

非入侵式攻击测试流程是在一定的测试限制下,搜集和分析测量数据,并确定关键安全参数的信息泄露程度,而这些测试限制条件包括数据搜集的最大上限,使用的测试时间。

7.3 测试框架

测试人员应检查密码模块的安全性,包括抵抗计时分析攻击,简单能量/电磁分析攻击,差分能量/电磁分析攻击的能力,非入侵式攻击测试框架如图 5 所示。测试人员应遵循图 5 中的操作顺序。例如,通过计时分析攻击测试之后才需要进行简单能量/电磁分析测试。

本文件中非入侵式攻击测试方法不需要提取密码模块中的完整密钥。只要在测试过程中出现了明显的敏感信息泄露则认为密码模块没有通过测试。

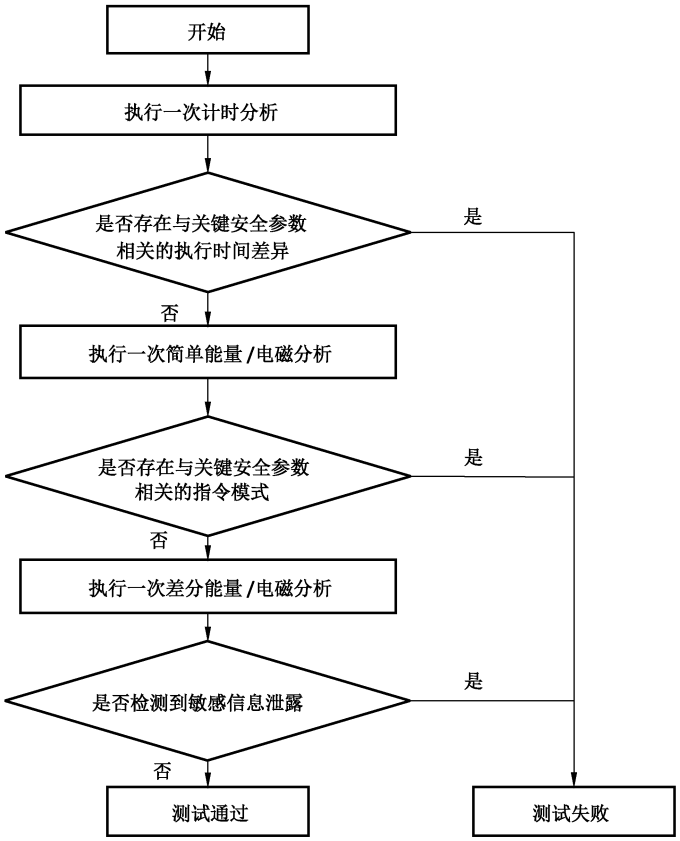

图 5　非入侵式攻击测试框架

7.4　测试流程

7.4.1　核心测试流程

针对具体的计时分析、能量泄露、电磁泄露测试，本文件给出了通用的核心测试流程。整个核心测试的流程如图 6 所示。针对计时分析攻击、简单能量/电磁分析、差分能量/电磁分析的泄露分析流程分别见图 7、图 8 以及图 9。

核心测试流程如图 6 所示：

a）　核对指定的关键安全参数的厂商文档；

b）　确定测量物理特征的可行性，若经过测试后未测到相关物理特征，则测试结果为通过；

c）　将测试实验室确定的一套关键安全参数配置到密码模块中；

d）　执行一次安全功能的泄露分析过程，并检查是否存在明显泄露，测试的结果分为观察到了明显泄露，或未观察到明显泄露。

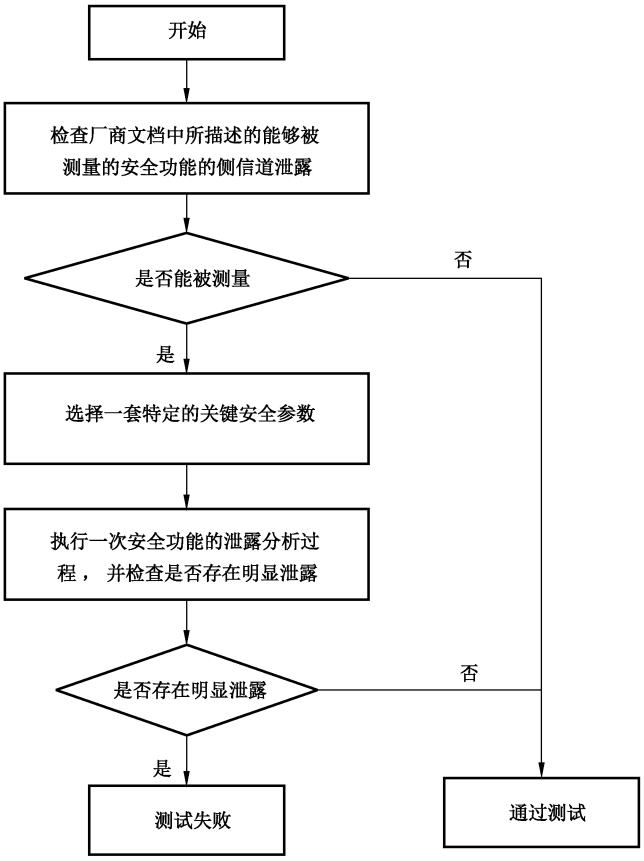

图 6　核心测试流程

测试流程步骤 c)中需要对厂商文档中指定类别的关键安全参数进行测试。关键安全参数类包括算法密钥,生物统计数据或 PIN 码。若一些安全功能涉及多个关键安全参数类,则所有关键安全参数类都需要进行泄露分析。测试时,应使用不同的关键安全参数类重复执行核心测试,直到第一次测试失败或所有的关键安全参数均通过了测试为止。若一个核心测试由于密码模块设定的重复操作次数上限而无法继续进行(如密码模块保护机制被触发,关键安全参数自动更新或者密码模块强制停止工作),则认为通过测试,且测试流程转向下一个关键安全参数类。

7.4.2　计时分析攻击泄露测试流程

图 7 展示了计时分析攻击的泄露分析流程。该流程被划分为两个阶段:

a)　在第一个阶段中,测量密码模块在固定的文本输入以及不同的关键安全参数下的执行时间。对应于固定关键安全参数以及固定文本的被测实现执行时间被多次测量。随后,测量到的时间的平均值和方差值被计算。此后同样的过程在其他的关键安全参数中被重复执行。若被测量的执行时间在统计分析中并不存在与关键安全参数的相关性,则测试进入第二阶段,否则测试失败。

b)　在第二阶段中,测量密码模块在不同的文本输入以及固定的关键安全参数下的执行时间。对应于固定关键安全参数以及固定文本的被测实现执行时间被多次测量。随后,测量到的时间的平均值和方差值被计算。此后同样的过程在其他的文本中被重复执行。若被测量的执行时

间在统计分析中并不存在与文本输入之间的相关性，则测试通过，否则测试失败。若被测密码模块的执行时间难以准确测量，则可使用目标密码模块的单个时钟周期值 ε 作为容错值。比较两个时间值(或者两个平均时间值)T1 和 T2，当|T1－T2|＜ε 时则测试通过，否则测试失败。

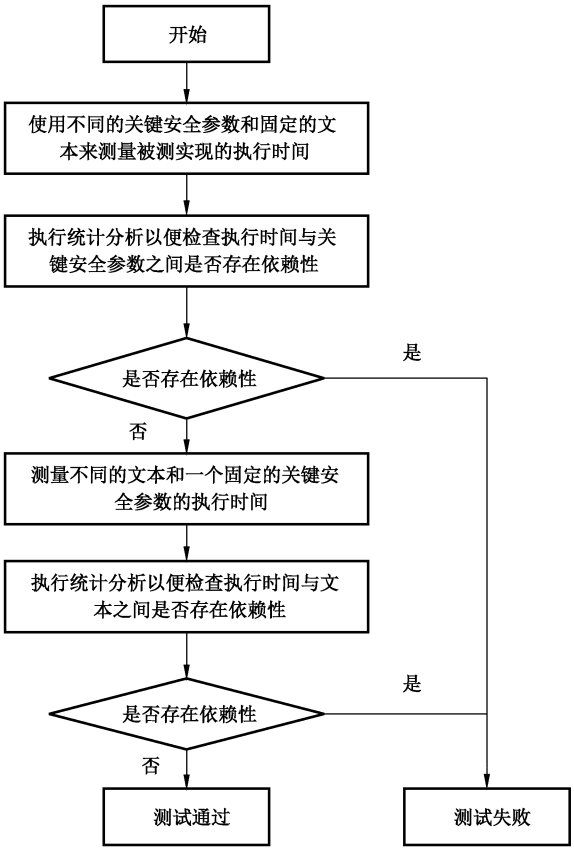

图 7　计时分析攻击泄露分析

7.4.3　简单能量/电磁泄露测试流程

图 8 展示了简单能量/简单电磁泄露分析的两阶段流程：

a)　测试实验室应根据期望达到的安全能力获取对应数量的侧信道测量信息；

b)　测试实验室进行密码算法指令序列识别分析。

步骤 b)中，对每个侧信道测量值，使用交叉关联的方法来检索指令序列。交叉关联方法是一种识别重复操作的有效方法。该方法有助于消除测试实验室的主观评估结果。当使用这种方法测量出的相关性过低以至于无法得出准确的结论时，测试实验室可使用聚类分析方法来协助评估。对于所有侧信道测量，若交叉关联方法识别出与关键安全参数相关的指令操作序列，则测试失败。

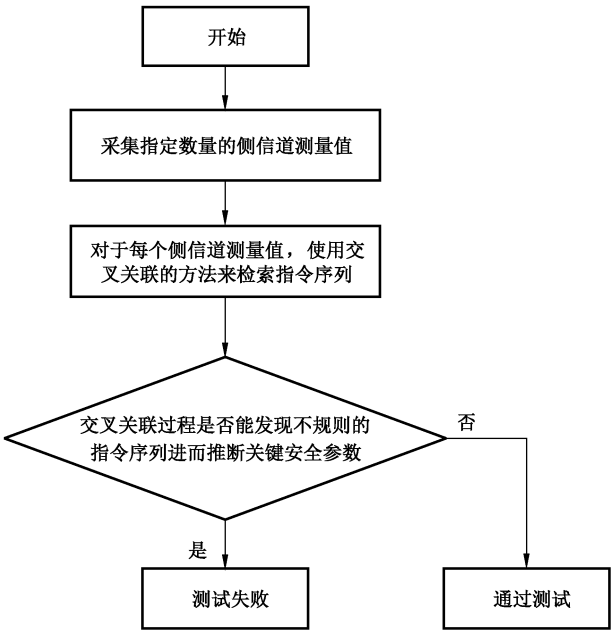

图 8　简单能量/电磁分析测试流程

7.4.4　差分能量/电磁泄露测试流程

图 9 给出了差分能量分析/差分电磁分析的泄露分析流程：

a）　测试实验室应根据期望达到的安全能力来获取对应数量的侧信道测量信息。

b）　使用校准函数进行静态或动态的曲线对齐操作，并计算信噪比 SNR。

c）　计算安全功能中的中间值。由于测试实验室使用了预先指定的测试向量集合来采集对应的侧信道测量值，因此计算安全功能中间值是可行的。测试实验室应精心选择测试向量以暴露和隔离潜在的泄露。

d）　对对齐的或者预处理的曲线进行统计测试。测试实验室应在多个预先指定的数据集上进行统计分析（即 Welch 测试），以此来检测侧信道中是否存在敏感信息泄露。

在无保护的密码实现中，测量信号的非对齐特性来源于能量消耗采集或者电磁消耗采集开始阶段的测量配置错误。若开始测量时的不确定性因素可被测量，则信号曲线就可被合适的对齐。这种对齐的方法称之为“静态对齐”。若存在或可提供一个指示操作开始的触发信号，则测量开始时的不确定性以及信号对齐的难度均将减少。当密码模块中主动引入了随机延时或者时钟频率变化时，静态对齐技术无法获得完全对齐的信号，则应使用“动态对齐”技术。该技术对曲线中的不同部分进行分段匹配，每段匹配时使用的偏移各不相同，并且对信号曲线进行非线性采样。通过这种处理，曲线中的不同部分就被对齐到相同的位置。

厂商应与测试实验室合作，以便协助测试实验室在密码模块中实现“校准函数”。该校准函数可同步信号波形（通过提供一个指示操作开始的触发信号）并且检测侧信道测量值的质量。此外，这种对齐校准函数也有助于检测外部噪声降噪方法的有效性（例如频域滤波或者均值去噪等）。上述校准函数可以针对公开（非敏感）变量（例如 RSA 中的公钥 e）的处理或者存储进行校准。若对应于该已知变量的侧信道测量值的信号噪声比足够高，则测试实验室执行后续的测试。反之，则测试实验室应在执行检测之前改进测量方法，提高测量质量。

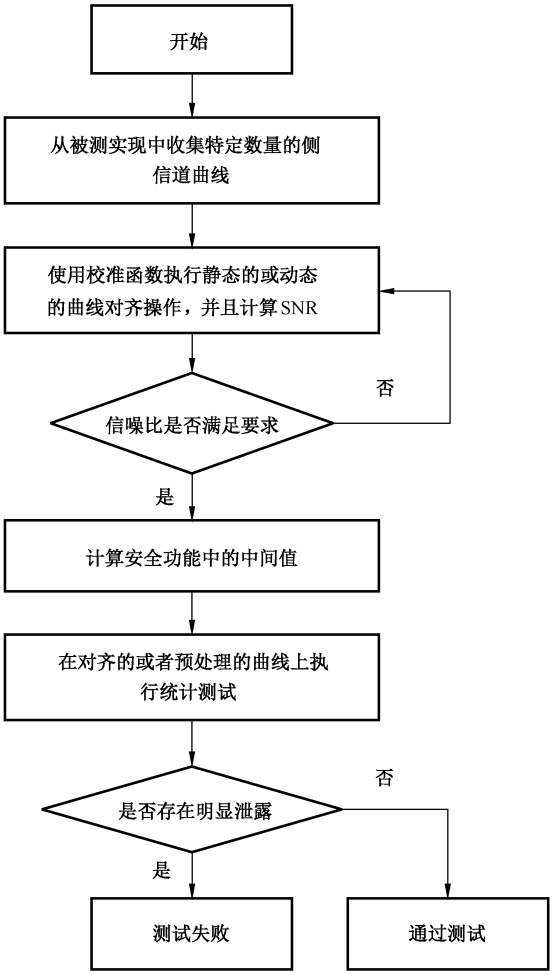

图 9　差分能量/电磁分析测试流程

7.5　测试所需厂商信息

厂商应提供如下信息：

——实现的密码算法；

——实现细节的设计方案；

——密码模块中使用的缓解技术；

——密码模块在使用时容易遭受侧信道攻击的条件或模式。

测试实验室应可在厂商提供的产品可选配置参数范围内，对关键安全参数以及密文信息进行选取配置，以便全面有效的反映测评结果。当通过测试后，最终产品的可选安全配置参数范围不可更改。

当执行测试流程时，一种常见的做法是先进行信号对齐操作，厂商需要与测试实验室进行合作以便为密码运算提供最好的同步起始信号。若起始和终止信息不可获得，测试实验室应采用标准的信号处理以及基于匹配的技术来完成信号对齐过程。若密码运算开始处信号被很好的对齐，测试实验室可要求厂商采用标准的，基于最小二乘拟合的信号匹配方法对特定的算法内部位置采取更精细的对齐。这些需要进一步对齐的内部位置以及位置的数量由测试实验室指定。随后，测试实验室应实现“校准函数”以便：

——同步测量到的物理量；

——检查测量物理量的质量。

附 录 A
（资料性）
SM2/SM9 和 SM4 的非入侵式攻击缓解技术介绍

A.1 SM2/SM9 缓解技术

SM2 和 SM9 算法是基于椭圆曲线算法设计的，针对他们的常见攻击主要针对椭圆曲线中的标量乘法展开。常用的标量乘法使用密钥的二进制展开形式来逐比特完成椭圆曲线上输入点到输出点之间的转换，主要操作即点加和倍点两种操作。由密钥各比特位不同导致的点加倍点序列的差异，该实现方案很容易受到计时分析攻击或者简单能量分析的威胁。

一种简单可行的缓解技术是通过引入“虚”点来平衡可能由私钥比特位引起的指令分支差异。这种方案可通过图 A.1 中的伪代码来简单描述。其中 Q_1 即为为了缓解技术的需要所引入的虚点变量。在这种保护方案中，不论计算过程中私钥 K 的当前比特位是 0 或者是 1，倍点与点加操作总是按顺序完成。两种操作的计算结果被分别存放在不同的变量 Q_0 与 Q_1 中。当私钥的当前计算比特为 1 时，表示真实的计算中间值应同时包括倍点与点加操作，此时 Q_1 的计算结果被赋值给了 Q_0，开始下一轮的计算流程。相反若私钥的当前计算比特为 0 时，真实的计算中间值应只包括一次倍点运算的结果，此时 Q_0 完成一次自身的赋值运算后结束本次循环流程。整个计算流程中的点加、倍点、赋值操作序列不因私钥的变化而产生任何的改变，可抵抗利用指令分支不平衡所导致的简单能量分析，同时也可有效抵抗计时分析攻击。

输入：P，$k=(k_{l-1},k_{l-2},\cdots,k_0)_2$
输出：$Q=kP$
$Q_0 \leftarrow O$
For $i=l-1$ downto 0 do
$Q_0 \leftarrow 2Q_0$
$Q_1 \leftarrow Q_0+P$
$Q_0 \leftarrow Q_{k_i}$
Return Q_0

图 A.1 平衡指令分支缓解技术

为抵抗通过逐比特私钥猜测的方式进行的差分能量分析或者差分电磁分析，本文件推荐采用盲化基点或者盲化私钥的方法来随机化每次标量乘过程中出现的计算中间值。

盲化私钥的方式如下所述，假设 n 是椭圆曲线中基点 P 的阶，则 $Q=kP$ 的计算过程可通过下面的计算过程进行转换：

a） 选择一个 n 比特的随机数 m。

b） 计算新的私钥值 $k'=k+n*m$。

c） 计算 $Q=k'P$，nP 为椭圆曲线中的无穷远点，则 $Q=k'P=(kP+m*nP)=kP$。

这种缓解技术通过在每次的算法执行过程中引入随机改变的掩码值 m 的方式隐藏了敏感私钥信息 k。攻击者无法在已知基点 P 的情况下通过猜测固定比特位的私钥信息来推测计算过程中产生的算法中间值，切断了敏感中间值与实际能量消耗之间的特定依赖关系，确保其对 DPA 或 DEMA 的抵抗力。

盲化基点方式指的是通过在每次计算过程中引入一个新的秘密随机点 R 的方式对计算中间值进行盲化操作。原有标量乘算法被分解为两部分，即 $k*(P+R)$ 以及 kR 且 $Q=k*(P+R)-kR$。因 R 是一个秘密的随机点，$(P+R)$ 也是一个随机点，在生成最终结果 Q 的两个计算子过程中的所有中间值均是不可预测的，确保了整个缓解技术具备 DPA 与 DEMA 攻击的抵抗力。

A.2 SM4 缓解技术

针对 SM4 密码算法的常见侧信道攻击主要使用统计分析方法（如差分能量分析或差分电磁分析）对算法计算过程中的敏感中间值变量进行攻击。针对这一主要的非入侵式攻击威胁，可通过引入掩码随机数的方式对 SM4 计算过程中的所有敏感中间值变量进行随机化处理，切断密码模块的能量消耗与可预测的敏感中间值之间的联系。掩码保护方案的核心问题是追踪和记录掩码在算法计算流程中的变化，在输出真实的密文之前消除当前的保护掩码值。对于 SM4 中的线性变换部分，变换函数自身具有的线性性质，即 $f(x*m)=f(x)*f(m)$，掩码的追踪计算可通过将掩码值经过相同的线性变化得到。因此不同掩码防御方案的差异主要体现在掩码经过非线性变换层 S 的追踪过程上。

本文件主要介绍两种简单的非线性层的掩码追踪方式供密码算法实现人员参考，他们根据是否需要重构非线性变换层被分为动态掩码修正实现和静态掩码修正实现两种。

在动态掩码实现中，非线性层 S 盒在每次使用之前根据输入掩码与输出掩码值进行重构，使得新生成的 S'满足如下的关系：$S'(x)=S(x\oplus r_{in})\oplus r_{out}$。其中 r_{in} 和 r_{out} 掩码值在每次加密过程中均随机产生。通过这种动态重构 S 盒的方式，由输入掩码保护的计算中间值 $(x\oplus r_{in})$ 在经过新构造的非线性层 S'得到的输出掩码值为正确输出值 $S(x)$ 与输出掩码 r_{out} 的异或结果，可实现非线性层变换中掩码可追踪的特性。

在静态掩码实现中，非线性层 S 盒并不进行重构而是通过查表的方式来直接获取非线性层输出值的掩码。实现过程中，密码模块需要预计算一张 256 * 256 的查找表，其中查找表的行索引为 r_{in}，列索引为 $(r_{in}\oplus x)$。而每一个行列索引所选中的具体掩码值由 $r_{out}=S(r_{in}\oplus x)\oplus S(x)$ 所决定，即为未经变换的非线性 S 盒在输入值为 $(x\oplus r_{in})$ 时产生的输出掩码。该方法也可追踪实际的输入掩码在经过非线性变换层之后生成的输出掩码值，以保证掩码在 SM4 的整个计算流程中均是可追踪的，确保 SM4 算法在掩码保护方案下得到正确的输出结果。

参 考 文 献

[1] ISO/IEC 17825:2016 信息技术 安全技术 密码模块非入侵式攻击缓解技术测试方法(Information technology—Security techniques—Testing methods for the mitigation of non-invasive attack classes against cryptographic modules)

中华人民共和国密码
行业标准
密码模块非入侵式攻击缓解技术指南
GM/T 0083—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 1.5 字数 44 千字
2021年5月第一版 2021年5月第一次印刷
*
书号:155066·2-35898 定价 27.00 元

GM/T 0083-2020

码上扫一扫 正版服务到