ISO/IEC 17825–2016《密码模块的非入侵式攻击缓解技术的测试方法》标准解读

鹿福祥　陈传禄　胡进伟　陈 鹏　张 登

（中国质量认证中心华南实验室）

摘　要：从密码模块上保障数据隐私和安全是一种行之有效的手段，因此近年来对密码模块的安全性评估倍受关注。非入侵式攻击缓解技术是密码模块安全指标之一，本文结合GM/T 0083–2020国密标准对IEC 17825–2016进行了学习与解读。主要针对非入侵式攻击方法与安全功能的关联性、基本测试项目和流程、通过/失败测试指标、缓解技术等方面进行了解读。希望能为相关人员对标准及测试方法的理解和密码模块安全设计、应用、评估提供些许参考。

关键词：非入侵式攻击，缓解技术，侧信道攻击，密码模块

DOI编码：10.3969/j.issn.1674–5698.2023.07.015

Interpretation of ISO/IEC 17825-2016 on Testing Methods for the Mitigation of Non-Invasive Attack Classes against Cryptographic Modules

LU Fu-xiang　CHEN Chuan-lu　HU Jin-wei　CHEN Peng　ZHANG Deng

（China Quality Certification Center South China Laboratory）

Abstract: It is an effective means to protect data privacy and security from cryptographic modules, so the security evaluation of cryptographic modules has attracted much attention in recent years. Non-invasive attack mitigation technology is one of the security indicators of cryptographic modules. This paper studies and interprets ISO/IEC 17825-2016 based on GM/T 0083-2020, and mainly explores the correlation between non-invasive attack methods and security functions, basic test items and processes, pass/fail test indicators, mitigation techniques, etc. It is expected to provide some reference for relevant personnel to understand the standard and its test methods, as well as the security design, application and evaluation of the cryptographic module.

Keywords: non-invasive attack, mitigation techniques, side channel attack, cryptographic module

0 引言

为贯彻落实《密码法》合理使用密码技术保护关键信息基础设施，2022年11月7日，发布了GB/T 39204–2022《信息安全技术 关键信息基础设施安全保护要求》[1]。在密码行业委员会、高校学者、企业专家等相关方的共同推进下，我国已发布商用密码相关国家标准31项、行业标准116项、ISO/IEC标准7项[2]。

基金项目：本文受中国质量认证中心科技课题“商用密码产品安全测评关键技术研究”（课题编号：2022CQC18-GZ）资助。

作者简介：鹿福祥，工程师，硕士学位，研究方向为密码芯片的侧信道泄露评估与防护、数据中心检测和认证。

陈传禄，高级工程师。

胡进伟，高级工程师。

陈鹏，工程师。

我国正在建立结构合理、配套协调的密码标准体系，为迎接信息网络安全“密码+”新时代铺垫基石。

密码算法的实现需要一个载体，往往应用过程中需要将密码算法嵌入到物理设备。如：现在常见的智能门锁、共享单车、移动支付等设备都采用了不同的密码技术，设备中都包含了相应的密码模块。ISO/IEC 19790:2012和GB/T 37092–2018中都定义密码模块应该包含硬件、软件、固件或者其中组合的集合，集合至少一个核准的密码算法、功能或过程实现的一项密码服务。密码模块是实现密码算法、密钥管理等功能的硬件、软件等一体的组件，根据不同程度的安全要求将其划分成4个不同安全等级（或者5个等级），从1至4级安全要求不断提高[3]。常见的密码模块安全要求相关标准如：ISO/IEC 19790:2012、GM/T 0028–2014、GM/T 0039–2015、ISO/IEC 24759–2017、GB/T 37092–2018等，这些标准中都包含了非入侵式攻击、缓解非入侵式攻击的检测方法或相关要求。这些标准为密码模块的设计、研发、生产、集成建设、运维、应用安全测评等活动提供依据。密码模块安全标准对安全等级1级、2级的要求仅需要通过文件声明密码模块是如何缓解非入侵式技术攻击的措施。对安全等级3级、4级的要求，需要实验室对密码模块抵抗非入侵式攻击的能力进行测试，来证明密码模块具有标准中列出的非入侵式攻击缓解技术[4]。

1　标准解读

为了确定密码模块是否符合ISO/IEC 19790:2012中的安全等级3级、4级的要求。ISO/IEC 17825:2016标准中规定了非侵入性攻击缓解测试指标与ISO/IEC 19790中规定的安全功能相关性[5]。ISO/IEC 17825采用的测试方法具有可靠性、有效性、可重复性、成本适中、易实现等优点。

ISO/IEC 17825:2016包含了分组密码算法和公钥密码算法非侵入性攻击缓解测试方法，和判定通过/失败的指标。结合我国商用密码算法的独特性和创新性，2020年12月28日国家密码管理局发布了GM/T 0083–2020，该标准规定了应用国产商用算法的密码模块非入侵式攻击测试方法及其判定指标[2]。

1.1　非入侵式攻击方法与安全功能的关联性

密码模块安全性评估应当根据其安全功能特点、模块特性、应用场景，来选择相应的非入侵式攻击缓解技术。其中，计时分析攻击（TA）、简单能量分析攻击（SPA）、简单电磁分析攻击（SEMA）、差分能量分析攻击（DPA）、电磁分析攻击（EMA）等攻击技术成熟容易实现，对密码模块的威胁最大，受到学术界和测评界广泛关注[4]。ISO/IEC 17825:2016中也针对这几种非入侵式攻击缓解情况规定了测试方法和要求。

表1　非侵入性攻击方法与安全功能的关联表

GM/T 0083中涉及的核准的安全功能与非侵入式攻击方法				
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	SM4	适用	适用	适用
流密码	GM/T 0001	适用	适用	适用
非对称面算法	SM2	适用	适用	适用
	SM9	适用	适用	适用
杂凑函数	SM3	适用	适用	适用
ISO/IEC 17825中涉及的核准的安全功能与非侵入式攻击方法				
核准的安全功能		非入侵式攻击方法		
		SPA/SEMA	DPA/DEMA	TA
对称密钥	AES	适用	适用	适用
	3DES	适用	适用	适用
	Stream Ciphers	适用	适用	适用
非对称密钥	Plain RAS（key Wrapping）	适用	适用	适用
	RAS KPCS #1 V1.5	适用	适用	适用
	RAS KPCS #1 V2.1	不适用	不适用	适用
	DSA	适用	适用	适用
	ECDSA	适用	适用	适用
散列机制	SHA	不适用	适用	适用
RNG和RNG	Deterministic	不适用	适用	适用
	Non–deterministic	不适用	适用	适用
数据认证机制	HMAC	适用	适用	不适用
秘钥生成		适用	不适用	不适用
从其他密钥派生密钥		适用	适用	不适用
从密码派生秘钥		适用	不适用	不适用
密钥建立	DLC	适用	不适用	不适用
	IFC	适用	不适用	不适用
秘钥登录与输出		不适用	不适用	不适用
操作员身份验证机制	PIN/Password	适用	适用	适用
	Key	不适用	不适用	适用
	生物统计学	适用	不适用	适用

表1中的“适用”意味着安全功能容易受到这些类型的攻击，“不适用”意味着安全功能不容易受到这些类型的攻击[5]。

1.2 非侵入性攻击和缓解技术

没有任何标准和检测技术能够完全保证密码设备可免受非入侵式攻击的侵扰。ISO/IEC 17825和GM/T 0083的测试目的是评估已使用非侵入性攻击缓解技术的密码模块，能否在期望的安全级别上提供抵抗非入侵式攻击的能力，验证在设计和实施阶段采取了足够的注意来缓解非侵入性攻击。测试的基本原理是以非入侵的方法从密码模块周围提取物理信息，检测这个物理信息与密码模块的CSP（关键秘密参数）是否有依赖关系。如果通过这种依赖关系足够开展非入侵式攻击，则认为密码模块存在泄露，不能通过非入侵式攻击测试。如果收集到的物理信息与CSP不存在依赖关系或者现有技术条件检测不到，则认为不存在泄露通过测试。

在密码模块安全性测试中，应依次进行TA、SPA/SEMA、DPA/DEMA分析攻击的抵抗能力测试。图1给出了非入侵式攻击的测试框架，测试人员应当按照图中顺序进行测试。必要时进行高级的测试如：Mico-architectural TA、Markov SPA、Adress-bit DPA、高阶DPA攻击等[5]。下文分别介绍了TA、SPA/SEMA、DPA/DEMA[6]缓解技术的测试流程如图2~4所示。

1.3 计时攻击的泄露测试

图2计时攻击的泄漏分析流程可分为两个阶段。第一阶段，测量几个不同CSP和固定文本的执行时间。如果测量的加/解密执行时间与不同CSP没有明显的统计学相关性，那么测试继续到第二阶段；否则，测试失败。第二阶段，使用不同的明文和固定的CSP进行加/解密操作。如果加/解密操作的

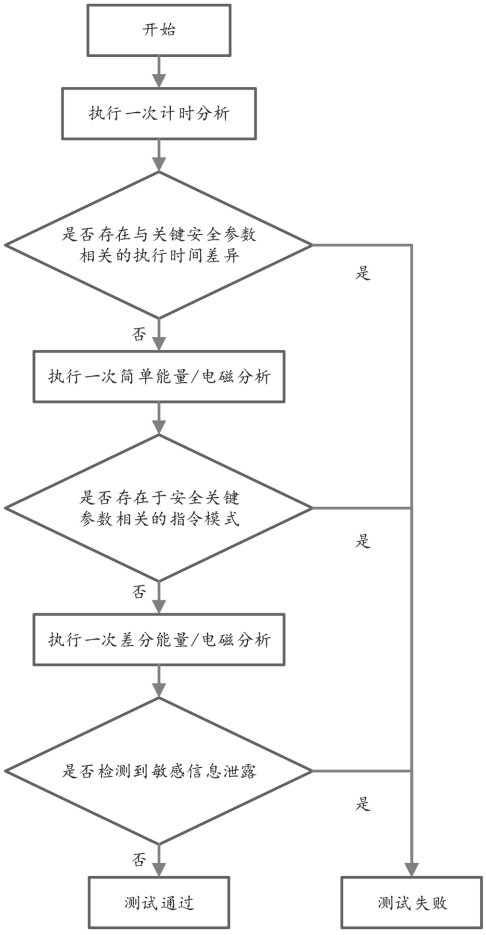

图1 非入侵式攻击测试框架图

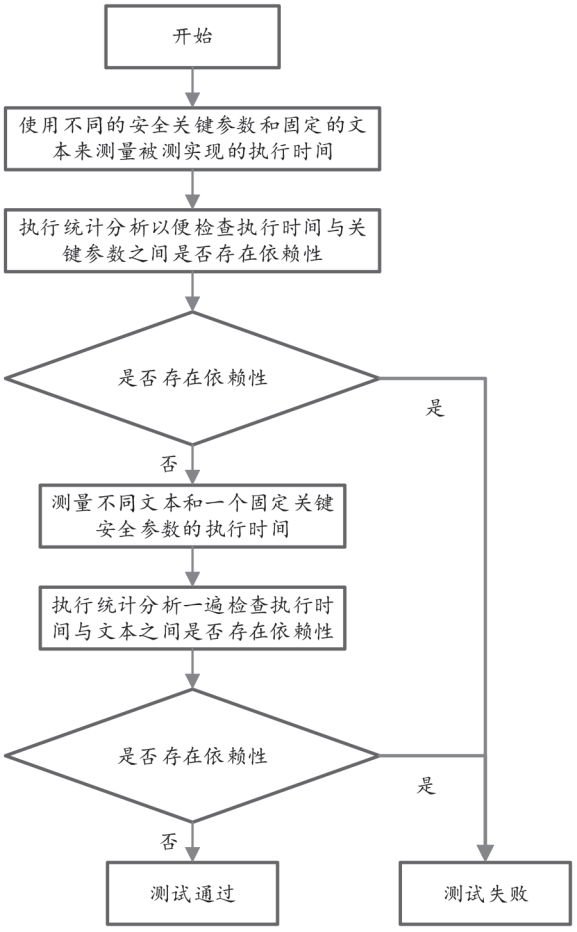

图2 计时分析攻击泄露分析流程图

执行时间与不同明文之间无明显的统计学相关性，测试通过。否则，测试失败。当密码模块的执行时间难以准确测量，应使用被测密码模块芯片的时钟周期ε作为容错值。比较时间值（或两个平均时间值）T_1和T_2，如果$|T_1-T_2|<\varepsilon$不成立，则测试不通过[5]。

因为高级时间分析攻击存在一定的威胁，所以泄露测试不仅应计算均值差，还应计算方差或者其他统计学特征，以便检测是否存在二阶或高级计时泄漏。

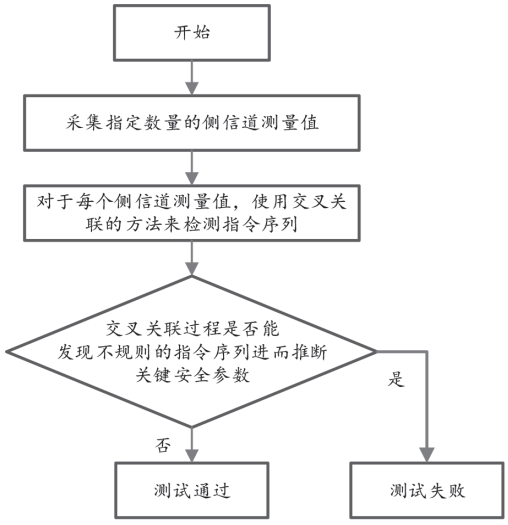

图3 简单能量/电磁分析攻击测试流程图

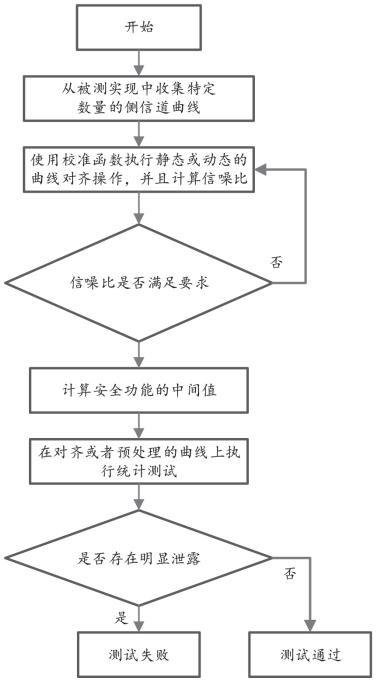

图4 差分能量/电磁分析攻击测试流程图

1.4 简单能量/电磁分析泄露测试

简单能量/电磁分析攻击测试流程图如图3所示。首先，测试实验室应获取与所需安全等级相关的物理测量值，在非侵入性攻击缓解通过/失败测试指标中，对不同安全等级的密码模块测试，采集信息的时间和数据量有不同要求。其次，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，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[7]，则密码模块测试失败。

1.5 差分能量/电磁分析泄露测试

差分能量/电磁分析泄露测试流程如图4。首先，从待测设备上收集对应测试安全等级所需物理测量值，通过滤波、动态对齐、静态对齐技术对测量值曲线进行预处理。然后计算SNR（信噪比），若SNR足够进行密码算法的中间值分析，则计算出对应的中间值，再对预处理的测量值曲线进行统计学假设检验。通常进行Welch t检验，如果同一时间点测量值的T表明显著性不同，则认为存在泄露。如果发现所有的点都存在显著性不同，需要重新分析测量值曲线对齐和SNR的计算是否正确。

统计检验按以下方法进行。侧信道轨迹将被分为两个子集，并使两个子集之间正在处理的敏感信息具有显著性不同。这两个子集的设计要求根据待测设备、中间值、密码算法特性等影响因素不同进行单独设计。在ISO/IEC 17825中有给出RSA、AES通过调整明文、密文、中间值等CSP设计不同的子集。对于每种算法，都要进行多次Welch t检验，每次都针对不同类型的泄漏；每个测试应重复两次，使用两个不同的数据集；减少假阳性的出现[1]。

图5假设检验测试流程图中，设计两个不同CSP收集对应的物理测量值分别进行T检验，观察$|T_1|$和$|T_2|$，若均超过了C值则认为该位置存在泄露，否者认为该点通过测试；收集到的物理测量值涉及很多个点，逐个进行假设检验测试，得出最后测试结果。置信度99.999%对应于C=4.5，也可以进行调整[8]。由于一次实验中可能会出现一些假阳性，所以需要重复Welch t检验；多次测试失败才可以拒绝一台设备。对于每种密码算法，都要进行多次t检验，每

次都针对不同类型的泄漏。每次测试应重复两次，使用两个不同的数据集。在进行统计试验前，检测实验室应明确使用那一组物理测试值曲线进行试验。将物理测试值曲线分为两组，组1和组2。组1和组2为两个不相交的数据集，用于执行两个独立的Welch t检验。其中A_1和B_1代表不同的子集，μ_{A1}、μ_{B1}和σ_{A1}、σ_{B1}代表各自的均值和标准差，N_{A1}、N_{B1}代表子集A和B的大小，通过如下公式计算$|T_1|$：

$$T_1 = \frac{\left(\mu_{A_1} - \mu_{B_1}\right)}{\sqrt{\frac{\sigma_{A_1}^2}{N_{A_1}} + \frac{\sigma_{B_1}^2}{N_{B_1}}}}$$

然后通过相同的方法计算$|T_2|$，最后与C进行比较，判断是否存在显著性不同。除了t检验，还可以采用NICV（归一化类间方差）进行多位或高阶的泄露检测[9]。

2 非侵入性攻击缓解通过/失败测试指标

对于安全等级3级和4级需要通过ISO/IEC 17825标准规定测试项目，不同等级对应测试通过/失败指标不同，主要体现在物理测量值收集时间、物理测量值曲线数量、数据的预处理（数据对齐、滤波等）、测试仪器设备等要求不同[10]。

目前主要的非入侵式攻击缓解技术，如：采用平衡指令分支技术、随机延时插入技术、盲化操作技术、隐藏技术、掩码技术等来减少操作依赖性或数据依赖性，在GM/T 0083–2020第6章节有非入侵式攻击缓解方法的介绍[4]。

3 结 语

非入侵式攻击缓解技术测试是密码模块安全性测试重要的一部分，特别是安全等级3级和4

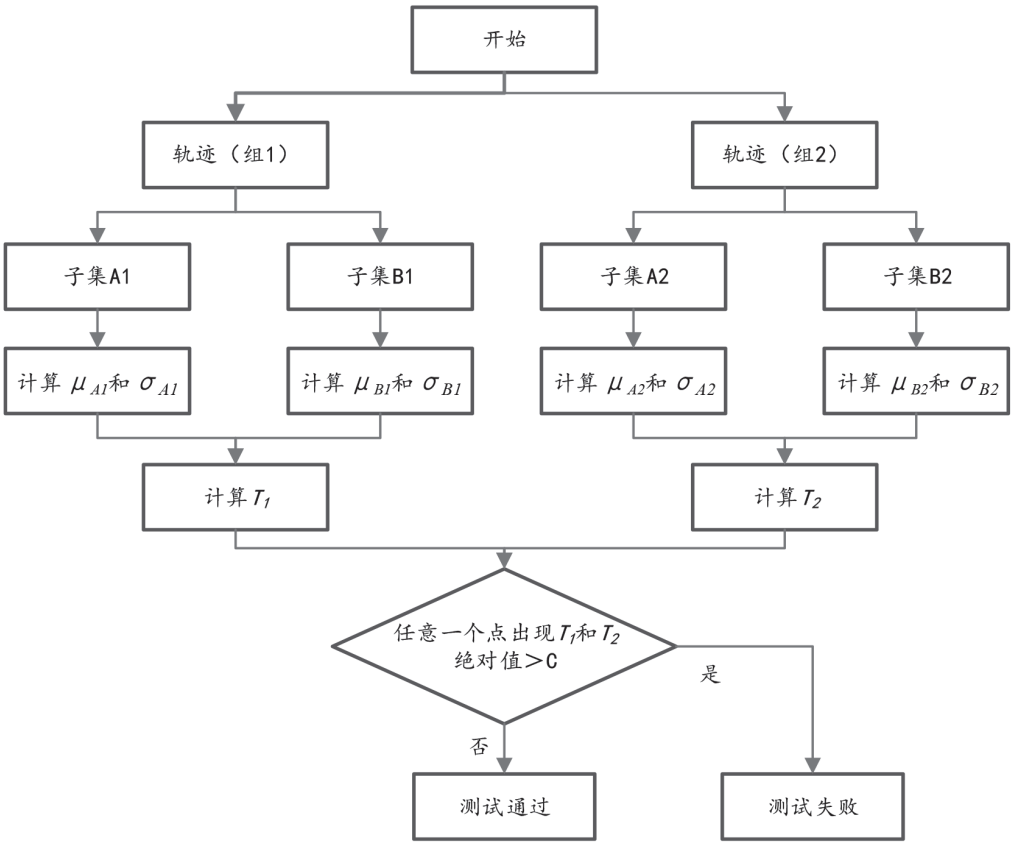

图5 统计学假设检验流程图

级必须具有非入侵式攻击缓解技术并通过测试。为了避免测试消耗过多的财力和精力，并由于测评技术的发展一般滞后于技术等原因，ISO/IEC 17825标准中的测试方法不能完全保证密码模块能够避免非入侵式攻击。但是通过测试可验证密码模块设计和实践中充分考虑了非入侵式攻击缓解技术，能够有效缓解现存的非入侵式攻击。ISO/IEC 17825–2016和GM/T 0083–2020标准的实施有助于高安全性密码模块设 计、生产和应用。

参考文献

[1] 国家市场监督管理总局，国家标准化管理委员会. GB/T 39204–2022,信息安全技术 关键信息基础设施安全保护要求[S].

[2] 田敏求,夏鲁宁,张众,等. 我国密码行业标准综述(下) [J]. 信息技术与标准化, 2019(04):52–55.

[3] Kusumah R M I T, Andriawan Y. Implementation of cryptography module security certification based on SNI ISO/IEC 19790: 2012–security requirements for cryptography module[C]//2019 international seminar on intelligent technology and its applications (isitia). IEEE, 2019: 216–221.

[4] 中华人民共和国国家密码管理局.GM/T 0083–2020，密码模块非入侵式攻击缓解技术指南[S]. 北京: 中国标准出版社,2020.

[5] Information technology – Security techniques – Testing methods for the mitigation of non–invasive attack classes against cryptographic modules：ISO/IEC 17825–2016.

[6] 陈华,习伟,范丽敏,等. 密码产品的侧信道分析与评估[J]. 电子与信息学报, 2020,42(08):1836–1845.

[7] Ding A A, Chen C, Eisenbarth T. Simpler, faster, and more robust t–test based leakage detection[C]// International workshop on constructive side–channel analysis and secure design, 2016: 163–183.

[8] Becker G, Cooper J, Demulder E, et al. Test vector leakage assessment (TVLA) methodology in practice[C]// International Cryptographic Module Conference, 2013: 1001–1013.

[9] Bhasin S, Danger J–L, Guilley S, et al. NICV: normalized inter–class variance for detection of side–channel leakage[C]// 2014 International Symposium on Electromagnetic Compatibility, Tokyo, 2014: 310–313.

[10] 冯登国, 周永彬, 刘继业. 能量分析攻击[M]. 北京: 科学出版社, 2010.