软件学报 ISSN 1000-9825, CODEN RUXUEW
2026,37(2):894−914 [doi: 10.13328/j.cnki.jos.007455] [CSTR: 32375.14.jos.007455]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

私有算法密码芯片非入侵式攻击检测框架*

魏淙洺[1,3], 王 菁[2], 王 安[1], 丁瑶玲[1], 孙绍飞[1], 祝烈煌[1]

[1](北京理工大学 网络空间安全学院, 北京 100081)

[2](北京理工大学 计算机学院, 北京 100081)

[3](先进密码技术与系统安全四川省重点实验室 (成都信息工程大学), 四川 成都 610054)

通信作者: 王安, E-mail: wanganl@bit.edu.cn

摘 要: 近年来, 密码芯片迅速发展, 与此同时也面临着非入侵式攻击的严重威胁. 目前已有国内外标准给出了非入侵式攻击检测流程与方法, 但这些标准均针对公开算法制定, 对于私有算法并不适用, 私有算法密码芯片存在着很大的安全隐患. 针对这一问题, 提出面向私有算法密码芯片的非入侵式攻击检测框架, 该框架包含计时分析测试、简单能量/电磁分析测试、差分能量/电磁分析测试 3 大部分. 对于计时分析测试, 采用基于平均去噪的计时分析方法, 提高所采集时间的可用性. 针对简单能量/电磁分析, 提出面向私有密码算法的视觉观察法和交叉关联分析方法. 针对差分能量/电磁分析, 通过 TVLA-1 和 TVLA-2 双重检测方法有效检测私有算法密码芯片不同来源的泄露, 评估私有算法密码芯片的抗差分能量/电磁攻击能力. 该框架是对传统非入侵式攻击检测的有效补充, 极大提高了非入侵式攻击检测的检测范围. 为了验证该框架的有效性, 在多款密码芯片上开展黑盒实验, 实验结果表明该框架能够有效检测私有算法密码芯片的抗非入侵式攻击安全性.

关键词: 非入侵式攻击; 私有算法; 密码芯片; 计时分析; 能量分析

中图法分类号: TP309

中文引用格式: 魏淙洺, 王菁, 王安, 丁瑶玲, 孙绍飞, 祝烈煌. 私有算法密码芯片非入侵式攻击检测框架. 软件学报, 2026, 37(2): 894–914. http://www.jos.org.cn/1000-9825/7455.htm

英文引用格式: Wei CM, Wang J, Wang A, Ding YL, Sun SF, Zhu LH. Detection Framework of Non-invasive Attack Against Private-algorithm Cryptographic Chips. Ruan Jian Xue Bao/Journal of Software, 2026, 37(2): 894–914 (in Chinese). http://www.jos.org.cn/1000-9825/7455.htm

Detection Framework of Non-invasive Attack Against Private-algorithm Cryptographic Chips

WEI Cong-Ming[1,3], WANG Jing[2], WANG An[1], DING Yao-Ling[1], SUN Shao-Fei[1], ZHU Lie-Huang[1]

[1](School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100081, China)

[2](School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China)

[3](Advanced Cryptography and System Security Key Laboratory of Sichuan Province (Chengdu University of Information Technology), Chengdu 610054, China)

Abstract: In recent years, cryptographic chips have developed rapidly. However, they are also facing a significant threat from non-invasive attacks. Although both international and domestic standards provide testing methods for non-invasive attacks, these standards are formulated for public algorithms and are not applicable to private algorithms, which still present considerable security risks. This study proposes a detection framework for private-algorithm cryptographic chips, which includes three components: timing analysis tests, simple power/electromagnetic analysis tests, and differential power/electromagnetic analysis tests. For the timing analysis test, a method based on average denoising is adopted, which significantly improves the accuracy of execution time measurements. Methods based on visual

* 基金项目: 国家重点研发计划 (2022YFB3103800); 国家自然科学基金 (62272047, 62302036, 62402039); 北京市自然科学基金 (L244044, QY24173)
收稿时间: 2024-04-16; 修改时间: 2025-01-15; 采用时间: 2025-04-29; jos 在线出版时间: 2025-09-10
CNKI 网络首发时间: 2025-09-11

observation and cross-correlation analysis are presented for simple power/electromagnetic analysis tests. Finally, for differential power analysis, TVLA-1 and TVLA-2 are employed to detect leakages from various sources and evaluate the vulnerabilities of private-algorithm cryptographic chips to differential power attacks. The proposed framework serves as an effective supplement to traditional non-invasive attack detection, significantly expanding its application range. To verify the effectiveness of the framework, black-box experiments are conducted on several cryptographic chips. The results demonstrate that the framework can effectively assess the resilience of private-algorithm cryptographic chips against non-invasive attacks.

Key words: non-invasive attack; private algorithm; cryptographic chip; timing analysis; power analysis

传统密码分析技术通过分析密码算法执行的明密文来恢复密钥, 关注的是算法本身的安全性, 然而, 随着算法设计能力的大幅提升, 传统密码分析手段很难实现实际的密钥恢复攻击. 1996 年, 美国密码学家 Kocher[1]提出侧信道攻击方法. 侧信道攻击是极具实用性和破坏性的非入侵式攻击方法, 通过获取密码设备在执行加密等运算过程中意外泄露的侧信息来恢复密钥等关键安全参数. 计时攻击[1]、能量攻击[2]、电磁攻击[3]、缓存攻击[4]、声音攻击等都属于非入侵式攻击, 该技术的有效性远高于密码分析数学方法, 以简单、直观、成本低等特点, 迅速受到广泛关注, 现已成为密码设备安全性的重要威胁之一[5].

非入侵式攻击技术的发展, 对密码设备物理安全性提出了更高的要求, 目前国内外主流芯片测评机构均把抗非入侵式攻击能力作为衡量芯片安全性的主要指标, 与密码安全相关的国内、国际标准也都对非入侵式安全提出了具体要求. 密码芯片需要具备缓解非入侵式攻击的能力, 从而能够抵御非入侵式攻击, 保障关键信息基础设施的安全.

目前, 侧信道分析领域大多针对公开的密码算法展开研究, 在密码安全相关的标准中, 关于非入侵式攻击的检测方法也是针对已有公开算法进行规定说明的. 然而, 为了提高安全性, 军事等关键领域的密码设备可能使用私有算法, 私有算法包括未公开的密码算法, 如我国的国密算法 SM1 和 SM7, 或者基于公开算法进行修改后的算法, 如使用未知 S 盒的 AES 算法. 在未知算法细节的情况下, 对于私有算法密码芯片的安全性检测尤为重要, 但目前关于这一问题的研究甚少, 缺少明确针对私有算法密码芯片的非入侵式攻击检测技术.

本文研究黑盒条件下私有算法密码芯片非入侵式攻击检测方法, 提出了私有算法密码芯片的非入侵式攻击检测框架, 主要贡献如下.

(1) 该框架针对黑盒条件下私有算法密码芯片开展非入侵式攻击检测研究, 大大扩展了密码芯片非入侵式安全的检测范围. 整个框架包含私有密码算法的计时分析检测、简单能量/电磁分析检测、差分能量/电磁分析检测这 3 部分, 并在各部分中对面向公钥密码、分组密码两大类密码算法的适用性展开讨论, 以期提高非入侵式攻击检测的准确性.

(2) 该框架重点研究面向私有密码算法的能量/电磁分析. 对于简单能量/电磁分析检测, 该框架使用视觉观察和交叉关联方法检测不规则操作序列, 进而判断波形与密钥之间的关系, 能够在黑盒条件下检测私有算法密码芯片的抗简单能量攻击能力. 对于差分能量/电磁分析检测, 该框架提出基于 TVLA-1 和 TVLA-2 的双重检测方法, 分别从固定明文和固定密钥两个方面有效检测私有算法密码芯片的能量信息泄露. 这两种方法所检测的泄露来源不同, 能够多方面保障算法安全. 最后, 我们使用多款私有算法密码芯片开展测评应用实验, 对私有算法密码芯片非入侵式攻击检测框架的有效性进行验证.

(3) 该框架并不局限于私有算法, 同样可以应用于公开算法, 在一定程度上能够保障公开算法密码芯片的安全性, 具有很强的普适性.

本文第 1 节为预备知识, 介绍非入侵式攻击检测的相关研究工作, 并为后续章节提供理论支持. 第 2 节提出私有算法密码芯片非入侵式攻击检测框架. 第 3 节通过测评应用实验对私有算法密码芯片非入侵式攻击检测进行验证. 第 4 节对全文进行总结.

1 预备知识

1.1 非入侵式安全检测技术

随着非入侵式攻击技术的迅速发展, 非入侵式安全成为衡量密码设备安全性的重要因素, 如何保障密码设备

的非入侵式安全这一问题受到越来越多的重视与关注.

目前, 非入侵式安全领域的泄露评估方法研究已取得了一系列成果. 2011 年, Goodwill 等人[6]提出了基于 Welch's t-test 的泄露评估方法, 随后, 在 2013 年这种方法被重命名为 TVLA (test vector leakage assessment), 包含非特定型泄露测试和特定型泄露测试. 此外, TVLA 泄露检测方法还可以扩展到公钥密码算法[7], 如 RSA、ECDSA、ECDH 等算法. 之后, Schneider 等人[8]给出了一个评估实验室可以遵循的高效的测试路线图. 2014 年, Bhasin 等人[9]提出了基于归一化类间方差 (normalized inter-class variance, NICV) 的泄露检测方法, 该方法的优点为计算速度快, 还可用于评估泄露模型的准确性并选择最佳适用模型. 除了经典的 Welch's t-test, 基于 ρ 检验[10]、χ^2 检验[11]、T^2 检验[12]的泄露检测方法相继被提出, 通过使用不同的假设检验方法, 发挥出不同的统计优势[13]. 2021 年, Moos 等人[14]首次提出了基于深度学习的泄露评估方法, 该方法适用范围广, 它使评估者可以不必担心泄露的位置、对齐和统计顺序, 高效地完成对不同密码设备的泄露评估.

上述泄露评估方法极大提高了非入侵式安全检测的准确性和效率, 然而, 这些方法都是针对公开算法提出的, 并未考虑私有算法的情况, 针对私有算法密码芯片的适用性还有待讨论.

1.2 非入侵式攻击检测相关标准

目前国内外已有多个非入侵式安全相关标准. 国际标准 ISO/IEC 19790:2012[15]规定了加密模块的 4 个安全级别, 其中包括非入侵式安全; ISO/IEC 17825:2016[16]规定了非入侵式攻击缓解测试指标, 用于确定是否符合 ISO/IEC 19790:2012 中的要求. 国内标准 GM/T 0008-2012[17]中, 对非入侵式安全提出了要求; GM/T 0028-2014[18]中分别给出了 4 个安全等级的密码模块非入侵式安全具体要求; GM/T 0083-2020[19]介绍了针对密码模块的非入侵式攻击方法及对应的缓解技术, 并给出了密码模块非入侵式攻击测试方法. 这些标准有力保障了密码设备的非入侵式安全, 但都适用于公开算法, 目前还没有专门针对私有算法制定的非入侵式安全检测标准.

1.2.1 GM/T 0083-2020 标准

GM/T 0083-2020《密码模块非入侵式攻击缓解技术指南》[19]是国家密码管理局于 2020 年发布的一项密码行业标准. 如图 1 所示, 在进行非入侵式攻击测试时应遵循操作顺序, 对于密码模块的每个安全功能, 只有全部通过了计时分析、简单能量/电磁分析、差分能量/电磁分析这 3 部分测试, 才能认为密码模块通过测试.

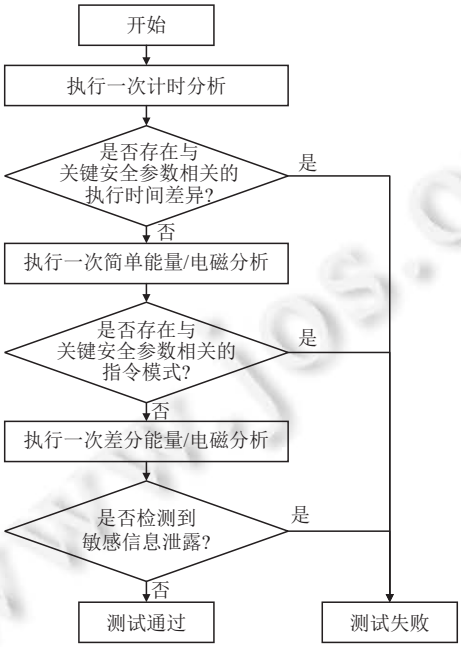

图 1 GM/T 0083-2020 非入侵式攻击测试框架

对于计时分析测试, 泄露分析流程如图 2 所示, 该流程包含两个阶段. 第 1 阶段测量多个不同的关键安全参数 (如密钥) 和固定消息 (如明文) 的执行时间; 第 2 阶段测量多个不同消息和固定关键安全参数的执行时间如果执行时间未显示对消息与关键安全参数的依赖性, 则测试通过, 否则测试失败. 实际中可以利用时钟周期 E 判断执行时间, 对于两个时间值 (或平均时间值) T_1 和 T_2, 如果 $|T_1-T_2|<E$, 则测试通过, 否则失败.

对于简单能量/电磁分析测试, 泄露分析流程如图 3 所示, 该流程包含两个阶段. 第 1 阶段, 采集能量/电磁信息, 采集的测量值数量根据所需安全能力而定. 第 2 阶段, 使用交叉关联的方法对每个测量值进行分析, 如果无法识别出关键安全参数的不规则指令操作序列, 则测试成功, 否则测试失败.

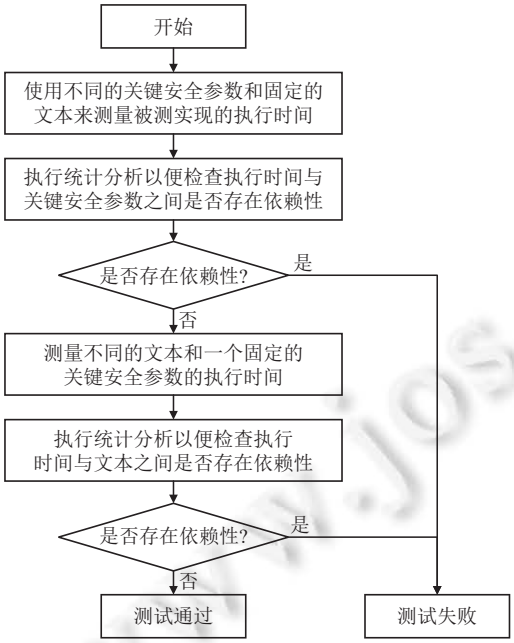

图 2 GM/T 0083-2020 计时分析攻击测试流程

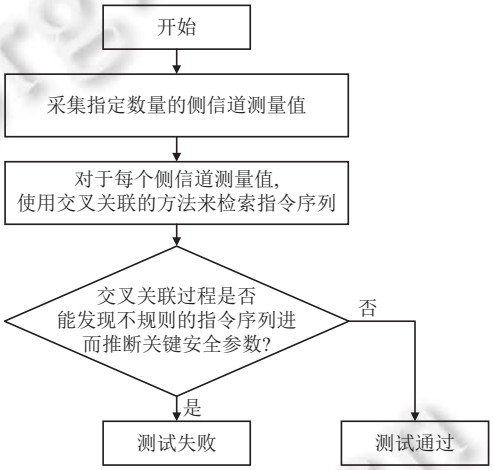

图 3 GM/T 0083-2020 简单能量/电磁攻击测试流程

对于差分能量/电磁分析测试, 泄露分析流程如后文图 4 所示, 该流程包含 4 个步骤. 第一, 采集能量/电磁信息, 采集的测量值数量根据所需安全能力而定; 第二, 对采集的波形进行静态对齐或者动态对齐处理, 并计算信噪比 SNR; 第三, 在信噪比 SNR 满足要求的前提下, 计算密码模块的中间值; 第四, 根据采集的测量值和计算的中间值, 进行 Welch 统计测试, 若统计结果显示无明显泄露, 则通过测试, 否则测试失败.

1.2.2 ISO/IEC 17825:2016 标准

ISO/IEC 17825:2016[16]是第 1 个侧信道攻击方面的国际标准, 该标准按照对称密码体制、非对称密码体制进行分类, 给出相应的计时分析、简单能量/电磁分析、差分能量/电磁分析检测方法. 该标准主要检测方法与 GM/T 0083-2020 类似, 此外还有针对特定算法的检测技术, 这里暂不讨论.

1.3 交叉关联方法

交叉关联是指信号在一个时刻的瞬时值与在另一个时刻的瞬时值之间的依赖关系, 是对一个信号的时域描述, 它是找出重复模式的数学工具. 交叉关联方法可运用到简单能量分析中, 通过计算交叉关联分析结果图来可视化单条能量波形中的重复执行模式, 识别出不规则的指令操作序列.

使用交叉关联对单条能量波形进行分析, 首先需要选定一个“窗口”长度, 以该长度为单位, 每次在波形上向前滑动一个位置, 计算该窗口片段与其他片段的相关系数. 按照此方式计算得到一个相关系数矩阵, 以 $n\times n$ 黑白点阵的形式对相关系数矩阵进行可视化, 黑白点阵中越白的地方说明交叉关联程度越强, 越黑的地方说明交叉关联程

度越弱, 由此构成专用二维图形界面, 以宏观展示交叉关联分析结果. 显然, 在黑白点阵中, 从左上角到右下角的对角线始终是一条白线, 因为这表示片段与其自身的相关性. 分析者可通过该方法识别特定的算法结构, 并获得有关执行敏感操作的位置的信息.

以 ECC 算法波形为例, 使用交叉关联的方法对该波形执行分析, 窗口长度设为 1 000 (约为 1/5 个片段长), 得到的黑白点阵如图 5 所示, 根据黑白点阵中呈现的相关性规律, 可以识别出点加和倍点操作 (图中分别标记为 A 和 D), 从而恢复出 k 值.

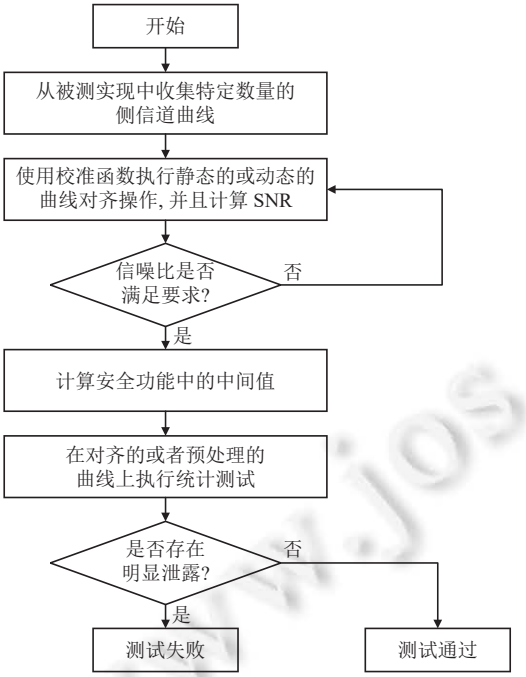

图 4 GM/T 0083-2020 差分能量/电磁攻击测试流程

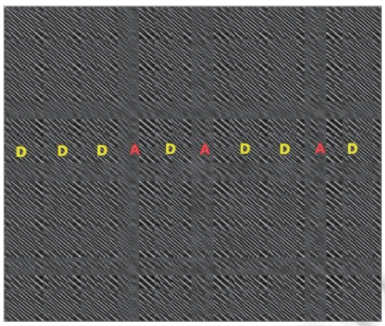

图 5 ECC 算法交叉关联分析结果

1.4 TVLA 泄露评估

在侧信道分析领域, 除简单能量分析、相关能量分析等分析方法外, 还有用于信息泄露量化评估的测试方法. TVLA 方法是一种基于 t-test 的侧信息泄露评估方法[6,8], 该方法常用于敏感信息的泄露检测, 是检测密码设备潜在物理安全风险的简单、可靠的测试方法.

TVLA 分别使用固定明文和随机明文进行加密, 用获得的波形数据进行 t-test, 根据两者统计特性的异同判断波形中是否存在信息泄露. 一组测试包含两次实验, 实验 1 使用固定明文加密 n_1 次, 采集 n_1 条波形; 实验 2 使用随机明文加密 n_2 次, 采集 n_2 条波形. 利用 t-test 判断波形数据的统计特性是否相同, 公式如下:

$$t=\frac{\bar{X}_1-\bar{X}_2}{\sqrt{\frac{S_1^2}{n_1}+\frac{S_2^2}{n_2}}} \tag{1}$$

其中, S_1^2 和 S_2^2 为两组波形数据的方差, $\bar{X}_1$ 和 $\bar{X}_2$ 为两组数据的平均数. 若 $|t|\leqslant 4.5$, 就说明无明显泄露; 否则说明存在泄露. 在 TVLA 方法[8]中, 使用固定明文和随机明文分别得到数目为 n 的波形集, 然后每次 $n/2$ 组数据进行测试, 若两次测试在同一位置均有 $|t|\leqslant 4.5$, 则表明存在泄露.

2 私有算法密码芯片非入侵式攻击检测框架

近年来, 我国芯片市场规模逐渐扩大, 面对非入侵式攻击的威胁, 已有国际国内标准虽然给出了密码模块非入

侵式攻击的测试流程与方法, 但存在以下局限性.

(1) 部分测试方法适用算法范围有限. 目前已有的标准适用于公开算法, 其检测方法大多需要知道所分析密码算法的具体实现, 对于算法细节未知的私有算法, 部分测试无法进行.

(2) 部分测试流程中泄露检测不全面. 现有标准中所使用的分析方法尚不完备, 检测中可能遗漏一些有效的侧信息泄露.

为了解决上述问题, 本文提出一种面向私有算法密码芯片的非入侵式攻击检测框架. 该框架提供了黑盒条件下私有算法密码芯片的测评方案. 在讨论该框架之前, 首先定义私有算法密码芯片非入侵式攻击检测的应用条件.

(1) 芯片中密码算法未知;

(2) 芯片中密码实现方案未知;

(3) 通过明密文位宽、运行时间等信息可判断芯片中密码算法类型为分组密码或公钥密码.

2.1 私有算法密码芯片非入侵式攻击检测框架

我们基于 GM/T 0083-2020 和 ISO/IEC 17825:2016 标准中的非入侵式攻击检测方法, 提出一种面向私有算法密码芯片的非入侵式攻击检测框架, 解决黑盒场景下密码芯片的物理安全性问题. 整体检测框架如图 6 所示, 该框架包含 3 部分: 私有密码算法的计时分析、简单能量/电磁分析和差分能量/电磁分析. 各部分具体的检测流程将在后续章节详细说明. 对于芯片的每个安全功能, 都应遵循框架中的检测顺序, 只有某一环节通过了检测, 才能进入下一环节, 只有通过全部 3 项分析检测, 才能认为密码芯片通过测试. 该框架在不需要了解密码算法中间细节的情况下, 实现对私有算法密码芯片的有效检测, 大大扩展了密码芯片非入侵式安全检测的范围. 此外, 该框架并不局限于私有算法, 也可应用在公开算法, 并在一定程度上能够保证公开算法密码芯片的安全性.

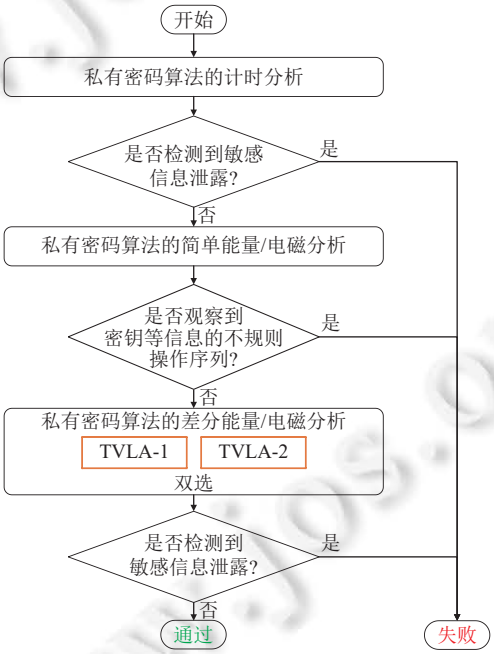

图 6 私有算法密码芯片非入侵式攻击检测框架

与传统非入侵式攻击检测方法不同, 针对私有算法密码芯片的非入侵式攻击检测不涉及算法细节. 表 1 给出了私有算法密码芯片检测框架和传统检测框架之间的各检测环节的比较, 尽管二者都包括计时分析、简单能量/电磁分析和差分能量/电磁分析这 3 个检测环节, 私有算法密码芯片检测框架较传统方法有以下不同.

(1) 对于简单能量/电磁分析环节, 由于检测人员无法定位可能存在简单能量分析泄露的位置, 需要针对整条

波形中各段位置分别进行不规则操作序列判定.

(2) 在简单能量/电磁分析环节, 检测人员在对私有算法密码芯片进行检测后, 需要将检测结果反馈给厂商, 由厂商对疑似存在的泄露位置进行实际泄露判定.

(3) 差分能量/电磁分析环节采用非特定型 TVLA-1 和非特定型 TVLA-2 两种方法对私有算法密码芯片进行检测, 而传统检测框架中只针对公钥密码采用上述两种方法, 对于分组密码采用非特定型 TVLA-1 方法.

(4) 对于差分能量/电磁分析环节, 由于检测人员无法知道算法中间过程, 针对私有分组密码算法芯片的检测不包含特定型 TVLA 分析方法.

表 1 传统检测框架和私有算法检测框架比较

检测环节	传统密码芯片检测框架	私有算法密码芯片检测框架
计时分析	基于平均去噪的计时分析方法	基于平均去噪的计时分析方法
简单能量/电磁分析	采用交叉关联法检测是否存在密钥相关的不规则指令操作序列	采用视觉观察法、交叉关联法分别检测是否存在不规则指令操作序列 检测结果交由厂商确认泄露是否与密钥相关
差分能量/电磁分析	分组密码采用特定型TVLA和非特定型TVLA-1两种方法 公钥密码采用非特定型TVLA-1方法和TVLA-2方法	非特定型TVLA-1方法和TVLA-2方法

与传统非入侵式攻击检测方法相比, 本检测框架在简单能量/电磁分析环节增加了泄露位置反馈步骤, 有效避免了检测过程中产生的误判, 更加适用于私有算法密码芯片检测. 对于差分能量/电磁分析, 本框架提出双重检测方法, 分别从随机明文和随机密钥两个方面对私有算法密码芯片进行检测, 覆盖不同的侧信息泄露来源, 从多角度保障算法安全. 本框架中所使用的非入侵式攻击检测方法不要求恢复完整密钥, 只要存在明显敏感信息泄露, 即可说明所测芯片存在安全隐患, 可能受到非入侵式攻击的威胁, 无法通过检测. 检测框架只提供客观的密码芯片检测结果, 对于检测到的信息泄露, 需要进一步执行安全性评估.

2.2 私有密码算法的计时分析

计时分析根据密码算法执行不同运算所消耗时间的差异来恢复密钥等关键信息. 其差异可能来源于缓存架构带来的时间差异, 缓存未命中比缓存命中花费更多的时间来执行; 执行不同的数学运算带来的时间差异, 有些密码算法根据密钥执行不同操作, 这些操作本身需要不同的时间来进行运算; CPU 的分支预测[20]功能带来的时间差异, CPU 为错误预测的分支付出的代价可用于密码分析等.

目前, 计时分析已成为密码设备安全性的重要威胁之一, 因此对私有算法密码芯片开展计时分析检测是十分必要的. 在私有算法密码芯片非入侵式攻击检测框架中, 我们采用基于平均去噪的计时分析检测方法. 平均去噪是通过对同一测量对象重复采集若干次相加后取平均值来进行噪声消除的方法. 基于平均去噪的计时分析, 就是利用这一原理, 通过 PC 端与芯片通信来获取算法的执行时间, 然后对时间信息去噪后再进行分析. 该方法的实施过程可简单总结为以下两部分.

(1) 设置芯片算法的明文 (或密钥) 为固定值, 选取几个不同的密钥 (或明文), 通过 PC 端与芯片通信获取芯片使用几个不同密钥 (或明文) 进行若干次算法加密的时间, 对使用每个密钥 (或明文) 进行算法加密得到的多次时间值进行平均去噪.

(2) 根据去噪后的时间计算芯片使用不同密钥 (或明文) 执行算法的时间差异, 若存在某一时间差异大于芯片的一个 CPU 时钟周期, 则说明存在时间信息泄露, 测试不通过. 否则, 测试通过, 进入简单能量/电磁攻击测试.

2.3 私有密码算法的简单能量/电磁分析

对于某些添加了缓解计时攻击技术的密码芯片, 虽然在时间上无法检测出信息泄露, 但从能量/电磁信号的变化中, 依然可能获取密钥等关键信息. 能量/电磁分析包括简单能量/电磁分析和差分能量/电磁分析. 为了便于描述, 下文讨论的均为能量分析, 电磁分析与之同理, 不做赘述.

简单能量分析根据密码算法运行时产生的能耗变化, 通过视觉观察或其他简单分析方法, 对指令执行模式进

行直接分析, 信息泄露一般来源于密码相关的不规则操作序列. 不规则操作序列指包含一系列操作, 且包含的操作是不以固定形式循环出现的序列. 简单能量分析检测不规则操作序列并判断其是否和密钥等关键信息相关. 目前已有的国际标准 ISO/IEC 17825:2016、国内标准 GM/T 0083-2020 中, 给出了简单能量泄露测试流程, 芯片检测人员可以通过流程中的测试方法判断芯片是否存在简单能量分析泄露, 但这些标准中给出的测试方法都是针对公开算法, 对于私有算法没有相关检测说明.

简单能量分析的核心是判定能量波形中是否存在“不规则操作序列”, 以及该序列与密钥是否存在关系. 对于已知算法, 检测人员可根据算法过程直接锁定可能存在简单能量分析泄露的位置进行检测; 但对于未知算法, 其问题在于检测人员无法确定密钥与中间操作之间的关系, 因而无法定位可能存在简单能量分析泄露的位置进行检测, 只能针对整条波形中各段位置分别进行不规则操作序列判定, 并由厂商对不规则操作序列与密钥之间的关系进行确认.

本文提出的私有算法密码芯片非入侵式攻击检测框架中, 简单能量分析的泄露测试流程如图 7 所示, 该流程包括 4 个步骤.

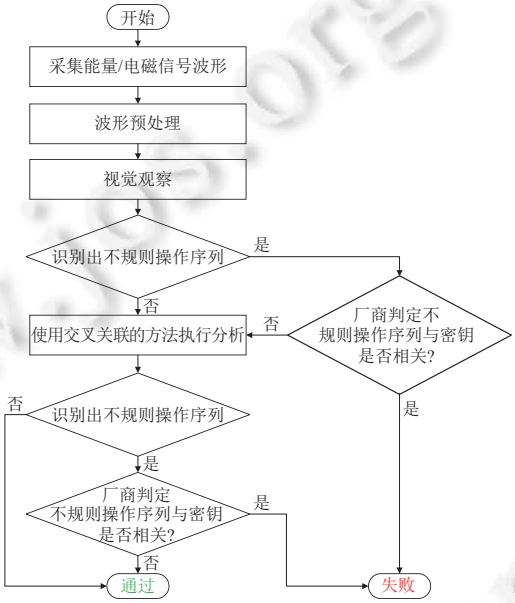

图 7　私有算法简单能量/电磁分析测试流程

(1) 采集密码算法运行时产生的能量/电磁信号波形.

(2) 对采集的波形进行预处理, 如采用低通滤波、对齐等波形处理方式. 预处理能提高分析效率, 使分析结果更明显.

(3) 通过视觉观察的方式, 对波形进行分析. 视觉观察阶段检测人员需要肉眼观测来识别波形中是否存在不规则操作序列, 若检测人员能够识别出不规则操作序列, 则由厂商根据所分析算法的实现过程对不规则操作序列进行判定, 如果其与密钥等关键信息是无关的, 则继续进行下一步骤, 否则测试失败.

(4) 使用交叉关联的方法对波形进行分析, 检测人员通过计算交叉关联分析结果图来可视化单条能量波形中的重复执行模式, 从而识别不规则指令操作序列, 具体方法介绍详见第 1.3 节. 若分析结果显示波形中存在不规则操作序列, 则由厂商根据所分析算法的实现过程对不规则操作序列进行判定, 若其与密钥等关键信息无关, 则测试通过, 进入差分能量/电磁攻击测试. 否则, 测试失败.

为了进一步说明简单能量分析检测方法的适用性, 我们分别对私有公钥密码算法和私有分组密码算法进行探讨.

2.3.1 私有公钥密码算法简单能量分析

对于公钥密码算法, 其能量波形往往存在两个明显特征. 第一, 算法执行时间长, 公钥密码算法实现复杂, 导致其速度比对称密码算法慢几个数量级. 第二, 波形中呈现长时间规律性运算的部分, 往往与常见的密钥位宽相关, 如 RSA 算法的密钥位宽有 1 024、2 048 等, ECC 算法的密钥位宽有 256 等. 在密码芯片算法类型未知的情况下, 可以根据能量波形是否存在这些特征, 判断芯片使用的是否是公钥算法.

在假定待测算法为公钥算法的前提下, 可进一步通过长时间规律性运算来猜测其特定操作序列是否为公钥密码算法中常见的标量乘、模幂等运算, 并采用视觉观察、交叉关联等典型方法对该运算进行信息泄露判定. 若推测出该运算为标量乘、模幂等常见运算, 则判断波形是否存在不规则操作序列. 不规则操作序列, 指包含一系列操作, 且操作不以固定形式循环出现的序列.

除了常见的 RSA、ECC 算法, 现实中还存在其他公钥密码算法, 如后量子算法. 若私有公钥密码算法的能量波形特征显示该算法不是 RSA、ECC 这类算法, 则无法使用上述方法进行泄露分析. 另外, 虽然在经典 RSA、ECC 算法中, 标量乘、模幂以外的运算一般不存在简单能量分析泄露, 但这并不能说明私有公钥密码算法中除标量乘、模幂这些常见运算以外的其余部分也不存在简单能量分析泄露. 对于私有公钥算法而言, 检测人员在对不规则操作序列进行检测后, 可以将检测结果反馈给厂商, 由厂商对疑似存在泄露的位置进行实际泄露判定.

2.3.2 私有分组密码算法简单能量分析

对于存在条件分支语句的私有分组密码算法, 可以通过简单能量分析对分支语句的不同操作进行区分, 从而获得不规则操作序列.

若不规则操作序列对应的中间值与密钥相关, 则存在信息泄露. 例如, AES 算法首轮中间状态 state 进行列混合运算时各个字节的第 1 比特存在简单能量分析泄露, 如图 8 所示, 检测人员可根据此处分支语句呈现的不同特征区分出该密钥比特, 进而恢复密钥. 若不规则操作序列对应的中间值与密钥无关, 尽管区分出了不同操作, 也无法恢复密钥, 不存在信息泄露. 例如, DES 算法的密钥扩展中, 分支语句仅与密钥轮数相关, 左循环移位 LS_i 操作根据密钥轮数 i 选择循环左移一位或两位, 不涉及具体密钥值或中间值.

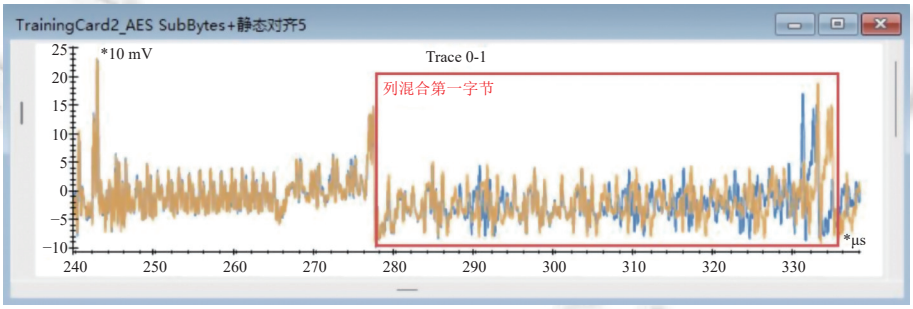

图 8 AES 算法首轮列混合运算第 1 字节的波形, 两条波形显示不同分支语句呈现的不同特征

实际中, 在算法过程未知的条件下, 检测人员仅能通过简单能量分析对私有分组密码算法进行检测, 找到波形中可能存在不规则操作序列的位置, 而无法判定其是否与密钥直接相关. 因而, 该环节后续需要厂商的配合, 各个不规则操作序列是否真正存在泄露, 需要由厂商结合算法过程进行判断分析.

2.4 私有密码算法的差分能量/电磁分析

若简单能量/电磁分析方法无法获取密码算法的密钥等关键信息, 或者分析结果显示无明显信息泄露, 需要继续进行差分能量/电磁分析测试. 差分能量/电磁分析通过统计方法, 进一步对密码算法运行时产生的能耗/电磁辐射信息进行分析. 为了便于描述, 下文讨论的均为能量分析, 电磁分析与之同理, 不做赘述.

对于差分能量/电磁分析测试, 本检测框架使用 TVLA 方法进行检测. 该方法基于 t-test 分析进行侧信息泄露分析, 分为特定型 TVLA 和非特定型 TVLA. 特定型 TVLA 方法是针对算法特定位置的分析方法, 如选取特定中

间值为 0 或者具有很小汉明重量的波形, 而非特定型 TVLA 只要求选取随机明文. 然而, 对于私有密码算法, 密码算法细节不公开, 检测人员无法获得算法实现过程, 因此不能使用算法中间值进行特定型 TVLA 分析. 本文采用非特定型 TVLA 方法, 该方法只对明文和密钥有要求, 不受算法过程的影响, 适用于私有密码算法. 此外, 考虑到明文和密钥均可能带来能量信息泄露, 我们采用了 TVLA-1 和 TVLA-2 两种非特定型方法对私有密码算法进行双重检测. 具体方法如下.

(1) TVLA-1 (test vector leakage assessment-type 1) 方法: 在固定密钥的情况下, 分别使用固定明文和随机明文进行一定次数的加密, 得到对应的两组能量波形. 用获得的两组能量波形进行 t-test, 根据两者统计特性的异同判断波形中是否存在明文导致的信息泄露. 判别过程详见本文第 1.4 节.

(2) TVLA-2 (test vector leakage assessment-type 2) 方法: 在固定明文的情况下, 分别使用固定密钥和随机密钥进行一定次数的加密, 得到对应的两组能量波形, 用获得的两组能量波形进行 t-test. 该方法旨在检测密钥导致的能量信息差异, 与第 1 种方法所检验的泄露来源不同, 但具体实施过程类似.

本文提出的框架中, 差分能量/电磁分析的泄露测试流程如图 9 所示, 该流程包括 6 个步骤.

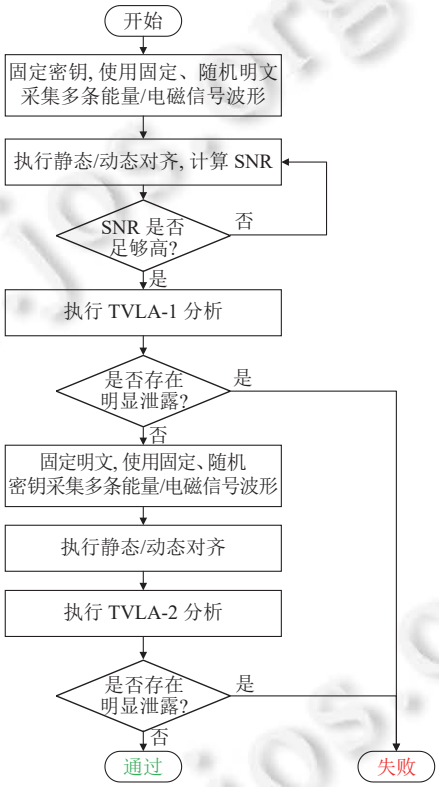

图 9 私有算法差分能量/电磁分析测试流程

(1) 分别以固定明文和随机明文作为输入, 使用固定密钥多次执行算法, 采集得到固定明文和随机明文的两组能量波形;

(2) 对波形执行静态/动态对齐, 以便在分析计算时, 可以在同一点比较不同的波形. 计算信噪比 SNR, 若 SNR 足够高, 则执行下一步骤, 否则重新执行本步骤;

(3) 使用对齐后的两组波形, 采用 TVLA-1 方法进行分析, 若分析结果显示存在明显信息泄露, 则测试失败, 否则继续执行下一步骤;

(4) 以固定明文作为输入, 分别使用固定密钥和随机密钥多次执行算法, 采集得到固定密钥和随机密钥的两组

能量波形;

(5) 对波形执行静态/动态对齐, 以便在分析计算时可以在同一点比较不同的波形;

(6) 使用对齐后的两组波形, 采用 TVLA-2 方法进行分析, 若分析结果显示无明显信息泄露, 则测试通过, 整个测试流程完成, 否则, 测试失败.

接下来, 我们分别对分组密码算法和公钥密码算法这两种类型的私有算法进行探讨.

2.4.1 私有公钥密码算法的差分能量分析方法

标准 ISO/IEC 17825:2016、GM/T 0083-2020 中给出的面向公钥密码算法的非特定型 TVLA 差分能量分析方法天然适用于私有公钥密码算法的场景, 本文同样采用非特定型 TVLA 方法对私有公钥密码算法进行差分能量分析检测. TVLA-1 和 TVLA-2 两种方法对公钥密码算法执行差分能量分析, 能够对不同的泄露进行有效检测. TVLA-1 能够有效检测明文及中间值带来的能量信息泄露. 根据算法使用固定明文和随机明文进行加密的能量信息差异, 可以获取算法运算过程或者中间值相关信息. 例如 RSA 数字签名算法的 $x^d \bmod N$ 过程, 如果 N 和明文 x 未加防护 (如掩码), 而私钥 d 加了防护, 且该算法未加其他防护, 则该算法可能无法通过 TVLA-1 检测, 而通过 TVLA-2 检测. TVLA-2 能够有效检测密钥带来的能量信息泄露. 我们可以根据算法使用固定密钥和随机密钥进行加密的能量信息差异, 获取算法的密钥相关信息. 仍然以 RSA 数字签名算法的 $x^d \bmod N$ 过程为例, 如果私钥 d 未加防护, 而 N 和明文 x 加了防护, 且该算法未加其他防护, 则该算法可能无法通过 TVLA-2 检测, 而通过 TVLA-1 检测. TVLA-2 还能够有效检测简单能量分析检测不出来的指令执行模式差异. 例如 RSA 算法模幂运算的平方-乘操作, 在加了防护的情况下, 平方运算的能量特征和乘操作的能量特征可能仅存在较小的差异, 我们无法通过视觉观察、交叉关联等简单能量分析方法从单条能量波形中识别出来. 而 TVLA-2 方法借助 t-test 统计方法, 使用多条能量波形进行 t 值计算, 能够有效识别不同操作的细微差异, 从而更有力地检测芯片算法的简单能量分析泄露.

TVLA-1 和 TVLA-2 能够从不同角度实现泄露检测, 因此私有公钥密码算法应使用这两种方法执行差分能量分析, 无论使用这两种方法中的哪一种检测出了信息泄露, 都说明芯片可能存在安全性问题.

2.4.2 私有分组密码算法的差分能量分析方法

与公钥密码算法不同, ISO/IEC 17825:2016、GM/T 0083-2020 标准中使用特定型 TVLA 和非特定型 TVLA-1 这两种方法对分组密码算法进行差分能量分析. 然而, 该标准无法直接应用于私有分组密码算法. 首先, 特定型 TVLA 方法使用算法中间值进行分析, 这就要求检测人员了解算法实现过程, 而私有分组密码算法的过程未知. 其次, 关于非特定型 TVLA 方法, 标准中仅使用 TVLA-1 方法对分组密码算法进行差分能量分析泄露检测, 未提及 TVLA-2 方法.

由于特定型 TVLA 方法是针对算法特定位置的分析, 该方法不适用于私有分组密码算法, 故在我们的检测方法中不予考虑. 对于非特定型 TVLA, TVLA-1 方法能够有效检测分组密码算法中明文及中间值带来的能量信息泄露, 例如, Schneider 等人[8]使用该方法对 AES 算法进行了有效泄露检测. 我们建议沿用 TVLA-1 方法对私有分组密码算法执行差分能量分析检测. 除此之外, 我们认为私有分组密码算法还需要使用 TVLA-2 方法进行泄露检测. 除明文及中间值带来的能量信息泄露之外, 分组密码算法中也可能存在密钥或子密钥带来的能量信息泄露, 例如, 在 IDEA 算法的轮结构中, 存在中间值与子密钥的整数模 2^{16} 加操作和整数模 $2^{16}+1$ 乘操作, 这些操作可能泄露密钥信息. 因而对于私有分组密码算法, 同样需要使用 TVLA-2 方法进行差分能量分析检测.

对于私有分组密码算法而言, 应使用 TVLA-1 和 TVLA-2 两种方法执行差分能量分析泄露检测, 不论使用这两种方法中的哪一种检测出了信息泄露, 均表示芯片可能存在安全性问题.

3 私有算法密码芯片非入侵式攻击检测实例

由于传统的基于平均去噪的计时分析方法不涉及算法细节, 同样适用于私有算法密码芯片的计时分析检测, 因此本文略去对第 1 部分计时分析检测的描述, 仅对第 2、3 部分能量/电磁分析检测实例进行详细介绍.

我们共采购了 7 种密码芯片, 分别以 A、B、C、…、G 进行编号, 相关信息如表 2 所示.

表 2 待测私有算法密码芯片

指标	芯片A	芯片B	芯片C	芯片D	芯片E	芯片F	芯片G
算法类型	公钥密码	公钥密码	分组密码	公钥密码	公钥密码	公钥密码	分组密码
明密文长度 (比特)	1 024	1 024	128	1 024	1 024	1 024	32
密钥长度 (比特)	1 024	1 024	128	1 024	1 024	1 024	64
是否带防护	否	否	—	是	是	是	—

3.1 私有算法密码芯片的简单能量分析测评

本节使用视觉观察和交叉关联的方法, 分别对公钥密码算法芯片 A、芯片 B 和分组密码算法芯片 C 开展黑盒条件下简单能量分析测评应用实验.

3.1.1 私有公钥密码的简单能量分析测评

芯片 A 是一款公钥密码算法智能卡芯片, 算法实现了对 1 024 比特的密文进行解密, 并返回 1 024 比特的明文结果, 所使用的 1 024 比特的私钥支持更改. 对于芯片 A 算法中解密过程的具体实现, 该厂商未透露任何信息. 我们使用图 10 所示的接触式智能卡采波平台获取芯片 A 运行过程中产生的能量信息, 进行芯片的简单能量分析测评实验.

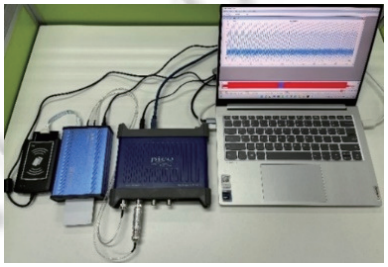

图 10 接触式智能卡采波平台

首先, 我们采集芯片 A 执行解密算法的能量波形. 设置私钥为:

d= 0x00DB3717BDBCF6191AC1DE815CB60F6FD2DAC9D8B724039887BB8C02EBF0E56E6D27453FA4954C807C7F34EB60D2E54FFB28B6360847E65B68671D0953AE45C0EB7D257BFFDB6A21F04418BA48AF793D93BA4DDCD3DA5344521526A3F18A9066E5E5E4C1514AA693A71C4AD5C7AA1F54B0E7CD3E744F8EA446D564E3CC2BE55D.

以 12.5 MSa/s (MSa/s 表示百万样本每秒, 用于描述数字示波器或数据采集系统的采样率) 采样率采集得到的单条波形如图 11 所示, 该波形有 8 000 000 个采样点.

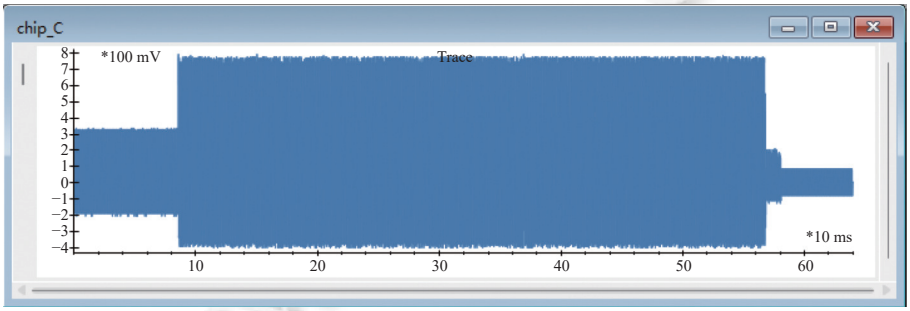

图 11 芯片 A 单条能量波形

观察可知, 在波形的 80–580 ms 区间内, 芯片执行算法消耗能量较高, 我们选取 100–120 ms 波形区间放大查看, 如图 12 所示. 以尖峰作为波形段切分点, 在 80–580 ms 区间内共计 1 547 个波形段, 而在私钥 d 的 1 024 比特

中, 有 523 个比特 1 和 501 个比特 0, 由此推测, 该芯片算法是一种类 RSA 算法. 该芯片算法的指令操作序列可分为两种, 我们记为 O_1 和 O_2. 私钥的每个比特 0 对应一个 O_1, 私钥的每个比特 1 对应一个 O_1 和一个 O_2.

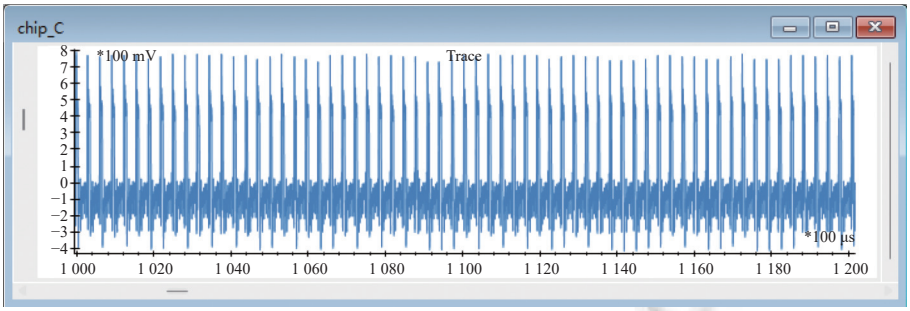

图 12 芯片 A 单条能量波形部分区间

接下来, 通过视觉观察与交叉关联的方法来辨别 O_1 和 O_2, 如图 13 所示, 结尾位置 565 800–567 160 µs 区域包含 5 个操作, 根据框选区域的特征可直接通过视觉区分 O_1 和 O_2, 红色框选区域对应 O_1, 黑色框选区域对应 O_2, 这 5 个操作依次为 O_1、O_2、O_1、O_1、O_2, 对应的比特值是 101, 与私钥的第 2、1、0 位正确对应. 同理, 图 14 所示, 起始位置 85 880–87 280 µs 区域包含 4 个操作, 这 4 个操作均为 O_1, 对应的比特值为 0000, 与私钥的第 1 023、1 022、1 021、1 020 位正确对应. 继续按照此规律进行分析, 私钥的其余 1 017 个比特位也能够被成功恢复, 因此存在明显泄露.

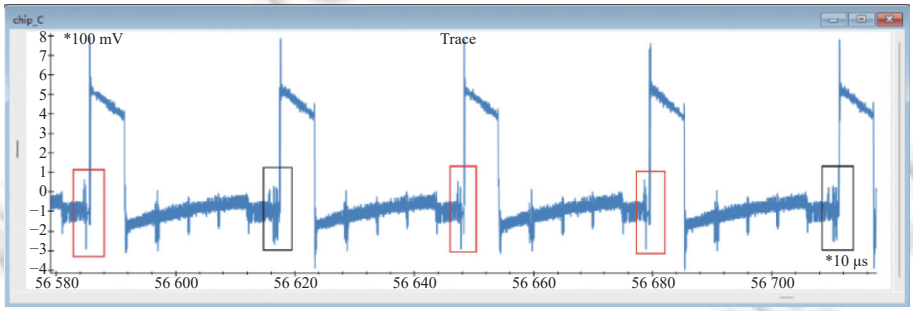

图 13 芯片 A 能量波形操作序列末尾区域

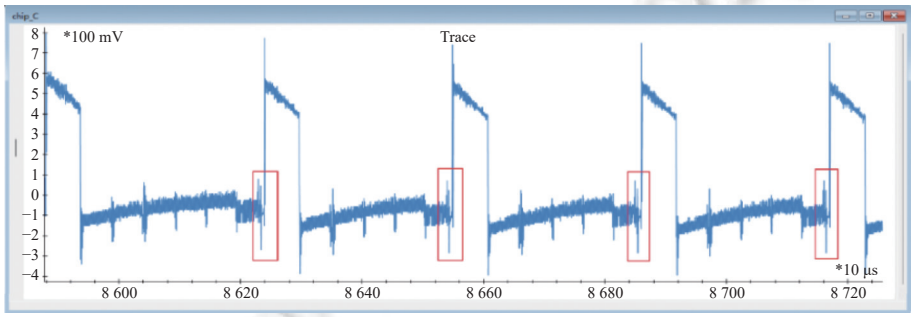

图 14 芯片 A 能量波形操作序列起始区域

我们继续使用交叉关联的方法对指令操作序列进行分析, 图 15 给出交叉关联分析在波形末尾区域的结果. 根据交叉关联的分析结果, 能够通过条形带的宽度区分出 O_1 和 O_2, 进一步证明存在明显泄露. 视觉观察和交叉关联分析结果说明, 该芯片无法通过简单能量分析测试.

随后我们使用同类型另一款芯片 B 进行实验. 我们继续使用设定的私钥 d 执行解密算法, 以 12.5 MSa/s 采样率采集得到的单条能量波形如图 16 所示, 该波形有 7 000 000 个采样点.

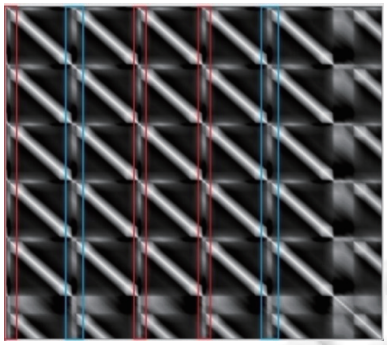

图 15　芯片 A 能量波形操作序列末尾区域交叉关联分析结果

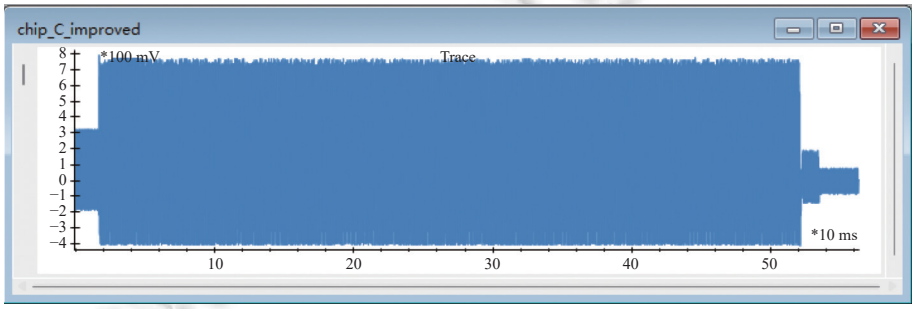

图 16　芯片 B 单条能量波形

以尖峰作为波形段切分点, 在波形的 10–530 ms 区间内共计 1 547 个波形段, 数量无变化. 我们定位到指令操作序列的末尾和起始区域进行分析, 图 17 所示 515 920–517 360 μs 区域包含末尾的 5 个操作, 如后文图 18 所示, 17 280–18 720 μs 区域包含起始的 4 个操作, 可以发现与芯片 A 不同, 这里 O_1 和 O_2 特征相似, 我们通过视觉观察无法区分. 继续使用交叉关联的方法对指令操作序列的末尾进行分析, 交叉关联分析结果如后文图 19 所示, 图中黄色框选区域的条形带宽度相同、明暗特征相似, 同样无法区分 O_1 和 O_2, 不存在明显泄露. 实验说明同类型的芯片 B 能够通过简单能量分析测试.

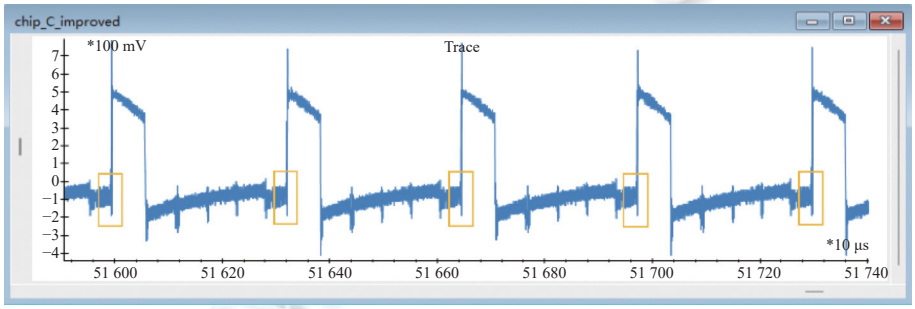

图 17　芯片 B 能量波形操作序列末尾区域

3.1.2　私有分组密码的简单能量分析测评

芯片 C 是一款智能卡芯片, 算法实现了使用 16 字节的密钥, 对 16 字节明文进行加密, 返回 16 字节的密文结

果. 我们使用图 10 所示的接触式智能卡采波平台获取芯片 C 运行过程中产生的能量信息, 来完成芯片的简单能量分析测评实验. 以 12.5 MSa/s 采样率采集到的单条波形如图 20 所示, 该波形有 17 000 个采样点.

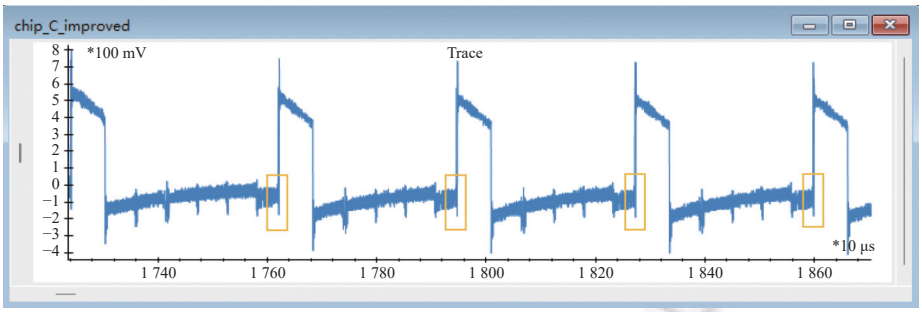

图 18　芯片 B 能量波形操作序列起始区域

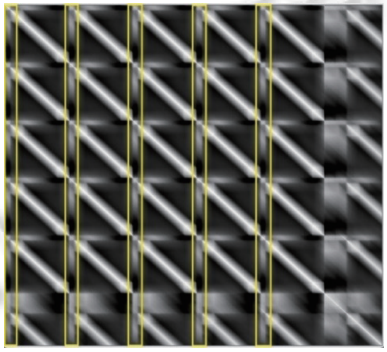

图 19　芯片 B 能量波形操作序列末尾区域交叉关联分析结果

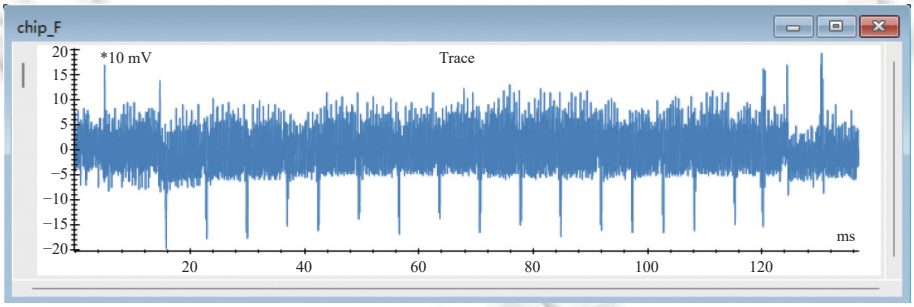

图 20　芯片 C 单条能量波形

若以向下的尖峰作为波形段切分点, 在波形的 160–1 200 µs 区间内共计 16 个波形段, 且每个波形段特征都很相似. 由于该算法的明文和密钥均为 16 个字节, 因此我们猜测这 16 个波形段与明文或者密钥相关, 每个波形段在执行一个字节明文或者密钥的运算操作. 除此之外, 这 16 个波形段存在两种形态, 一种波形段较长, 另一种较短, 且易于区分, 于是我们猜测这两种波形段代表两种不同的操作, 我们将较长的波形段对应的操作记为 O_7, 较短的记为 O_8. 由此可恢复出操作序列: O_7、O_7、O_7、O_8、O_7、O_7、O_7、O_7、O_7、O_7、O_7、O_8、O_8、O_8、O_7、O_8. 我们使用交叉关联的方法对图 20 波形执行分析, 得到的分析结果如图 21 所示, 根据该分析结果也能恢复出操作序列. 因此, 芯片 C 可能存在信息泄露. 但我们无法判断其泄露是否真的与明文或者密钥相关, 具体安全性结论需要厂商根据该泄露检测结果进一步分析.

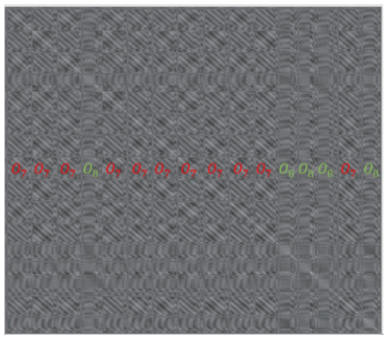

图 21　芯片 C 单条能量波形交叉关联分析结果

3.2　私有算法密码芯片的差分能量分析测评

本节对几款不同的密码芯片开展黑盒条件下差分能量分析测评应用实验. 其中, 芯片 B、芯片 D–F 使用的是公钥密码算法, 芯片 G 使用的是分组密码算法, 芯片 D–F 厂家声称增加了侧信道防护手段.

3.2.1　私有公钥密码的差分能量分析测评

在第 3.1.1 节中, 我们对芯片 B 执行了简单能量分析检测, 测试结果表明, 芯片 B 能通过简单能量分析检测. 由于私有密码算法差分能量分析方法中的 TVLA-2 方法能够有效检测简单能量分析检测不出来的指令执行模式差异, 我们使用 TVLA-2 方法进一步检验芯片 B 的安全性. 与此同时, 为了验证防护的效果, 我们对相同厂商几款声称添加了防护的公钥密码芯片也执行 TVLA-2 检测.

(1) 对芯片 B 执行 TVLA-2 检测

设置密文为固定值, 芯片使用固定私钥和随机私钥进行解密, 以 12.5 MSa/s 采样率采集得到 10000 条能量波形, 如图 22 所示, 每条波形有 7000000 个采样点. 其中, 使用固定私钥和随机私钥采集得到的波形数量约为 1:1.

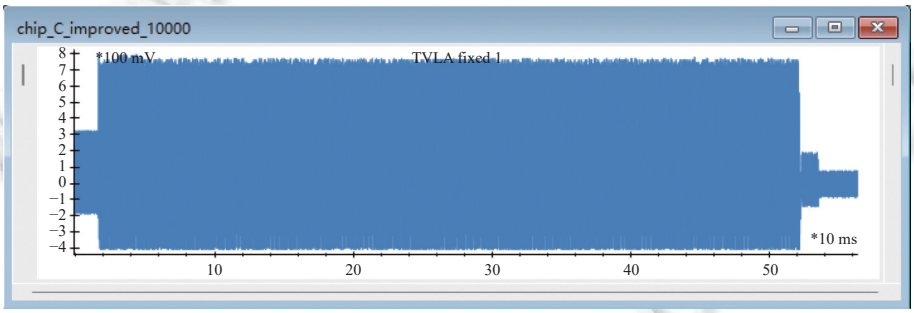

图 22　芯片 B 能量波形

对采集的 10000 条能量波形执行静态对齐, 然后进行 TVLA-2 分析, 得到的 t 值结果曲线如图 23 所示, 阈值 4.5 在图中以黄色水平线进行标示. 可以看出, 整个解密过程中存在大量区域 t 值高于阈值 4.5, 存在明显信息泄露. 实验结果说明了即使密码设备通过了简单能量分析检测, 仍可能存在能量信息泄露.

(2) 对带防护的芯片 D 执行 TVLA-2 检测

我们对带防护的芯片 D 以相同的设置采集得到 10000 条能量波形, 如图 24 所示, 每条波形有 8500000 个采样点. 其中, 使用固定私钥和随机私钥采集得到的波形数量约为 1:1.

可以观察到, 在波形的 20–640 ms 区间内, 芯片执行算法消耗能量较高, 我们猜测该区间内芯片在执行算法解密. 对采集的 10000 条能量波形执行静态对齐后, 针对算法解密结束的位置叠加多条波形进行查看, 如图 25 所示, 能够发现算法多次解密的时间基本一致. 除此之外, 可以估算出, 解密过程中执行 O_1 和 O_2 操作的总数量约为私钥比特数的 2 倍. 因此, 我们猜测不论算法的密钥为何值, 解密过程均交替执行 O_1 和 O_2 操作, 或者 O_1 和 O_2 的伪操作.

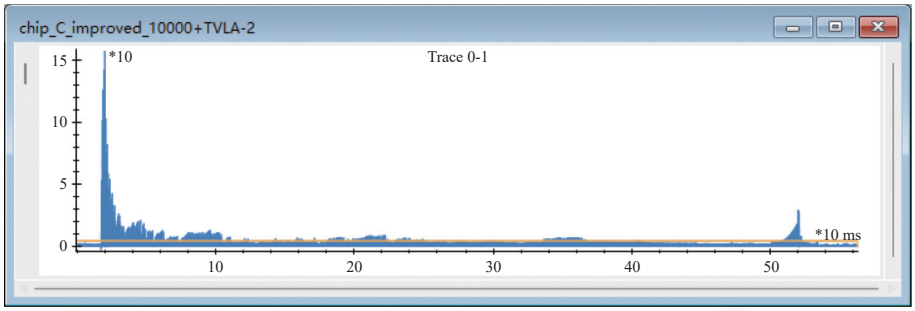

图 23　芯片 B 的 TVLA-2 分析结果

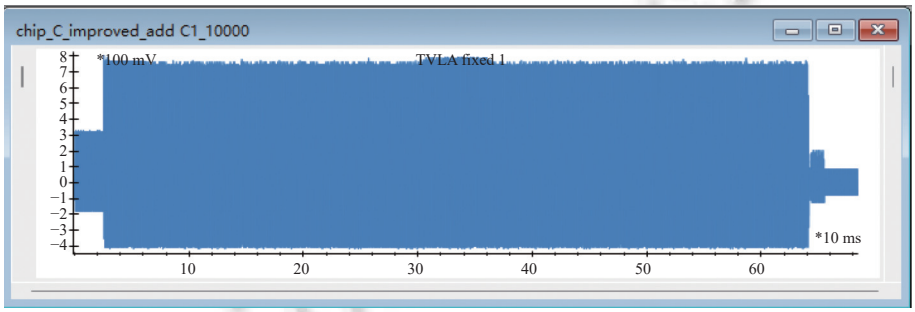

图 24　芯片 D 能量波形

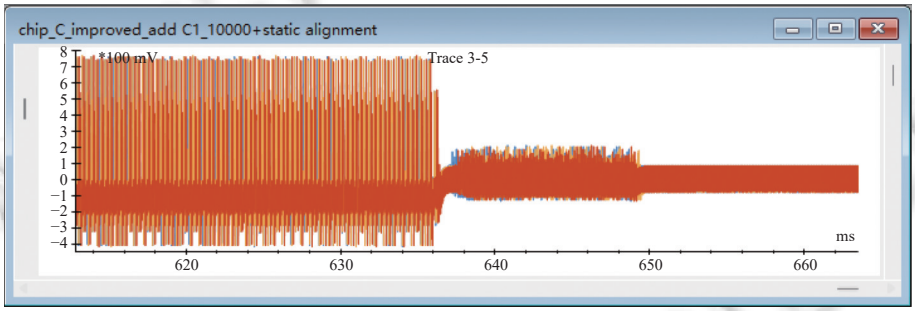

图 25　芯片 D 解密结束位置叠加多条能量波形

我们对静态对齐后的波形执行 TVLA-2 分析, 得到的 t 值结果曲线如图 26 所示. 可以看出, 波形最后区域的泄露情况较不加防护时有所减轻, 但整体仍然存在较高泄露, 我们猜测泄露来源于真 O_2 与伪 O_2 之间的差异.

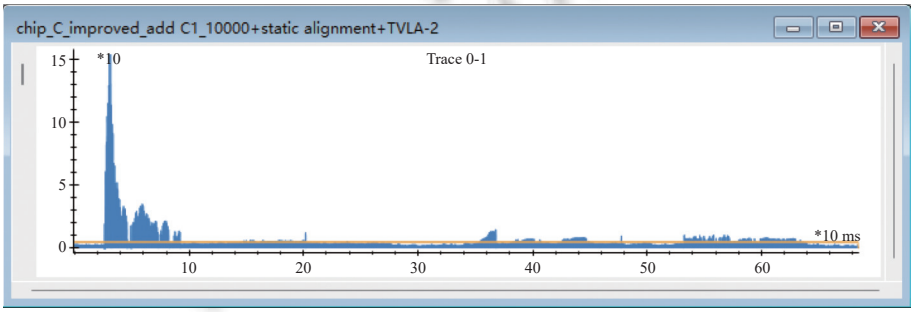

图 26　芯片 D 的 TVLA-2 分析结果

(3) 对带防护的芯片 E 执行 TVLA-2 检测

我们对带防护的芯片 E 采集得到 10 000 条能量波形, 每条波形有 8 000 000 个采样点. 其中, 使用固定私钥和随机私钥采集得到的波形数量约为 1:1. 我们对所采集波形的单条波形进行局部查看, 如图 27 所示, 根据波形特征, 我们猜测所加防护可能为随机延时.

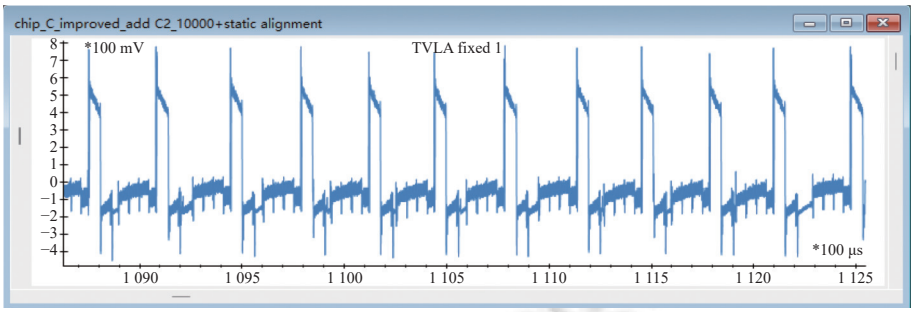

图 27 芯片 E 能量波形局部区域

对静态对齐后的波形执行 TVLA-2 分析, 得到的 t 值结果曲线如图 28 所示. 可以看出, 仅在解密的开始和结束位置存在泄露, 我们猜测开始区域的泄露来源于延时发生之前 O_1 和 O_2 之间的差异, 结束位置的泄露来源于随机延时带来的多次解密结束时间的不一致.

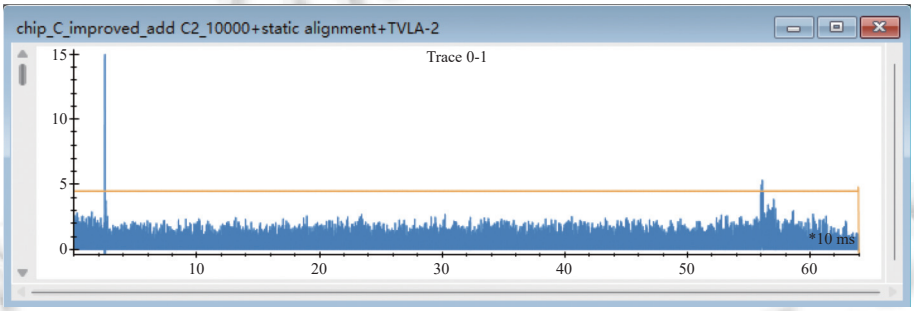

图 28 芯片 E 的 TVLA-2 分析结果

(4) 对带防护的芯片 F 执行 TVLA-2 检测

我们对带防护的芯片 F 采集得到 10 000 条能量波形, 每条波形有 10 000 000 个采样点. 其中, 使用固定私钥和随机私钥采集得到的波形数量与前相同, 约为 1:1. 对静态对齐后的波形执行 TVLA-2 分析, 得到的 t 值结果曲线如图 29 所示, 可以看到无明显信息泄露. 该芯片的防护手段足够安全, 能够通过 TVLA-2 检测.

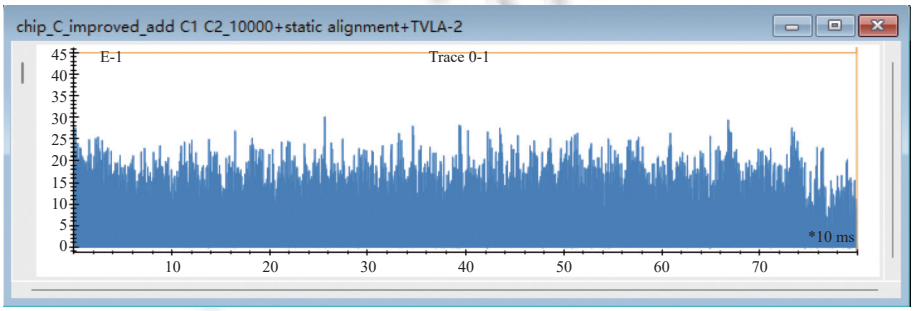

图 29 芯片 F 的 TVLA-2 分析结果

3.2.2 私有分组密码的差分能量分析测评

芯片 G 是一款智能卡芯片, 实现了对 4 字节的明文进行加密, 并返回 4 字节密文, 密钥为 8 字节. 对于芯片 G 算法中的加密过程、密钥值和防护方式的具体实现, 我们均不知. 由于私有密码算法差分能量分析方法中的 TVLA-1 方法能够有效检测明文及中间值带来的能量信息泄露, 我们使用 TVLA-1 方法检测芯片 G 的安全性.

我们使用固定明文和随机明文进行加密, 采集得到 10 000 条能量波形, 如图 30 所示, 每条波形有 30 000 个采样点. 其中, 固定明文的值为 p = 0x375C6AB9, 随机明文的值为随机生成的 4 字节数据, 使用固定明文和随机明文采集得到的波形数量约为 1:1. 根据波形特征和分组密码算法相关知识, 我们猜测在 120–1 120 μs 区间内算法在执行密钥扩展, 1 120–2 160 μs 区间内算法在执行加密, 需要分析的为加密阶段.

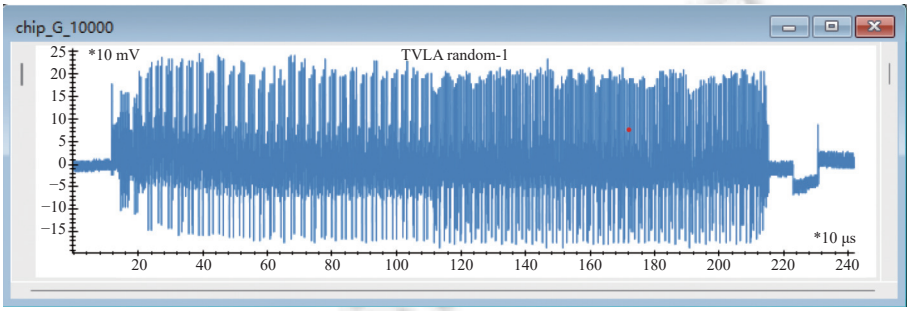

图 30 芯片 G 能量波形

以密钥扩展结束后加密开始位置的波形片段为模板, 对采集的 10 000 条能量波形执行静态对齐, 然后进行 TVLA-1 分析, 得到的 t 值结果曲线如图 31 所示, 加密的大部分区域 t 值大于 4.5, 存在明显的信息泄露.

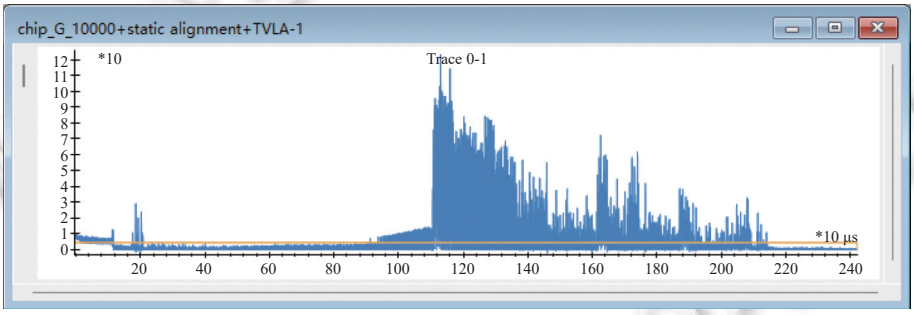

图 31 芯片 G 的 TVLA-1 分析结果

4 总 结

近年来, 非入侵式攻击对密码芯片的安全性造成了严重威胁. 国际标准 ISO/IEC 17825:2016、国内标准 GM/T 0083-2020 中给出了非入侵式攻击检测流程与方法, 用于检测密码模块的抗非入侵式攻击能力, 但这些标准是针对公开算法制定的, 不适用于使用私有算法的密码芯片, 存在局限性. 基于这一现状, 本文研究了黑盒条件下私有算法密码芯片的非入侵式攻击检测方法, 提出了私有算法密码芯片非入侵式攻击检测框架. 该框架包含私有密码算法的计时分析测试、简单能量/电磁分析测试、差分能量/电磁分析测试这 3 大部分, 无需了解密码算法中间细节, 大大扩展了密码芯片非入侵式安全的检测范围. 本文对多款密码芯片开展黑盒条件下简单能量分析测评和差分能量分析测评实验, 实验表明, 我们的方法能够在一定程度上检测私有算法密码芯片的抗能量攻击能力. 私有算法密码芯片非入侵式攻击检测这一方向具有广阔前景, 未来我们还会在目前研究的基础上继续探索, 尝试通过更多的方法对私有算法密码芯片进行检测, 例如, 可以尝试结合机器学习方法进行黑盒能量分析检测等.

References

[1] Kocher PC. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Proc. of the 16th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 1996. 104–113. [doi: 10.1007/3-540-68697-5_9]

[2] Kocher P, Jaffe J, Jun B. Differential power analysis. In: Proc. of the 19th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 1999. 388–397. [doi: 10.1007/3-540-48405-1_25]

[3] Gandolfi K, Mourtel C, Olivier F. Electromagnetic analysis: Concrete results. In: Proc. of the 3rd Int'l Workshop on Cryptographic Hardware and Embedded Systems. Paris: Springer, 2001. 251–261. [doi: 10.1007/3-540-44709-1_21]

[4] Tsunoo Y, Saito T, Suzaki T, Shigeri M, Miyauchi H. Cryptanalysis of DES implemented on computers with cache. In: Proc. of the 5th Int'l Workshop on Cryptographic Hardware and Embedded Systems. Cologne: Springer, 2003. 62–76. [doi: 10.1007/978-3-540-45238-6_6]

[5] Wang A, Ge J, Shang N, Zhang F, Zhang GS. Practical cases of side-channel analysis. Journal of Cryptologic Research, 2018, 5(4): 383–398 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000249]

[6] Goodwill G, Jun J, Jaffe J, Rohatgi P. A testing methodology for side-channel resistance validation. In: Proc. of the 2011 NIST Non-invasive Attack Testing Workshop. Nara: NIST, 2011. 115–136.

[7] Jayasena A, Andrews E, Mishra P. TVLA*: Test vector leakage assessment on hardware implementations of asymmetric cryptography algorithms. IEEE Trans. on Very Large Scale Integration (VLSI) Systems, 2023, 31(9): 1269–1279. [doi: 10.1109/TVLSI.2023.3297027]

[8] Schneider T, Moradi A. Leakage assessment methodology. In: Proc. of the 17th Int'l Workshop on Cryptographic Hardware and Embedded Systems. Saint-Malo: Springer, 2015. 495–513. [doi: 10.1007/978-3-662-48324-4_25]

[9] Bhasin S, Danger JL, Guilley S, Najm Z. NICV: Normalized inter-class variance for detection of side-channel leakage. In: Proc. of the 2014 Int'l Symp. on Electromagnetic Compatibility. Tokyo: IEEE, 2014. 310–313.

[10] Durvaux F, Standaert FX. From improved leakage detection to the detection of points of interests in leakage traces. In: Proc. of the 35th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Vienna: Springer, 2016. 240–262. [doi: 10.1007/978-3-662-49890-3_10]

[11] Moradi A, Richter B, Schneider T, Standaert FX. Leakage detection with the x2-test. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2018, 2018(1): 209–237. [doi: 10.13154/tches.v2018.i1.209-237]

[12] Bronchain O, Schneider T, Standaert FX. Multi-tuple leakage detection and the dependent signal issue. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2019, 2019(2): 318–345. [doi: 10.13154/tches.v2019.i2.318-345]

[13] Lu FX. Optimization research of side channel leakage evaluation method based on TVLA [MS. Thesis]. Guangzhou: Guangdong Polytechnic Normal University, 2020 (in Chinese with English abstract). [doi: 10.27729/d.cnki.ggdjs.2020.000236]

[14] Moos T, Wegener F, Moradi A. DL-LA: Deep learning leakage assessment: A modern roadmap for SCA evaluations. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2021, 2021(3): 552–598. [doi: 10.46586/tches.v2021.i3.552-598]

[15] ISO/IEC. ISO/IEC 19790:2012 Information security, cybersecurity and privacy protection—Security requirements for cryptographic modules. Geneva: ISO/IEC, 2025.

[16] ISO/IEC. ISO/IEC 17825:2016 Information technology—Security techniques—Testing methods for the mitigation of non-invasive attack classes against cryptographic modules. Geneva: ISO/IEC, 2024.

[17] State Cryptography Administration. GM/T 0008-2012 Cryptography test criteria for security IC. Beijing: Standards Press of China, 2012 (in Chinese).

[18] State Cryptography Administration. GM/T 0028-2014 Security requirements for cryptographic modules. Beijing: Standards Press of China, 2014 (in Chinese).

[19] State Cryptography Administration. GM/T 0083-2020 Guideline for the mitigation of non-invasive attacks against cryptographic modules. Beijing: Standards Press of China, 2021 (in Chinese).

[20] Yang Z, Tang M, Cheng JH, Zhang Y. Vulnerability analysis of timing protection for branch prediction. Journal of Cryptologic Research, 2021, 8(5): 820–833 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000479]

附中文参考文献

[5] 王安, 葛婧, 商宁, 张帆, 张国双. 侧信道分析实用案例概述. 密码学报, 2018, 5(4): 383–398. [doi: 10.13868/j.cnki.jcr.000249]

[13] 鹿福祥. 基于 TVLA 的侧信道泄露评估方法优化研究 [硕士学位论文]. 广州: 广东技术师范大学, 2020. [doi: 10.27729/d.cnki.ggdjs.2020.000236]

[17] 国家密码管理局. GM/T 0008-2012 安全芯片密码检测准则. 北京: 中国标准出版社, 2012.

[18] 国家密码管理局. GM/T 0028-2014 密码模块安全要求. 北京: 中国标准出版社, 2014.

[19] 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. 北京: 中国标准出版社, 2021.
[20] 杨珍, 唐明, 程金花, 张尧. 时间防护面向分支预测的脆弱性分析. 密码学报, 2021, 8(5): 820–833. [doi: 10.13868/j.cnki.jcr.000479]

作者简介

魏淙洛, 博士, 主要研究领域为侧信道分析, 分组密码分析与设计.
王菁, 硕士生, 主要研究领域为侧信道分析.
王安, 博士, 研究员, 博士生导师, CCF 专业会员, 主要研究领域为侧信道分析, 密码工程.
丁瑶玲, 博士, 副研究员, 博士生导师, 主要研究领域为侧信道分析, 分组密码分析.
孙绍飞, 博士, 副研究员, 主要研究领域为侧信道分析.
祝烈煌, 博士, 教授, 博士生导师, CCF 杰出会员, 主要研究领域为区块链技术, 云计算安全, 大数据隐私保护, 物联网安全.