软件学报 ISSN 1000-9825, CODEN RUXUEW
2026,37(1):442−463 [doi: 10.13328/j.cnki.jos.007454] [CSTR: 32375.14.jos.007454]

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

复杂应用场景下侧信道分析的可移植性研究综述*

李 迪, 张裕鹏, 汤宇锋, 龚 征

(华南师范大学 计算机学院, 广东 广州 510631)

通信作者: 龚征, E-mail: gongzheng@scnu.edu.cn

摘 要: 侧信道分析 (side-channel analysis, SCA) 是一种通过获取软硬件运行时产生的泄露信息来破解密钥的分析技术. 其中, 建模类侧信道分析已被证明是攻击密码系统的一种强有力的手段. 近年来, 随着人工智能技术的发展, 其在建模类侧信道分析中的应用极大丰富了攻击手段, 并显著提升了攻击效率. 在该类方法的建模阶段, 攻击者通过访问克隆设备以收集与目标设备相关的泄露信息, 但在实际场景中, 克隆设备与目标设备之间往往存在差异. 然而, 大部分的研究工作仅考虑使用一种设备进行支持和验证, 这导致所建立的方法依赖于特定环境, 其应用范围有限, 可移植性差. 为了解决该问题, 重点聚焦于复杂应用场景下面临的攻击可移植性问题, 深入探讨在不同参数设置、算法实现、设备差异等多方面所引发的挑战, 并对近年来国际上学者提出的解决方案和分析结果进行系统梳理. 在此基础上, 进一步总结当前侧信道分析可移植性研究中存在的不足, 并展望未来的发展方向.

关键词: 侧信道分析 (SCA); 可移植性; 迁移学习; 深度学习; 物理安全

中图法分类号: TP309

中文引用格式: 李迪,张裕鹏,汤宇锋,龚征. 复杂应用场景下侧信道分析的可移植性研究综述. 软件学报,2026,37(1):442–463. http://www.jos.org.cn/1000-9825/7454.htm

英文引用格式: Li D, Zhang YP, Tang YF, Gong Z. Review of Portability Research on Side-channel Analysis in Complex Application Scenarios. Ruan Jian Xue Bao/Journal of Software, 2026, 37(1): 442–463 (in Chinese). http://www.jos.org.cn/1000-9825/7454.htm

Review of Portability Research on Side-channel Analysis in Complex Application Scenarios

LI Di, ZHANG Yu-Peng, TANG Yu-Feng, GONG Zheng

(School of Computer Science, South China Normal University, Guangzhou 510631, China)

Abstract: Side-channel analysis (SCA) is a technique that extracts leaked information generated during hardware or software execution to compromise cryptographic keys. Among various approaches, profiling side-channel analysis has been proven to be a powerful method for attacking cryptographic systems. In recent years, the integration of artificial intelligence technology into profiling side-channel analysis has significantly enriched attack strategies and improved efficiency. During the profiling phase, leakage information related to the target device is typically collected by accessing a cloned device. However, practical scenarios often involve discrepancies between the cloned and target devices. Most existing studies rely on a single device for training and validation, resulting in methods that are highly environment-dependent, with limited applicability and poor portability. This study focuses on the portability challenges encountered in complex application scenarios. Challenges arising from variations in parameter settings, algorithm implementations, and hardware differences are analyzed in detail. Solutions and analysis results proposed in recent years are systematically reviewed. Based on this survey, current limitations in portability research on side-channel analysis are summarized, and potential future directions are discussed.

Key words: side-channel analysis (SCA); portability; transfer learning; deep learning; physical security

1 引 言

基于高性能服务器或轻量级微处理器, 各种信息系统与应用在互联网时代得到了飞速的发展. 与此同时, 人们

* 基金项目: 国家自然科学基金 (U2336209); 广东省科技计划 (2022A1515140090)
收稿时间: 2024-03-18; 修改时间: 2024-11-19; 采用时间: 2025-04-19; jos 在线出版时间: 2025-09-10
CNKI 网络首发时间: 2025-09-11

对于网络信息安全与用户隐私保护也更为重视. 密码算法作为搭建安全与信任协议的基础, 也在各个系统与应用中得到了广泛应用. 这些密码算法在设计阶段会通过一系列安全性分析, 以确保其在数学上证明是安全的. 在过去, 密码设备的安全主要取决于密码算法的数学设计, 密码算法的设计是否存在漏洞或缺陷是判断设备是否安全的关键. 实际上, 加密设备在运行过程中与外界环境存在物理交互, 这些物理泄露往往与密码设备的中间状态值存在相关性. 因此, 攻击者可以借助这些信息获取密钥. 1996 年, Kocher[1]首次利用密码设备运行过程中泄露的时间信息对密钥进行破译. 这项研究颠覆了人们对信息安全的认知, 借助泄露物理信息分析密钥的方法也被统称为侧信道分析 (side-channel analysis, SCA)[2]. 后续研究表明, 大多数密码算法难以抵御 SCA 攻击, 这一现象引发了广泛关注, 因此成为近年来密码学领域的研究热点.

根据不同类别的泄露信息, SCA 可分为计时攻击[3]、功耗攻击[4]、电磁攻击[5], 以及故障攻击[6]. 其中功耗攻击、电磁攻击, 因其在现实中容易实现且泄露信息采取方便而受到了广泛的关注. 根据是否需要建模设备可将 SCA 划分为建模类 SCA 与非建模类 SCA. 所谓建模设备是指攻击者事先拥有的一个与攻击目标设备完全相同的且具有完全控制权的设备. 在非建模类 SCA 中, 攻击者直接截取目标设备在加密过程产生的功耗信息, 利用功耗与中间状态操作之间存在的相关性, 通过统计分析方法破译密钥. 该类攻击主要包括简单功耗分析 (simple power analysis, SPA)[7]、差分功耗攻击 (differential power analysis, DPA)[8]和相关系数能量分析 (correlation power analysis, CPA)[9]等. 传统非建模 SCA 的主要缺点是容易受噪声和数据不足的影响, 可能导致错误猜测占据概率分布的峰值, 这一现象也称为假峰现象[10].

相较于非建模类 SCA, 建模类 SCA 的攻击表现更为强大, 一旦模型构建成功, 则具有极高的攻击效率与正确率. 建模类 SCA 的基本假设是攻击者拥有一个用于建模的设备. 在建模阶段, 攻击者收集该设备在加密过程中产生的功耗与明文信息, 并根据设备的泄露特征构造概率分布模型. 在攻击阶段, 使用该模型进行模版匹配来破解密钥. 它主要包括模板攻击 (template attack, TA)[11]和随机模型攻击 (stochastic attack, SA)[12]. TA 是最受研究者关注的一种方法, 它假设所有设备的侧信道信息都服从多维高斯分布, 而实际上许多加密设备的侧信道信息不一定能被表示为多维高斯分布, 这使得该类分析攻击很难对此类加密设备造成威胁[13].

在 2011 年, 研究者正式明确研究基于人工智能的 SCA, 这些技术可视为建模类 SCA 的一种扩展[14]. 人工智能技术能够自动从数据中学习特征, 并能概括数据的表示, 且不需要目标设备功耗分布满足多维高斯分布, 这些属性让其在 SCA 领域中大放异彩. 从实验部署来看, 建模类 SCA 中的建模和攻击阶段几乎等同于人工智能技术中的训练和测试步骤. 因此, 求解密钥问题很自然地转化为人工智能技术中的分类问题. 研究人员首先从机器学习技术开始引入, 如随机森林 (random forest, RF)[15]、支持向量机 (support vector machine, SVM)[16]和自组织映射 (self-organizing map, SOM)[17]. 实验结果表明基于机器学习的侧信道分析 (machine learning-based side channel analysis, ML-SCA) 非常强大, 特别是在训练样本有限的情况下, 但是该方法无法做到自动化特征提取, 依赖于精准的特征工程. 在 SPACE 2016 上, 深度学习技术被正式引入 SCA 领域, Maghrebi 等人[18]对比了各类建模类 SCA 方法, 并分别对无防护以及带掩码防护数据集进行了攻击测试. 实验证明了与传统 SCA 方法相比, 基于深度学习的侧信道分析 (deep learning-based side channel analysis, DL-SCA) 是一种更强大的攻击方式, 它在各个场景的攻击性能上有着显著优势. 在诸多深度学习方法中最著名的方法是多层感知器 (multi-layer perceptron, MLP)[19]和卷积神经网络 (convolutional neural network, CNN)[20], 其中基于 CNN 的方法显现出强大攻击性能, 因为它在原始轨迹中提取相关特征方面有着出色的表现[21]. 因此, 大量文献探索了适合 SCA 的 CNN 模型结构[22,23]. 在 2024 年, Transformer[24]和生成对抗网络[25]也被引入 SCA 领域中应用, 它们分别在处理时钟抖动[26]对策和特征提取方面有着显著优势. 总体而言, 相较于传统的 SCA, 深度学习方法主要有 3 大优势: 一是不需要关注泄露区间[27], 二是不需要手动对齐波形[28], 三是可对带掩码的防护设备进行攻击[29]. 表 1 总结了 SCA 的发展历程.

目前, 大多数建模类 SCA 只进行了理论上的验证攻击, 即假定建模设备和目标设备是完全一致的[30]. 然而, 在现实场景下几乎不可能确保建模与目标设备是完全一致的. 由于实验设置和现实场景之间的差距, 攻击的性能和实用价值被高估. 可移植性问题的出现是源于建模设备与目标设备之间因采集设置、算法实现、芯片参数等外部

因素而导致的分布差异, 其原理详见图 1. 当实际的目标设备与建模设备差异过大时, 会导致攻击性能直线下降, 甚至完全失效.

表 1 侧信道分析发展历程

分类	方法	首次提出	特点	不足
非建模类SCA	SPA、DPA、CPA	会议CRYPTO 1996	实现成本低	易受噪声和数据不足影响
建模类SCA	TA、SA	会议CHES 2004	一旦建模成功, 有着极高正确率	分析对象需要满足多维高斯分布
	ML-SCA (RF、SVM)	期刊JCE 2011	分析对象无需满足多维高斯分布	依赖于精准的特征工程
	DL-SCA (MLP、CNN)	会议SPACE 2016	无需对轨迹预处理, 且可攻击掩码防护对策	数据依赖性强

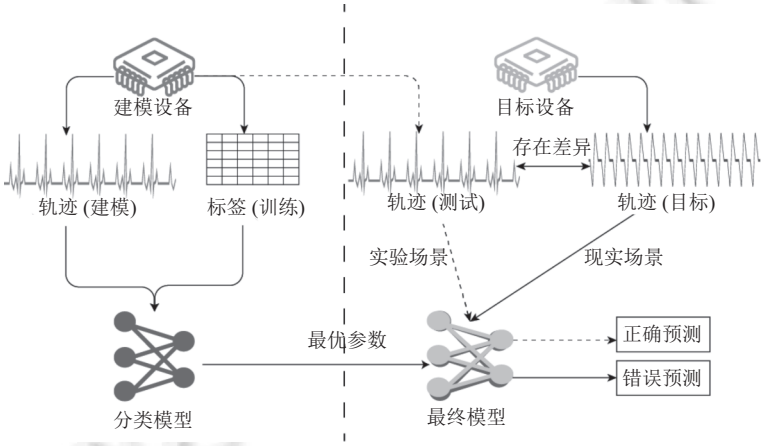

图 1 可移植性问题示意图

攻击的可移植性问题早在 Eurocrypt 2011 会议上就引起了研究者的关注, Renauld 等人[31]对 20 个不同的设备进行 TA 的可移植性测试, 研究结果表示当建模设备与目标设备的芯片存在差异时, 攻击将完全失效. 除一系列在加密芯片上的可移植性研究[32–34]以外, Kim 等人[35]还对无线键盘中的 AES 加密执行了 TA. 该研究表明, 即便在同一键盘上进行分析和测试的 TA 成功率能达到 100%, 但在不同键盘上的成功率仅为 28%. 这些报告都表明了建模与目标设备之间细微的差异都会导致 TA 的攻击性能受到严重影响.

由于深度学习技术在 SCA 领域表现出惊人的潜力, 研究者开始关注其在可移植性方面的表现. 深度学习技术的一个隐式假设为训练和测试数据是独立且具有相同分布的[36]. 当建模设备与分析设备存在差异时, 其数据分布很难具有相同分布, 导致训练出一个过度专业化 (over-specialization) 的神经网络[37]. 它学习的最终结果导致模型只针对一个特定的数据集有效, 而不能推广到其他数据集. 在 DAC 2019 会议上, Das 等人[38]指出当密钥和设备发生变化时轨迹样本之间的均值差会发生改变. 因此, 针对特定分析设备进行训练的模型将不能很好地推广到其他设备. 在 CHES 2019 会议上, Carbone 等人[39]使用深度学习对 RSA 的安全实现进行评估, 其中训练、验证和测试数据来自 3 种不同的智能卡. 实验结果表明, 深度学习技术强烈地依赖于设备、目标算法和采样设置. 即使重用原攻击方案的设计原则, 它们也不能直接应用于新的攻击场景. 在 CHES 2020 会议上, Wouters 等人[40]使用 MLP 技术对车辆固定器系统中的 DST80 密码进行分析. 实验结果表明, 在面对型号不同的设备时, 使用单设备训练的 MLP 模型将完全失效. 综上所述, 深度学习技术也同样面临可移植困难问题.

可移植性是各类攻击走向应用的必备前提, 为了弥补设备差异对攻击性能的影响, 构建更通用的攻击方法, 攻击的移植性研究被作为一个重要的研究方向. 然而, 已有的侧信道分析综述也各有侧重, 缺乏对可移植性研究的全面梳理与分析. 王安等人[41]总结了侧信道分析实用案例概述的研究进展, 其侧重点在于对非建模类 SCA 的分析. 吴伟彬等人[42]侧重于介绍后量子密码算法中的侧信道攻击与防御研究进展. 王永娟等人[43]对侧信道攻击与防御技术进行了综合性的总结, 但其工作重点在于对传统方法的分析, 缺乏对最新的深度学习技术的深入探讨. Picek

等人[44]对 DL-SCA 进行了总结与分析, 但未对可移植场景进行详细分析. 为弥补这部分内容的空白, 本文按照图 2 的结构框架, 系统梳理了在复杂应用场景下侧信道分析的可移植性研究进展, 它包括传统方法与深度学习方法的全面总结.

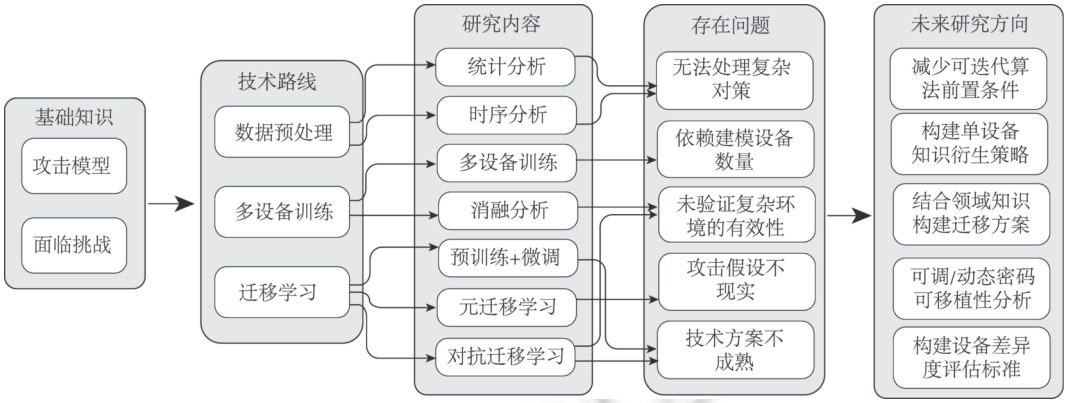

图 2　整体架构示意图

本文第 2 节对目前 SCA 面临的可移植性问题与挑战进行详细阐述与分析. 第 3–5 节分别从数据预处理、多设备训练以及迁移学习这 3 类技术角度介绍可移植性方案的基本原理、应用场景以及发展现状. 第 6 节对全文进行总结, 并对前沿技术进行展望.

2　可移植攻击模型与面临的挑战

2.1　可移植性攻击模型

可移植性攻击模型是模拟实际攻击情况的一种模型, 在该模型中假设攻击者拥有两个设备, 一个设备用于建模, 另一个用于执行目标攻击. 其中, 建模设备与目标设备是相似型号的芯片, 但在功耗分布上存在一定差异性. 攻击者能够访问来自建模设备中轨迹、密钥、明文等任意信息. 但对于目标设备, 攻击者只能执行加密操作获取相应的轨迹. 除此之外, 加密过程中的芯片差异、实现细节、密钥信息、采样设置等其他细节对于攻击者来说都是黑盒, 详情可见图 3. 这些差异对攻击者建立可移植性攻击模型具有相当大的挑战, 即便是细微的差异都会对模型性能造成致命影响. 因此, 如何验证和构造可移植性攻击成为研究的两大难点.

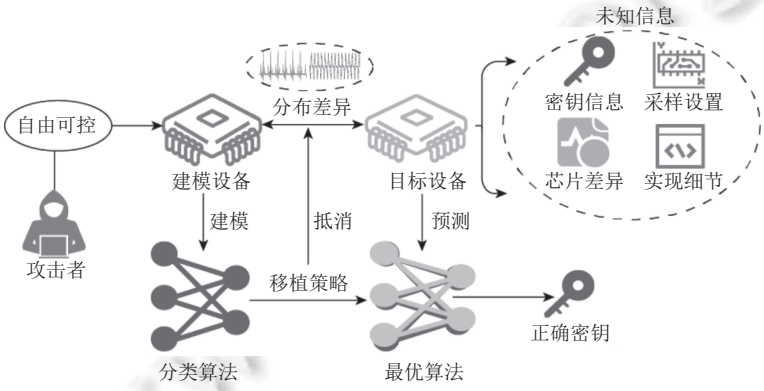

图 3　可移植性攻击模型

在验证可移植性方面, 攻击者必须确保所构建的分类算法具有高泛化性, 能够适用各类差异性场景. Bhasin 等人[45]建议在算法构建过程中至少需要 3 种设备对构建的模型进行验证, 其中一个用于训练, 一个用于验证, 另一

个用于执行实际攻击. 因为在建模设备上的轨迹进行验证, 无法考验算法适应差异化场景的能力, 即便在建模数据上拥有较强的攻击性能, 也不能代表其在目标设备上能够表现良好. 在构造可移植性方案方面, 研究者们需要根据差异化内容的具体表现, 构造相应方案抵消差异. 这其中涵盖了数据预处理、训练策略、迁移学习等一系列技术, 合理搭配使用这些方法, 是构建可移植性攻击的关键, 在后续章节本文将详细介绍这些技术.

2.2 在相同设备环境下面临的挑战

本节探讨了可移植性攻击在相同设备环境下所面临的挑战. 所谓“相同设备”, 指的是建模设备与目标设备是同类的芯片, 其所有的设计和生产参数都是相同的. 根据现有文献研究, 我们对这些场景细分为“相同设备、不同设置”“相同设备、不同副本”“相同设备、不同实现”, 并对这些场景中所带来的挑战进行了详细的分析.

1) 相同设备、不同设置

在“相同设备、不同设置”的情况下, 建模和目标设备的加密芯片是完全一致的, 甚至是使用同一块芯片进行实验, 但其内部存在密钥参数、采集参数等设置的多样性. 这种差异可能导致攻击的不稳定性, 使得在不同参数设置下的可移植性受到挑战. 现有研究显示, 即使是在同一块芯片上进行建模与分析, 当密钥发生改变时, 轨迹采样点的绝对均值差会出现差异[45]. 当建模和目标设备的采样设置不同时, 会出现垂直振幅和时间采样点不同步的情况, 这些情况都对攻击可移植性造成影响[32].

2) 相同设备、不同副本

在“相同设备、不同副本”的情况下, 建模和目标设备是同一芯片上两个不同物理副本. 通常, 这两个副本是从同一批产品中购买, 有着相同的电路设计, 但芯片之间存在微小的差异. 这些差异可能由于芯片定制来自不同的印刷电路板 (printed circuit board, PCB)[46], 在芯片制造和包装过程中引入了随机过程[47–49], 或者在 CMOS 技术中采用了不同纳米工艺[33]. 该场景在实际攻击中很常见, 因而受到研究者的热点关注. 现有研究显示, 即便是在一些简单的可编程集成电路, 不同副本之间的差异仍然会显著增加可移植攻击的错误率[34]. 此外, 副本之间的内部差异将会导致轨迹中直流偏移、信噪比、绝对均值差发生改变.

3) 相同设备、不同实现

在“相同设备、不同实现”的情况下, 建模和目标设备是同一芯片上两个不同物理副本, 除芯片以外更大的差异源自于内置算法的实现方式以及芯片内部的防御对策. 其中, 建模设备和目标设备使用的是同一种加密算法, 但目标设备的算法可能采用了不同的加密模式 (比如 ECB、CBC、CFB 等)[50], 芯片内部可能带了噪声[47,51–53]、时钟抖动[47,51,52,54]、掩码[55,56]等防护对策. 甚至, 该算法是其可调分组密码 (tweakable cipher)[57]的一种变种形式, 或者其内部组件、结构是动态可变的[58]. 在这些场景中, 加密模式之间的实现差异、时钟抖动策略会导致采样轨迹不同步, 而噪声策略会影响轨迹的信噪比. 掩码对策的情况则更为复杂, 整体轨迹泄露分布都会发生改变, 并且不会暴露一阶泄露. 此外, 可调分组密码, 以及组件、结构动态的分组密码会导致一个更复杂的攻击场景, 它们在实现细节上的差异会如何影响轨迹分布还需要进一步的探讨. 在实际情况中, 这些对策的组合会严重影响攻击的可移植性, 对构建的可移植方案的要求更高.

2.3 在不同设备环境下面临的挑战

本节探讨了可移植性攻击在不同设备环境下所面临的挑战. 所谓“不同设备”, 指的是建模设备与目标设备的芯片在结构、型号以及指令集架构存在差异. 该场景是最困难的场景, 目前仅文献 [46,59] 对其进行研究. 其中, 这些场景又可细分为“同质设备”“异构设备”. 下面, 本文对这些场景所带来的挑战进行详细分析.

1) 同质设备

在“同质设备”的情况下, 建模设备和目标设备虽然来自同一制造商, 但芯片之间存在一定的差异. 这些差异可能体现在芯片型号、架构设计、时钟频率等方面. 而在采样轨迹上则体现在泄露位置和采样点的信噪比之间的变化. 攻击者需要制定特定的特征提取和建模方法, 以适应同质设备之间差异带来的挑战.

2) 异构设备

在“异构设备”的情况下, 建模设备和目标设备是完全不相同的两类芯片, 它们来自不同的制造商, 并且在电路模版、指令集架构 (instruction set architecture, ISA)、功率耗散等方面各不相同. 这种异构性使得构建可移植性方

案更加困难, 因为不同设备之间轨迹的泄露区间和采样点的信噪比的差异过大. 攻击者需要深入了解目标设备的硬件特征, 分析与建模设备之间的异同点, 通过一系列复杂的泄露分析、预处理策略找到并提取共性部分. 此外, 异构设备的广泛应用要求研究者考虑不同制造商芯片之间可能存在的标准化差异, 以应对不同场景.

2.4 用于可移植性分析的公开数据集

公开数据集有利于促进研究领域的发展, 它能够为研究者提供一个公平、统一的对比基准. 用于评估可移植性攻击场景下通常需要提供多组数据集, 以便于体现差异对比. 下面, 本节将介绍现有公开的可移植性分析的数据集, 并详细阐述构建可移植性数据集的常见策略, 以便于研究者能够更好研究这类场景.

1) ASCAD 数据集[21]

该数据集常用于评估 DL-SCA 模型的攻击性能, 它包含在时钟频率为 4 MHz 的 ATMega 8518 目标板上 AES 掩码实现的功耗轨迹. 其内部提供了密钥固定版本与密钥随机版本的数据集, 这两个数据集分别命名为 ASCAD^f 和 ASCAD^r. 每个版本中的数据集提供了软件模拟的时钟抖动版本. 即数据集根据偏移参数对轨迹在 x 轴上移动进行样本抖动, 这些偏移参数分别为 0、50 和 100. 因此, 该数据集常用于分析不同时钟抖动对策参数之间的可移植性场景. 为了便于描述, 本文按照密钥状态和偏移参数进行命名, 例如密钥固定版本且偏移参数为 50 的数据集命名为 ASCAD$^f_{desy50}$. 该数据集可通过以下链接获取: https://github.com/ANSSI-FR/ASCAD.

2) CHES CTF 2018 数据集[60]

该数据集是 CHES CTF 2018 竞赛中发布的公开数据集, 包含 4 组基于掩码实现的 AES 加密功耗轨迹. 每组数据由 10 000 条轨迹组成, 分别采集自 4 个不同的 STM32 硬件平台, 每个平台均提供独立的功耗轨迹. 该数据集可用于评估“相同设备、不同副本”场景下的可移植攻击性能. 该数据集可通过以下链接获取: https://www.dropbox.-com/s/lpw1k3so99krmmq/ches_ctf.h5?dl=0.

3) CPDA 数据集[47]

该数据集主要是测试跨设备建模类攻击 (cross-device-profiled-attack, CDPA) 在设备、采样设置、实现差异因素上的可移植性表现, 所以本文将其命名为 CDPA 数据集, 它的具体参数如下.

● 不同设备: 该数据集包含在 XMEGA 和 SAKURA 两类目标板上运行 AES-128 加密时采集的功耗轨迹. 其中 XMEGA 采用 C 语言实现的软件算法, 通过在微控制器与接地之间插入电阻测量功耗, 采样率为 125 MS/s (mega samples per second, 即每秒百万采样点数). SAKURA 中算法为硬件实现, 通过监测 FPGA 核心电压获取功耗轨迹, 采样率为 500 MS/s.

● 不同采样设置: 提供了在 XMEGA 目标板上运行 AES-128 加密时使用 Langer LF-U5 近场探针采集的电磁轨迹, 采样使用 Teledyne LeCroy Waverunner 610zi 示波器完成, 采样率为 250 MS/s. 每次探针位置尽量保持一致, 但可能存在人为误差.

● 不同实现差异: 通过向原始 ASCAD 数据集添加人工对策/噪声来模拟不同的实现方式, 添加的对策/噪声包括高斯噪声、去同步化、时钟抖动.

该数据集可通过以下链接获取: https://github.com/CDPA-SCA/Cross-Device-Profiled-Attack/tree/main.

4) SoftPower 数据集[61]

该数据集基于 ChipWhisperer 平台采集, 包含在 XMEGA (8 位 RISC) 和 ARM STM32 (32 位 Cortex-M4) 两种微控制器上运行 AES-128 加密时的功耗轨迹. 数据集设置了随机延迟、指令重写、优化级别和代码混淆这 4 种差异因素, 为分析软件实现差异的可移植性提供了重要支持. 其中随机延迟策略是通过随机移动功耗轨迹的样本来模拟. 指令重写策略是在汇编代码级别进行修改, 并通过逆向工程工具 Ghidra 对 ELF 文件进行调整. 而优化级别差异是基于交叉编译器分别设置 Os、O1、O2 和 O3 这 4 种优化级别生成. 代码混淆策略则借助 Tigress 工具实现 3 种不同的混淆方案. 该数据集为分析不同软件实现间的差异对功耗轨迹的影响提供了丰富的实验基础. 该数据集可通过以下链接获取: https://github.com/UCdasec/SoftPower.

5) AES_PTv2 数据集[55]

该数据集包含 3 个不同的 AES 软件实现: 未加保护的 AES-128 (ECB 模式)、基于弱掩码方案的 AES-128 和

强掩码方案的 AES-128. 数据采集自 5 块嵌入式设备, 其中 4 块是 STM32F411VE 开发板, 另一块是 Piñata 开发板. STM32F411VE 的采样频率为 1 GHz, 轨迹噪声较大. 而 Piñata 的采样精度更高. 弱掩码方案在 SBox 操作后移除掩码, 易泄露掩码信息. 而强掩码方案在 ShiftRows 后移除掩码, 提升了安全性. 该数据集可用于评估“相同设备、不同副本”“相同设备、不同实现”“不同设备”场景下的可移植攻击性能. 该数据集可通过以下链接获取: https://github.com/urioja/AESPT.

以上列出了所有可用于可移植性分析的公开数据集. 尽管大多数研究尚未公开其实验所使用的数据集, 但许多研究基于 ChipWhisperer 平台提供的工具和套件采集现有数据, 研究者可参考目标论文所提供的实验参数对齐实验设置. 此类研究不建议使用仿真轨迹进行验证, 因为仿真轨迹无法有效反映现实中硬件差异对可移植性的影响, 大幅降低研究的可信度. 而基于真实轨迹添加相应的人工对策或噪声来模拟不同实现是一种公认的有效方法, 对于这方面本文推荐采用 ASCAD 数据集所提供的模拟噪声和抖动对策的方法.

2.5 可移植性场景及其影响因素分析

表 2 列举了目前文献中所有可能影响攻击可移植性的因素, 其中包括设备参数、算法实现、硬件异质性、制造商特定的防护策略等多方面因素. 此外, 本文提出了对可调/动态分组密码算法的可移植性场景. 这些因素构成了攻击可移植性的多维度难题. 在实际应用中这些因素的相互交织和组合将使攻击者面临更为复杂的环境. 这些场景严重限制了攻击方案的实用性和应用场景, 如何对不同差异场景建立精准、高效的可移植方案是需要持续探索的方向.

表 2 不同场景下所出现的可移植性挑战

实验设置	目标设备存在的差异	轨迹采样点是否发生以下情况的变化					是否需要可移植方案	参考文献
		均值差	不同步	垂直振幅	直流偏移	信噪比		
相同设备、不同设置	轨迹采样设置不统一	√	√	√	√	×	√	[32]
	密钥设置不同	√	×	×	×	×	×	[45]
相同设备、不同副本	制造和包装过程中引入的随机过程	√	√	—	√	√	√	[46–49]
	不同的CMOS技术	√	√	—	—	√	√	[33]
	不同的印刷电路板	√	×	—	—	√	√	[46]
相同设备、不同实现	不同加密模式	√	√	—	—	×	√	[50]
	不同防护对策 (噪声)	√	×	—	—	√	√	[47,51–53]
	不同防护对策 (时钟抖动)	√	√	—	—	√	√	[47,51,52,54]
	不同防护对策 (掩码)	√	√	—	—	√	√	[55,56]
	可调密钥 (Tweak)	√	—	—	—	×	—	本文
	算法的组件、结构动态可变	√	√	—	—	√	—	本文
不同设备	芯片型号和结构不同	√	√	—	—	√	√	[46,59]
	芯片型号、指令集架构不同	√	√	—	—	√	√	[46,59]

注: 符号“√”代表“是”, “×”代表“否”, “—”代表未进行实验验证

3 基于数据预处理的可移植性方案

数据预处理是指在进行数据分析任务之前, 对原始数据进行清理、转换和整理的过程. 该过程涵盖了去噪、降维以及归一化等多种操作. 通过这些操作, 攻击者能够消除数据中的噪声、减少数据的维度, 并将数据转化为更适合进行进一步分析的形式.

在传统的侧信道攻击中, 预处理技术发挥着重要作用[62]. 一方面, 消除原始数据中的噪声, 能够提高攻击的准确性和可靠性. 另一方面, 数据降维操作有助于减少分析的复杂度和计算量, 提高攻击的效率. 在攻击的可移植性方面, 预处理技术还有助于使模型更好地适应不同设备中的功耗数据. 通过提取特征操作, 它有效地减少了不同设备之间数据分布差异, 使得分类算法更容易适应不同分布的功耗数据. 总体而言, 数据集预处理技术在侧信道攻击中扮演着关键角色, 其整体方案如图 4 所示.

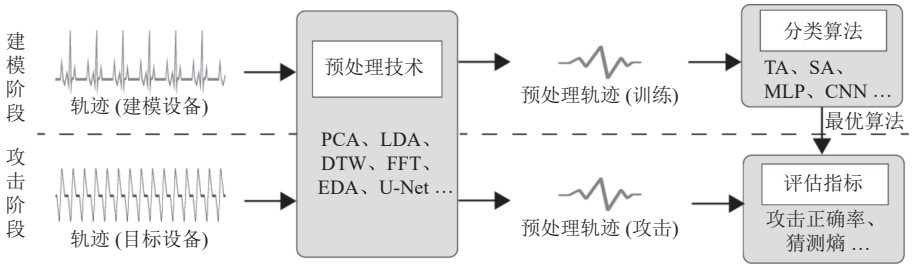

图 4 基于预处理的可移植性攻击方案

3.1 基于统计分析的方法

基于统计方法的数据预处理方法是使用统计学原理和技术来处理数据, 以便更好地适应建模和分析. 这些方法旨在利用数据的统计性质、分布和关系, 以提高数据的质量、减少噪声和无关特征. 在此类方法中, 根据算法能否自动迭代更新参数又可细分为可迭代算法和不可迭代算法.

1) 不可迭代算法

统计分析中两种常见的不可迭代方法是主成分分析 (principal component analysis, PCA)[63]和线性判别分析 (linear discriminant analysis, LDA)[64]. 其中 PCA 是一种无监督降维技术, 用于将高维数据转换为低维表示, 同时保留尽可能多的信息. 其目标是通过找到数据中的主要变化方向. 而 LDA 是一种监督降维技术, 主要用于在分类问题中提取最具判别性的特征. 其目标是通过最大化类别间的离散度和最小化类别内的散度矩阵之间比值来实现最佳的特征投影. 与 PCA 不同, LDA 考虑到了类别标签信息, 以便在降维的同时保留最大的类别间差异. 这两种方法经常在模式识别和人脸识别等领域中广泛应用, 其特点同样也适用于功耗轨迹的预处理. 因此, 一系列学者展开了 PCA、LDA 在模型可移植性方向的研究.

2012 年, Elaabid 等人[32]提出了使用 PCA 技术预处理功耗轨迹. 实验结果表明, 当目标设备的采集设置发生变化时, 产生的垂直振幅差异会导致 TA 失效, 而使用 PCA 预处理技术可以消除这部分差异. 但在该方案中只考虑 PCA 方法, 并且没有详细探讨 PCA 具体参数的选择和作用. 在 COSADE 2014 会议上, Choudary 等人[48]详细探讨了 PCA 和 LDA 的参数选择和适用场景. 他们采用 XMEGA[65]微控制器的 4 个不同副本进行实验, 其工作主要考虑温度变化引起的直流偏移对攻击性能的影响. 实验结果表明, 选择良好参数的 LDA 或 PCA 能最大化 TA 的性能, 其中 LDA 能够补偿由合并协方差矩阵捕获的温度变化, 并且这种温度变化在不同的设备中的活动是相似的. 他们表明使用 LDA 时应该忽略特征向量中最强的直流贡献, 而 PCA 应该选择足够数量的特征向量, 其中至少包括一个最强的直流贡献. 2018 年, Choudary 等人[49]继续完善对 TA 中 PCA 和 LDA 的工作. 他们对信噪比、平均差以及绝对平均差等多种样本选择方法进行讨论, 并额外添加了 AES 硬件实现的实验验证. 实验结果证明了 PCA 和 LDA 在硬件实现下同样适用, 并给出参数选择细节. 2021 年, Danial 等人[66]进一步讨论了在低信噪比环境下 PCA、LDA 等预处理方法对神经网络的训练帮助. 实验环境中功耗采集轨迹的信噪比为 19.6 dB, 而电磁采集轨迹的信噪比仅为 3.1 dB. 因此, 作者声明相较于功耗轨迹, 电磁轨迹的训练难度更大, 即便是使用同一设备下收集的电磁轨迹进行训练, 也会导致攻击失效. 在实验中, 他们对电磁轨迹进行均值化处理来提高信噪比, 并采用 PCA、LDA 方法对波形进行预处理并加入训练. 结果表明, 对于高维功耗数据, LDA 是最有效的预处理方法, 在跨设备攻击中其单字节正确率可达到 91.5%. 此外, 2021 年, Won 等人[67]总结了移动平均数、相位相关算法、PCA、弹性对齐等预处理方法在促进分类模型学习方面的积极效果, 并推广到不同的公开数据集上, 但尚未有人系统讨论这一类技术在可移植性攻击中的作用.

通过对现有文献分析可以得出, PCA、LDA 两种方法在处理“同一设备, 不同副本”场景有着良好的实用性, 其中 LDA 在各个环境的预处理效果更好. 在 Choudary 等人[48]的研究中表明, 在处理直流偏移时, LDA 效果更好. 同时 Danial 等人[66]的研究也表明, 在低信噪比环境下, LDA 在处理高维数据方面也有着更好的效果. 然而, LDA 是监督学习算法, 它的运算过程需要标签信息, 而在现实场景中攻击者很难获得目标设备的标签信息. 同时 LDA 的

计算过程中需要对一个高维度的协方差矩阵进行求逆, 设单类轨迹样本数为 N, 每个轨迹的采样点为 d, 为了确保协方差矩阵不为奇异矩阵, 至少满足 $N>d$ 的条件. 而 PCA 不需对协方差矩阵进行求逆, 因此, 在目标设备难以获取轨迹信息的情况下, PCA 是更好的选择.

2) 可迭代算法

除了 PCA、LDA 这些不可迭代算法, 自 2020 年起, 研究者开始向一些更复杂、可变性更强的可迭代算法展开研究, 这些算法能够适应更复杂的场景. 可迭代算法的优势在于在迭代更新的过程中, 算法能够根据目标优化函数自适应地调整参数, 以获得更优的结果. 下面, 本文将详细介绍这类技术的研究进展.

Wu 等人[51]利用自动编码器 (autoencoder, AE) 模型来消除功耗轨迹中的噪声. 他们主要考虑了一个白盒攻击场景, 即攻击者对目标设备有完全的控制. 因此, 在实验中他们可以关闭防护对策, 并从这些设备中获得无噪声的轨迹. 但这种假设在现实场景中很难满足. 此外, 他们构建的 AE 模型, 只能在相同的电路架构的设备上进行降噪实验, 该方法在跨设备上的有效性还需要更多实验的评估. 2021 年, Rioja 等人[55]使用分布估计算法 (estimation of distribution algorithm, EDA) 执行兴趣点选择、建模以及密钥恢复步骤. 该方法避免了手动执行各种类型的泄露分析、特征提取等繁琐步骤, 实现了自动化攻击. 实验中对 STM32F4[68]开发板的 4 个副本进行分析, 其中他们考虑了更困难的场景, 在每个副本上对 AES 算法添加了掩码对策. 对比实验的结果显示, PCA 无法处理带有掩码对策的功耗轨迹, 而 EDA 在经历多次迭代后获取的最优兴趣点能够帮助 TA 获取正确密钥. 2023 年, Yu 等人[52]利用 U-Net 模型对轨迹进行预处理, 实现跨设备降噪. 他们从建模设备收集的低噪声轨迹来对 U-Net 预训练. 然后, 使用目标设备中的噪声轨迹来微调 DL 模型, 其中在微调阶段中他们使用了 L2 正则化技术. 最后将去噪的轨迹用于构建攻击模型. 实验结果表明该方法能够有效针对高斯噪声[69]、随机延迟[70]、时钟抖动和洗牌 (dummy)[71]对策, 利用去噪轨迹进行训练的分类模型可以减少恢复密钥的轨迹数和计算成本. 但是该方法需要攻击者知道目标设备所采用的对策方案, 并且能够控制建模设备中各对策的开关, 这在实现上需要一定成本.

相较于不可迭代算法, 可迭代算法能够面向更困难的场景, 例如 EDA 能够实现对带有掩码防护对策的场景进行可移植性攻击. 而 U-Net 能够对高斯延迟、随机延迟、时钟抖动和洗牌等对策的场景进行可移植性攻击. 但是, 技术复杂性的增加必然涉及时间和 CPU 资源的增加, 攻击者应该在面对不同场景合理地选择预处理技术. 此外, U-Net 和 AE 的方法对场景也有一定限制, 需要攻击者能够获取开启与关闭对策的轨迹用于训练, 这一前置条件使得它在实际应用中受到限制, 表 3 给出了基于统计分析方法的详细对比.

表 3 基于统计分析方法的详细对比

方法	应用场景	特点	局限性
PCA[32,48,49,66]	不同副本, 不同设置	能适用于轨迹采样受限的场景	无法处理带掩码、抖动防护的场景
LDA[48,49,66]	不同副本	利用类别信息进行降维, 适用于高维数据处理	各类轨迹的数目必须大于其维度, 且需要标签信息
EDA[55]	不同副本 (掩码防护)	能够有效处理带掩码防护对策	计算复杂度成本高
AE[51]	不同实现 (噪声、抖动)	非线性降维, 能够有效处理抖动防护对策	需要攻击者可控制对策开关
U-Net[52]	不同实现 (多类对策)	端到端学习, 能够处理多类对策组合的场景	需要攻击者可控制对策开关且能获取目标轨迹的标签

注: 多类对策指的是随机延迟、时钟抖动和洗牌这3种防护对策的组合场景

3.2 基于时序分析的方法

时序分析方法是一种用于处理时序信号的技术和方法集合, 其目标是揭示信号中的模式、趋势、周期性或其他关键特征, 以便更好地理解数据、进行预测或做出决策. 两种常用的时序分析方法为动态时间规划 (dynamic time warping, DTW)[72]和快速傅里叶变化 (fast Fourier transform, FFT)[73]. 其中 DTW 是一种用于比较两个时间序列之间的相似度的方法. 它可以解决在时间轴上有不同速度或长度变化情况下的序列匹配问题. 通过动态规划的方式计算两个序列之间的最佳匹配路径, 从而确定它们的相似度. FFT 通过将时域信号转换为频域信号, 可以提取

出频率分量的信息. 因此, 它被广泛应用于频谱分析、信号滤波和振动分析等方面. 而功耗、电磁轨迹都是一种时序信号, 这类方法在提取不同设备之间的共性部分有着独特优势.

2019 年, Golder 等人[74]将 DTW 用于深度学习技术中, 他们构造了一种 DTW 技术预处理功耗轨迹的方法. 该方法能够很好地克服由于触发故障、频率缩放、随机插入虚拟操作等对策导致的功率轨迹之间的错位. Rioja 等人[75]的工作中提出将 DTW 技术作为量化不同副本之间差异性的评估工具, 并证明该指标与攻击性能直接相关. 他们发现借助 DTW 技术能够选择出不同副本之间最相似的部分, 将该部分用于执行 TA 能够显著提高攻击性能. 此外, Zhang 等人[46]指出之前的可移植性研究的工作都在“相同设备”的场景下进行的, 他们进一步在同质与异构设备上进行可移植性分析. 在实验中, 该方案采用 FFT 对不同设备的轨迹进行预处理, 通过选择幅度最高的频率分量, 以及排除点指数为 0 的直流偏移量作为频率的表征, 这样能够提取不同设备之间的共性特征. 随后将选取的特征加入神经网络中训练, 实现在同质与异构设备的可移植性攻击.

与基于统计分析的预处理方法不同, 时序分析方法主要用于处理非对齐轨迹. Golder 等人[74]的研究表明使用 DTW 能够对轨迹进行对齐, 而在降维和降噪方面则更倾向于使用 PCA 进行处理. 其次, DTW 本身是一种比较两个时间序列之间相似度的方法, 因此它可用于设备差异性评估, 并选取设备轨迹之间最相关的部分[75]. 而 FFT 方法能够将轨迹转换到频域上进行分析, 并提取共性部分, 这种方法在处理同质和异构设备之间的差异时是有益的, 表 4 给出了基于时序分析方法的详细对比.

表 4 基于时序分析方法的详细对比

方法	应用场景	特点	局限性
DTW[74,75]	不同副本, 不同实现	可用于相似度分析且可处理抖动对策	需要对轨迹进行成对对齐, 不适合处理高维数据
FFT[46]	不同设备 (同质, 异构)	能够提取不同设备之间的共性特征	窗口长度和类型设置不当会导致失真

3.3 性能对比

表 5 总结了各类预处理方法在不同环境下的适用性, 其中不可迭代算法特别适合处理“相同设备, 不同副本”的差异. 为了更直观地对比各方法的性能, 表 6 展示了在不同实验条件下的性能比较. 在 H-field 传感器和 XMEGA-*C*7.37 设备上, LDA 算法优于 PCA 和 FFT, 达到 91.5% 的标签准确率. 对于 ASCAD 数据集添加掩码、噪声、抖动等防御措施的场景, PCA 表现不佳, 甚至在掩码防护下攻击失效. 而 AE 和 U-Net 等可迭代算法能够有效应对噪声和抖动等防御, 其中 U-Net 表现尤为突出, 仅需 25 条轨迹便可破解噪声对策, 并能处理多种防御对策组合. 然而, U-Net 依赖于目标设备的轨迹标签信息, 这在实际应用中较难实现. EDA 算法则能在 AES_PTv2 数据上, 仅通过 310 条轨迹破解带掩码防护的设备. FFT 技术能够挖掘同质及异构设备之间的共性, 分别通过 600 条和 800 条轨迹实现从 PIC16F887-*C*3 到 PIC16F914-*C*3 以及 ATMega-163 的跨设备攻击. 因此, 在未添加额外防御措施的环境中, PCA、LDA、DTW 和 FFT 是攻击者的首选方法, 因为这些方法成本低、效率高; 而在面对掩码、时钟抖动、洗牌等防御措施时, 则需要采用可迭代算法. 尽管 AE 和 U-Net 在这些防御场景中表现优异, 但其前置条件在实际应用中存在限制, 且其在不同场景下的适用性仍需进一步分析.

表 5 各类预处理方法对不同差异环境的适用性

方法	前置条件	垂直振幅差异	采样点不同步	信噪比不同	直流偏移	掩码	时钟抖动	洗牌
PCA[32,48,49,66]	无	√	×	√	√	×	×	×
LDA[48,49,66]	需要标签	—	×	√	√	×	×	×
EDA[55]	无	—	√	√	—	√	—	—
AE[51]	可控制对策开关	—	—	√	—	—	—	—
U-Net[52]	可控制对策开关	—	√	√	—	—	√	√
DTW[74,75]	无	—	√	√	—	×	√	—
FFT[46]	无	—	√	√	—	×	—	—

注: 符号“√”代表“能够适用”, “×”代表“不能适用”, “—”代表未进行实验验证

表 6 各类预处理方法在不同场景下的性能对比

方法	差异因素	数据集		建模轨迹数	测试轨迹数	攻击结果
		采样工具	设备			
PCA+MLP[66]	不同副本	H-field 传感器	XMEGA-*C*7.37	100 000	100 000	ACC: 90.7%
LDA+MLP[66]						ACC: 91.5%
FFT+MLP[66]						ACC: 91%
PCA+TA[51]	噪声参数	$ASCAD^{f}_{desy0}$		35 000	10 000	N_{GE}>10000
AE+CNN[51]						N_{GE}: 8 751
U-Net[52]				20 000	20 000	N_{GE}: 25
AE+CNN[51]	抖动参数			35 000	10 000	N_{GE}: 822
U-Net[52]	多类对策			20 000	20 000	N_{GE}: 100
PCA+TA[55]	不同副本(掩码)	AES_PTv2		10 000	500	无法攻击
EDA+TA[55]						N_{EG}: 310
FFT+CNN[46]	同质设备	DSOX3034T (1.25 GS/s)	PIC16F887-*C*3, PIC16F914-*C*3	16 000	1 000	N_{GE}: 600
FFT+CNN[46]	异构设备,示波器	DSOX3034T (1.25 GS/s), Waverunner 6100A (500 MS/s)	PIC16F887-*C*3, ATMega-163	16 000	1 000	N_{GE}: 800

注: 设备名-*C*[时钟频率 (MHz)]表示特定时钟频率的设备; ACC代表标签准确率; N_{GE}代表攻击所需轨迹数; 多类对策指的是随机延迟、时钟抖动和洗牌3种防护对策的组合场景

4 基于多设备训练的可移植性方案

多设备训练策略是针对基于机器/深度学习模型实现攻击可移植性的一类方法. 其本质上是集合多个设备的功耗轨迹共同训练, 通过调整超参数来拟合多设备数据集中的分布差异, 从而构建出一个高泛化性的攻击模型. 这种方法所构建的模型泛化性高, 并有着强大的攻击性能, 但对攻击场景有一定的要求. 它要求攻击者拥有多个与目标设备型号一致且具有完全的控制权的建模设备. 在攻击过程中, 攻击者向多个设备执行加密, 并获取功耗、明文、密钥等信息构建可供模型训练的多设备数据集, 该方法的流程图如图 5 所示. 下面将详细介绍这类技术的研究进展.

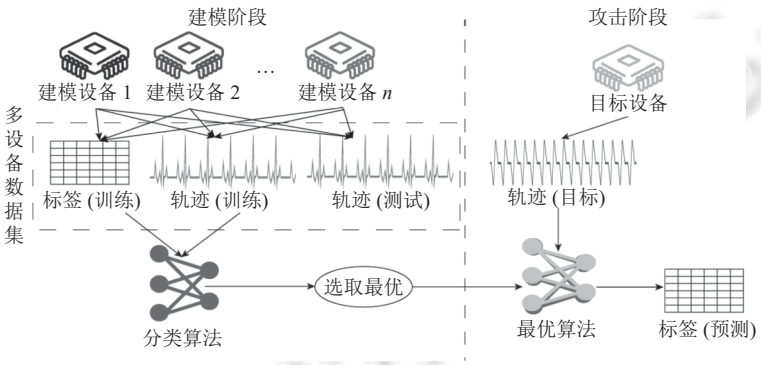

图 5 多设备训练方案流程图

在 DAC 2019 会议上, Das 等人[38]提出了第 1 项多设备训练策略的研究, 他们对 ATMega[76]微控制器 4 个不同副本进行采样, 并使用浅层的 MLP 进行训练. 然后, 使用同型号设备的另外 4 个副本进行攻击. 实验结果表明, 增加训练集中的设备数有利于模型推广到新设备中. 当训练设备数为 4 时, MLP 模型在各个副本的攻击正确率都能够达到 99%. 此外, 他们还验证了在低信噪比环境下的攻击效率, 与传统的 CPA 攻击相比, 多设备训练的 MLP 模型攻击所需的轨迹数能够减少至原来的 10%. 不足的是该研究的攻击场景仅考虑不同副本之间的少部分样本

点, 并且没有考虑密钥、采集设置等其他因素对模型移植性的影响. 因此, 使用没有任何预处理的 MLP 能够获得非常高的攻击准确率.

2019 年, Golder 等人[74]对文献 [38] 的研究进行扩展, 以提升多设备训练在现实场景中的实用性. 实验对象是 XMEGA 微控制器的不同副本, 并考虑了轨迹非对齐的情景. 为了消除差异数据对训练的影响, 他们采用了 PCA 和 DTW 预处理技术. 实验结果表明, 即使设备之间存在显著的变化, 多设备训练的 MLP 能够将单字节攻击的准确率从 8% 提升至 91.72%. 当使用 PCA 对轨迹进行预处理, 准确率则进一步提高至 99.43%. 然而, PCA 预处理的局限性在于需要轨迹采样点完全对齐, 否则将导致攻击失效. 为解决这一问题, 他们在 PCA 预处理前引入了一个 DTW 操作, 使得攻击重新生效并将准确率提高至 99.94%. 然而, 该方案存在一些不足之处是方案的步骤较为繁琐, 特别是在面对轨迹非对齐的情景时, 需要对功耗轨迹进行两次预处理操作, 增加了攻击实施的复杂性和计算成本.

Bhasin 等人[45]探讨了多种因素组合场景对模型可移植性的影响. 他们设置了“相同设备、相同密钥”“相同设备、不同密钥”“不同设备、相同密钥”“不同设备、不同密钥”这 4 个场景, 实验对象是 ATMega 微控制器的不同副本. 面对各类场景, 他们采用机器学习和深度学习方法进行可移植性测试和评估. 实验结果揭示了在密钥或设备发生改变时, 各种攻击方法的性能均受到影响. 值得注意的是, 相较于“不同密钥”场景, “不同设备”场景更为困难. 在“不同密钥”场景中, 攻击者无需作额外的处理, 仅依靠深度学习技术就能实现可移植攻击. 同时, 在其他场景下, 深度学习技术也表现出更好的性能. 总体来说, 使用多种设备数据进行训练时, 能够最小化过拟合的风险, 从而更好地推广模型. 此外, 面对不同探头位置的场景, 多设备训练策略也能够消除这些差异对攻击性能的影响. 该方法的不足之处是需要从多个副本获取大量轨迹数据, 这导致实现成本较高, 或者在现实场景中可能无法实现.

2023 年, Wu 等人[53]引入一种基于消融范式的神经网络层评估方法来克服可移植性问题. 该研究假设不同设备的差异是由于高斯噪声的扰动造成的. 因此, 他们首先消融了在原始设备中预训练模型的部分参数, 消除了其在原始设备轨迹上的过拟合影响. 然后, 使用带有噪声扰动的轨迹对消融模型进行恢复训练, 从而提高模型的可移植性. 通过这一做法可以实现从单个设备创建多设备场景, 为模型训练提供有价值的知识, 解决了攻击者没有多台设备进行训练的现实问题. 不足之处是该方法是假设设备之间的所有差异是由于噪声扰动造成的, 在面向目标设备的采样设置不同 (比如频率缩放、触发故障) 以及时钟抖动对策等其他差异情况, 这一方法是否有效仍然存在不确定性.

表 7 总结了基于多设备训练的可移植性攻击的应用场景, 特点以及局限性. 为了更直观、量化地对比各个方法的性能, 表 8 中总结了各个方法在“同一设备、不同副本”场景下所设置的实验环境与性能对比结果. 在 Chipwhisperer 设备环境下, 实验显示, 将训练设备数从 1 增加到 4 时, MLP 模型的分类准确率由 80% 提升至 99%. PCA 预处理方法能够很好地适配 MLP 模型, 即便在仅使用单个设备进行训练时, 准确率也能达到 90.09%. 如果采样过程中出现轨迹未对齐的情况, 需引入 DTW 技术以便更好地适配 PCA 并取得良好效果. 总体而言, 预处理技术结合多设备训练方法表现出强大的优势. 尤其在设备功耗分布存在显著差异时, 可以采用 PCA、DTW 等预处理技术来修正轨迹, 从而帮助模型更有效地进行训练[74].

表 7　各类训练策略的详细对比

方法	应用场景	特点	局限性
多设备训练 (MLP)[38]	不同副本	验证了设备数对攻击的性能的增益	未考虑除芯片差异外的其他因素
多设备训练+预处理[74]	不同副本、非对齐轨迹	使用预处理技术处理轨迹	操作步骤繁琐
多设备训练 (MLP, CNN)[45]	不同副本、不同密钥	系统性地研究多类场景组合	实现成本高
消融分析[53]	相同副本、不同实现	从单个设备创建多设备场景	仅考虑噪声对策

然而, 这类方法的最大缺陷在于依赖建模设备的数量, 攻击者必须同时拥有多个与目标设备相同的建模设备. 另一方面, 在 TDS2012 示波器 (2 GS/s) 与 ATMega328p-*C*16 设备环境下, Wu 等人[53]通过引入噪声扰动为单设备模型训练提供了新的知识. 与 Bhasin 等人[45]的方法相比, 他们减少了 3 个设备的训练, 并且减少了 50% 的攻击轨迹数量. 这证明了抖动扰动的可行性. 未来, 是否能够通过噪声、时钟抖动等策略组合来衍生或仿真出多个差异化数据集, 以提升模型的泛化能力, 从而实现可移植性攻击, 仍然是一个值得深入探讨的问题.

表 8 多设备训练方法在“同一设备、不同副本”场景下的性能对比

方法	数据集		训练集			测试集	攻击效果
	采样工具	设备	轨迹数	设备数目	额外因素	设备数目	
多设备训练 (MLP)[38]	Chipwhisperer	XMEGA-*C*7.37	10 000	1	无	4	ACC: 80%
			40 000	4	无	4	ACC: 99%
PCA+多设备训练 (MLP)[74]			10 000	1	无	30	ACC: 90.09%
			40 000	4	无	30	ACC: 99.43%
			40 000	4	轨迹未对齐	30	无法攻击
DTW+PCA+多设备训练 (MLP)[74]			40 000	4	轨迹未对齐	30	ACC: 99.94%
多设备训练 (MLP, CNN)[45]	TDS2012示波器 (2 GS/s)	ATMega328p-*C*16	40 000	4	无	4	N_{GE}: 60
消融分析[53]			10 000	1	无	4	N_{GE}: 30

注: 设备名-*C*[时钟频率 (MHz)]表示特定时钟频率的设备; ACC代表标签准确率; N_{GE}代表攻击所需轨迹数

5 基于迁移学习的可移植性方案

迁移学习是一种机器学习方法, 旨在将一个任务学习到的知识迁移到另一个相关任务上, 以改善目标任务的性能[77]. 在传统机器学习中, 通常需要大量标注数据用于训练模型, 但在现实应用中往往存在数据稀缺或者标注成本高的问题. 给定源域 D_s 和学习任务 T_s, 目标域 D_t 和学习任务 T_t, 迁移学习的目的是将 D_s 和 T_s 获得的知识用于提高目标预测函数 $F_t(\cdot)$ 在 D_t 上的性能, 其中 $D_s \neq D_t$ 或 $T_s \neq T_t$. 在 SCA 领域中, D_s 所对应的是建模设备的数据集, 而目标域 D_t 所对应的是目标设备的数据集.

在现实场景中攻击者可能会受到访问次数限定、采样轨迹时间长等各方面的限制, 导致没有足够的信息破解密钥. 因此, 迁移学习的属性非常契合建模类 SCA 的需求. 一系列研究采用迁移学习技术来弥补建模类 SCA 在可移植性上的不足. 在当前的研究中, 研究者通常采用一种名为“预训练+微调”的策略来实现可移植性攻击. 该方法整个流程如图 6 所示, 具体而言, 可分为以下 3 个步骤.

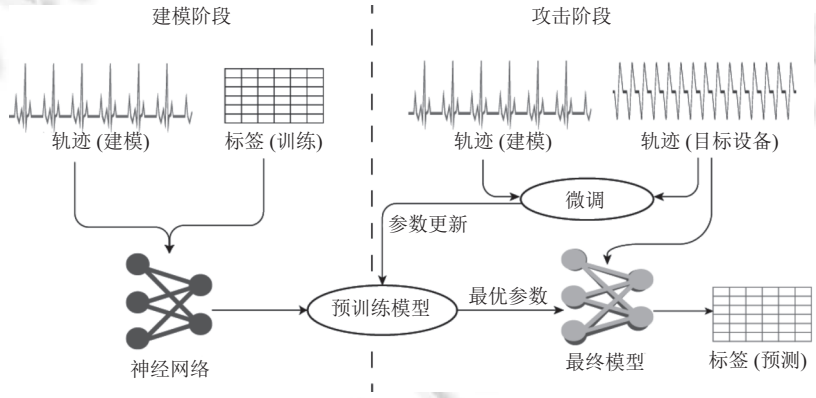

图 6 迁移学习可移植性方案流程图

● 预训练: 在建模设备上进行有监督训练, 学习任务相关的特征表示. 该部分需要使用标签数据, 目的是让模型学习在建模设备上破解密钥所需的知识.

● 微调: 通过一系列微调技术对预训练模型的参数进行调整, 以消除不同域之间差异.

● 攻击: 使用微调后得到的模型对目标设备进行密钥分析.

接下来, 本文将依据目标设备是否可获取标签信息将迁移学习的方法划分为两类来介绍基于迁移学习的可移植性攻击的研究进展.

5.1 面向目标设备可获取标签信息的方法

在目标设备可获取标签信息的场景中, 假设攻击者能够在目标设备上获取少量轨迹标签信息, 但总体采样轨迹数是受限的. 这种限制对应于现实中的一些特殊场景, 由于时间、资源和对策等多方面的限制, 攻击者无法收集足够的轨迹. 一方面, 如果攻击的加密程序是整体程序的一个子程序, 或者加密程序的位置是不固定的[78]. 在这些情况下, 攻击者在每次采集轨迹时需要等待整个程序运行完毕, 或花费大量精力去寻找加密位置, 导致采集轨迹的成本较高. 另一方面, 在实际应用中, 为了维护芯片的安全性, 一些设计者会在加密芯片布置控制逻辑, 其工作速度可能被限制为固定的速度, 导致采样大量轨迹的时间成本高[79]. 为了应对这些情况, 一系列针对小样本数据训练的策略被提出[80–82], 但这些研究没有考虑建模与目标设备的差异性. 下面, 本文将介绍迁移学习技术在这类场景的研究进展.

2020 年, Genevey-Metat 等人[83]将预训练的概念引入到 SCA 领域. 预训练即在已有的大规模任务或领域的数据集上预先训练模型. 然后将这个在源任务上学到的模型参数作为初始参数, 进一步在目标任务上进行微调. 与图像分类领域不同, SCA 领域的预训练模型并不容易获得, 除了 ASCAD 有公开预训练模型, 其他数据集尚未给出. 他们在论文定义了 3 个攻击场景.

● 场景 A0: 攻击者仅有一个克隆数据集 (与目标设备相同的数据集) 来训练一个神经网络, 然后对目标设备分析.

● 场景 A1: 攻击者仅用一个预训练模型进行攻击, 其中预训练数据集与目标数据集在探针类型/位置、侧信道信息以及设备芯片等方面存在差异.

● 场景 A2: 攻击者同时拥有克隆数据集和预训练模型进行攻击.

实验结果表明, 性能表现最差的攻击场景是 A1, 因为它缺乏对克隆数据集的训练. 当克隆数据集中的可用数据量低于某一阈值时, A2 的性能将优于 A0, 这个阈值取决于实验设置 (例如探针、侧通道或设备). 总体而言, A2 表现最为优异, 它能够用非常有限的轨迹数量 (低于 10 条) 来揭示密钥. 然而, 这项工作的不足之处是作者将克隆数据集定义为与目标设备相同的数据集, 这种假设是不现实的.

与其他工作不同, 2020 年, Thapar 等人[56]利用迁移学习技术减少攻击者对建模设备轨迹数的需求. 首先, 他们使用已有的任意设备训练一个模型. 接着, 冻结该模型的预测层, 并使用建模设备的轨迹数据进行微调. 最终, 将调整后的模型用于攻击目标设备. 由于模型提前在攻击者已有的设备中学到相关知识, 因此在建模阶段无需从头开始训练, 而根据建模轨迹进行参数调整. 这有助于降低训练时间和对建模轨迹数量的需求. 不同环境的仿真实验结果显示, 即使已有的设备与目标设备有着不同的底层架构, 甚至不同防护对策, 该方法仍能在这些场景实现知识迁移. 然而, 不足之处是, 该工作只进行了仿真实验验证, 尚未在真实设备上进行性能验证.

Yu 等人[59]基于元迁移学习的方法提出了一种跨设备攻击方案. 该方法的整体方案分 3 个步骤: 预训练、元迁移学习和攻击. 其中“元迁移学习”指攻击者应用元学习能够自适应学习新任务的特性对模型参数进行微调. 此外, 作者提出了皮尔逊乘积矩相关系数的方法用于评估不同设备之间的相似性. 实验中他们在 5 个不同的微处理器 (STM32F0-STM32F4, ATMega) 上采集了功耗与电磁轨迹. 结果显示, 在同一类型的微处理器上该方法只需要 10 条以内的轨迹数就能破解密钥. 在面对不同设备的跨设备攻击时, 该方法使用 500 以内数量的轨迹就能破解密钥. 该方法的不足之处是依赖攻击者能够获取目标设备中足够数量的带标签信息轨迹对模型进行微调, 其中功耗轨迹需要至少 800 条, 电磁轨迹需要至少 1 500 条, 而在实际攻击场景中, 目标设备中大量的标签信息是很难获取的.

2023 年, Paguada 等人[54]构造了一种基于深度学习的模块化网络. 在该方案中他们定义了一种可重用的训练模块, 它在非目标数据集上学习轨迹之间的共同特性. 在攻击目标数据集时, 攻击者不需要重新训练模型, 而是基于可重用模块已学习到的知识进行调整, 从而减少了攻击的成本. 在实验中, 他们以 AE 作为基础搭建模块化网络, 它包括 3 个主要部分: 编码器、解码器和分类器. 在该方案中, 首先使用编码器和解码器对建模数据集进行训练用于提取特征, 一旦其训练好, 就会弃用解码器. 然后, 使用编码器和分类器在目标数据集上进行参数调整并评估性能. 实验结果显示, 在面对不同数据集, 使用模块化网络能够减少搭建模型的训练时间和调整超参数的繁琐. 不足

之处是实验所使用的数据集 ASCAD^f 和 ASCAD^r[21]是同一块芯片上所采集的轨迹, 他们未考虑芯片差异对攻击可移植性的影响.

在表 9 中, 对面向目标设备可获取标签信息场景的方法进行了总结. 该类方法假设攻击者能够获取目标设备少量轨迹的标签信息. 为了更直观、量化地对比各个方法的性能, 表 10 总结了各类方法的实验设置与其所达到的攻击效果. 由于 Thapar 等人[56]的研究采用的是仿真环境, 因此不纳入本表中的数据对比. 在 Chipwhisperer 采集平台下, 对开发板 STM32F1-STM32F4 进行的跨设备攻击实验结果显示, 预训练+微调[83]的方法能够在使用 20 000 条建模轨迹训练, 2 500 条带标签目标轨迹进行微调的情况下, 通过 3 条轨迹就能完成攻击. 相较之下, 利用元迁移学习的方法能够仅使用 800 条轨迹微调的情况下, 达到相同的性能, 并且能够在使用 50 000 条建模轨迹训练, 1 500 条轨迹微调的情况下, 使用 230 条轨迹能够实现从 STM32Fx 到 XMEGA 的跨设备攻击. 模块化网络则能够极大减少训练时间成本, 在 ASCAD 数据集实验环境下, 针对其偏移参数为 0、50 和 100 的版本, 模型分别只需 9、65 和 100 个周期即可完成训练并破解密钥.

表 9　目标设备可获取标签信息场景方法的详细对比

方法	应用场景	特点	局限性
预训练+微调[83]	相同副本	考虑了不同采样设置、设备差异等因素	数据集假设不现实
预训练+冻结+微调[56]	不同设备、不同实现	减少对建模设备的轨迹数需求	未进行真实实验
元迁移学习[59]	不同设备	减少攻击轨迹数	实际场景难实现
模块化网络[54]	相同副本、不同实现	目标设备更换实现方式无需重新训练	未考虑芯片差异的影响

表 10　可获取标签信息场景下各类方法的性能对比

方法	差异因素	数据集		训练轨迹数	微调轨迹数	测试轨迹数	攻击效果
		采样工具	设备				
预训练+微调[83]	探头类别	RF-B 0.3-3, RF-K7-4 (1 GS/s)	STM32Fx-*C*7.37	20 000	2 500	20 000	N_{GE}: 10
	同质设备	Chipwhisperer	STM32Fx-*C*7.37	20 000	2 500	20 000	N_{GE}: 3
元迁移学习[59]	同质设备	Chipwhisperer	STM32Fx-*C*7.37	20 000	800	10 000	N_{GE}: 3
	异构设备	Chipwhisperer	STM32Fx-*C*7.37, XMEGA-*C*7.37	20 000	800	10 000	N_{GE}: 40
	异构设备, 探头类别	N2894A, LF-3 (2.5 GS/s)	STM32Fx-*C*7.37, XMEGA-*C*7.37	50 000	1 500	20 000	N_{GE}: 230
模块化网络[54]	抖动参数	ASCAD$^f_{desy50}$, ASCAD$^r_{desy0}$		50 000	200 000	100 000	EP: 9
		ASCAD$^f_{desy50}$, ASCAD$^r_{desy50}$		50 000	200 000	100 000	EP: 65
		ASCAD$^f_{desy50}$, ASCAD$^r_{desy100}$		50 000	200 000	100 000	EP: 100

注: 设备名-*C*[时钟频率 (MHz)]表示特定时钟频率的设备; EP代表模型攻击成功最低训练周期数; N_{GE}代表攻击成功所需轨迹数; STM32Fx代表开发板STM32F1–STM32F4的集合

然而, 这种假设存在根本性的问题, 因为已知目标设备的标签信息意味着攻击者事先了解目标设备的密钥信息. 这一假设在实际场景中是不现实的, 其可行性受到了严重挑战. 因此, 这些方法在本质上无法实现可移植攻击的目标. 尽管存在这一困境, 但对这类方法在减少训练所需轨迹数方面的研究仍具有一定的价值. 通过一系列微调技术, 研究者可以尝试降低建模阶段所需的轨迹数, 从而有效减少采集与处理轨迹的繁琐步骤以及模型训练成本. 例如, 攻击者可以通过可掌控的设备或利用网上公开数据来获取预训练模型, 然后通过微调或元学习的方式, 使用少量建模轨迹对预训练模型参数进行调整, 以减少模型训练所需的成本.

5.2　面向目标设备无法获取标签信息的方法

在目标设备无法获取标签信息的场景中, 攻击者无权获取到目标设备的标签信息, 并且总体采样轨迹数是受限的. 该场景最符合实际情况. 由于目标设备无法提供标签信息, 攻击者无法利用这一信息源来引导模型更新权重. 同时, 总体采样轨迹数的限制使得攻击者在微调过程中要更加慎重的使用数据以避免过拟合现象. 在此类场景中, 研究者引入无监督迁移学习来构造可移植性方案. 下面, 本文将详细介绍这些方法.

Cao 等人[47]在总损失中引入最大均值差异 (maximum mean discrepancy, MMD)[84]损失用于调整预训练的模型参数. 通过最小化 MMD 损失 L_{MMD} 和分类损失 L_C, 使得模型能够学习到设备不变性的隐式表示. 该损失函数 L 可表示为 $L=L_C+\lambda L_{MMD}$, 其中 λ 用于调整 L_{MMD} 的权重. 在不同的数据集中模型根据 L_C 和 L_{MMD} 的关系进行参数调整. 实验中他们分别对不同设备 (SAKURA-G[85]、XMEGA)、不同实现 (高斯噪声、时钟抖动策略) 以及不同采集设置 (功耗、电磁) 的场景进行验证. 但需要注意的是他们的攻击始终讨论的还是“同一设备、不同副本”场景. 比如在不同设备场景中, 他们所做的不是将 SAKURA-G 上训练的模型移植到 XMEGA 上执行攻击, 而是采用原设备对模型训练. 然后对这个设备的不同副本进行攻击. 实验结果证明该方案能够对不同设备、不同采样设置场景中的各类副本进行可移植性攻击. 但是由于添加时钟抖动后的轨迹差异过大, 无法对该场景进行攻击. 该项工作的最大优势是攻击者仅需要获取到目标设备的 200 条轨迹且不需要获得其标签信息. 不足之处是 MMD 损失对核函数的选择很敏感, 面对不同场景时很难找到最优参数.

Cao 等人[86]首次将对抗迁移学习引入到 SCA 领域. 该方法通过引入对抗性损失对模型参数进行微调, 使其在目标域上生成的特征表示与源域中的特征表示相似. 它有助于使模型更好地适应目标设备的数据, 提高可移植性攻击的性能. 该项技术类似于对抗生成网络, 它包含编码器 (encoding, E)、标签分类器 (classifier, C)、领域判别器 (discriminator, D) 这 3 部分. 在损失函数的设计中, 作者引入了额外的标签条件 g 来指导模型完成分类任务 f, 其中条件作用由 $f\otimes g$ 实现, $\otimes$ 表示外积操作. 在实验验证阶段, 该方法仅使用了 200 条无标签信息的目标轨迹进行模型微调. 在 XMEAG 数据集中, 该方法取得了最先进的攻击性能. 然而, 该方法仅讨论了汉明重量标签模型, 而未对中间值标签模型的效果和性能进行深入讨论. 这两种模型分别对应着高精度和低精度分类正确率的场景. 低精度的标签条件 g 能否正确指导模型完成分类任务 f, 还需要进一步讨论. 此外, 该方法在使用轨迹前需要进行预处理, 因为一旦轨迹采样点过多, 外积操作可能出现维度爆炸导致攻击失败.

表 11 总结了面向目标设备无法获取标签信息场景方法的详细对比. 在 CPDA 数据集上, 使用微调 (MMD) 的方法能够在仅使用 200 条无标签目标轨迹微调的情况下, 通过 34 条轨迹破解密钥. 然而, 该方法在面向不同场景时容易出现核函数寻优困难, 导致其大量成本消耗在核函数的优化上. 相较之下, 对抗迁移学习方法无需核函数, 更具适应性. 在相同条件下, 相比于微调 (MMD) 方法, 该方法攻击所需的轨迹数减少了 64%.

表 11 面向目标设备无法获取标签信息场景方法的详细对比

方法	应用场景	数据集	微调轨迹数	N_{GE}	特点	局限性
微调 (MMD)[47]	不同副本	CDPA	200	34	不同设备、不同采样环境下的副本迁移	核函数寻优困难
对抗迁移学习[86]	不同副本	CDPA	200	18	攻击效率高	无法处理高维数据

注: N_{GE}代表攻击成功所需轨迹数

由于场景要求苛刻, 目前这些方法仅能在“同一设备、不同副本”的场景进行分析. 对于“同一设备、不同实现”以及“不同设备”等更复杂的场景尚未进行讨论. 无监督迁移学习的引入为可移植攻击提供更广泛应用场景, 因为其不受采样限制的影响. 然而, 对于无监督迁移学习方法在 SCA 领域的研究仍处于起步阶段, 需要更多的技术探索和深入研究. 未来的研究方向可能涉及如何利用无监督迁移学习方法适应各种设备和场景, 以提高攻击的实用性和普适性. 同时, 图像、语言处理领域的方法不能完全能适用于 SCA. 如何结合 SCA 领域特性, 构建适用于 SCA 的无监督迁移学习理论, 这将是一个富有挑战性的方向.

6 总结与展望

当前可移植性方案的设计与构建是 SCA 研究的热点方向. 其核心目标在于为 SCA 提供更加灵活、广泛适用的威胁模型, 以满足不同场景和应用需求的多样性. 面对现有综述在这一领域存在的空白, 本文通过对各类场景中 SCA 面临的可移植性挑战进行深入分析和总结, 同时介绍各类可移植性研究的相关进展. 接下来, 本文将对复杂应用场景下 SCA 的可移植性研究进行详细总结. 同时, 基于可移植性环境的不断发展和变化, 本文提出了一系列可能的研究方向和问题, 探讨了该领域未来的研究方向. 这不仅包括理论层面的问题, 也包括实际应用中的挑战, 为研究者提供了一个系统全面的参考.

6.1 总 结

现有的可移植性方案主要涵盖数据预处理、多设备训练和迁移学习这 3 个技术方面, 以解决可移植性问题. 首先, 数据预处理作为操作最简便、实现成本最低的方法, 是攻击者优先考虑的方法之一. 不可迭代算法主要涉及了 PCA、LDA、DWT、FFT 等预处理技术, 其中 PCA、LDA 更擅长处理噪声、直流偏移所引起的差异, 而 FFT、DWT 则擅长处理未对齐的轨迹. 此外, 自编码器、U-Net 等深度学习技术则在更复杂对策的可移植场景进行探索. 相较于预处理技术, 基于多设备训练的可移植性方案在攻击性能上表现更为高效. 研究者推荐使用 CNN、MLP 作为基础网络来训练高泛化性模型. 然而, 该方法对攻击场景的设备数量以及采集轨迹的要求也更加苛刻. 基于迁移学习的方案对不同攻击场景的适用性更为广泛. 一方面, 在目标设备能够获取标签信息的场景下, 采用元学习迁移、有监督微调技术能够极大减少建模/攻击所需的轨迹数. 另一方面, 在目标设备完全不能获取标签信息, 甚至采集轨迹困难的场景下, 使用无监督微调和对抗迁移学习技术可以消除建模设备与目标设备的特征差异. 最后, 图 7 展示了这 3 种方案之间的特点以及它们对应的攻击场景.

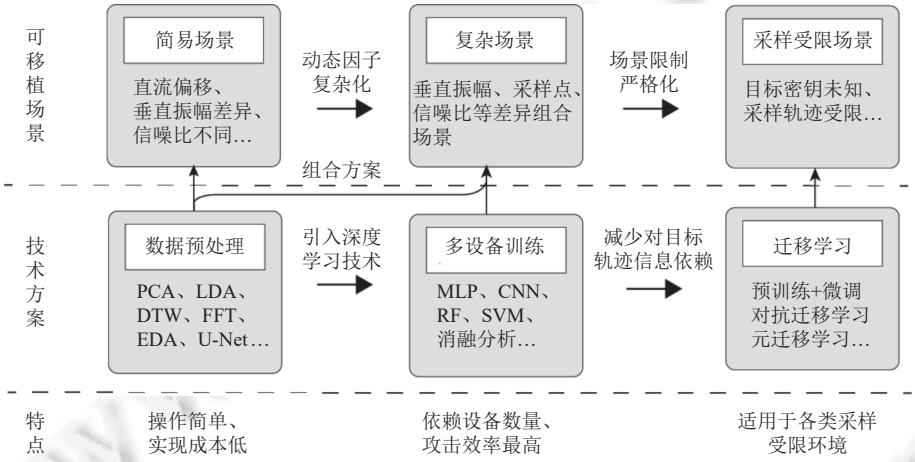

图 7 各类方法特点以及应用场景

为了更清楚地展示当前阶段可移植性技术的实际应用, 表 12 总结了各类方法的最佳实践和失败临界场景, 某个方法在临界场景中失效时, 它在面临更加复杂情况时也会失败. 我们仅纳入了成熟的技术方案进行分析, 不考虑需要控制目标设备且需要获取标签的方案, 因为这类方法尚无法直接应用于现实场景. 从理论上讲, 多设备训练方法具有最高的准确性和适应性, 但由于需要假设多个设备与目标设备一致, 这在实际应用中难以实现. 为了更贴合现实场景, 本文定义了最佳实践场景为: 在单设备训练环境中无法获取目标设备标签的情况下, 能够实现可移植性攻击的方法. 根据已有文献研究, 场景的困难程度排序如下, 其中<代表难度较小, ≈代表难度接近.

不同密钥<不同副本<不同探头位置<不同实现 (噪声)<不同实现 (抖动)≈不同实现 (掩码)<不同设备.

表 12 各类方法的最佳实践用例与失败场景

方法	具体技术	最佳实践用例	失败临界场景
数据预处理	PCA	不同副本	不同实现 (抖动)
	DTW	不同实现 (抖动)	不同设备
	EDA	不同实现 (掩码)	未进一步讨论
	FFT	不同设备 (异构、同质)	未进一步讨论
多设备训练	CNN (单设备、多密钥)	不同密钥	不同副本
	消融分析	不同副本	不同实现 (抖动)
迁移学习	微调 (MMD)	不同探头位置	不同实现 (抖动)
	对抗迁移学习	不同副本	不同实现 (抖动)

6.2 展　望

结合国内外已有研究成果的分析, 本文总结出当前尚需进一步探索和突破的若干关键问题, 具体如下.

1) 在数据预处理研究路线上, 现有研究表明使用 PCA、LDA、DTW、FFT 适用于大部分无防护对策场景, 但这些方法对于高斯延迟、随机延迟、时钟抖动、洗牌和掩码等对策鲜有进行讨论. 在 Rioja 等人[55]研究中更是验证了 PCA 对掩码对策设备的预处理无效导致移植失败. 而需要迭代训练的 EDA、AE、U-Net 算法对在这方面处理能力更强, 但对这类算法的研究还在起步阶段, 它在实验条件、计算成本上都存在一定缺陷. 因此, 有必要系统性研究该类算法, 以构造出适用场景更广泛的预处理方案.

2) 在多设备训练研究路线上, 一方面现有方案都是基于对“同一设备, 不同副本”的实验场景构建多副本通用的模型. 而 Zhang 等人[46]的研究揭示了如何使用 FFT 预处理技术来实现对同质和异构设备的跨设备攻击. 因此, 在多设备训练的强假设下, 如何通过有效的预处理方法, 针对不同类型的同质和异构设备进行联合训练, 克服同质和异构设备之间的差异, 提高模型在多样化设备上的性能是值得研究的. 另一方面, 多设备训练策略的主要缺陷是需要攻击者掌握多个可控且与目标相似的设备, 能否在单个设备上组合噪声、抖动、掩码等一系列策略来衍生或者仿真出多个存在差异性的数据集来提高模型的泛化性, 实现可移植性攻击也是值得探讨的方向.

3) 在迁移学习研究路线上, Cao 等人[47,86]所提出的无监督迁移学习的方法极大地弱化了攻击者对目标设备的获取轨迹信息的需求 (无需获取标签信息, 且仅需要少量轨迹数). 该类方法更符合现实场景的需求, 未来应该延续这一方向进行研究. 在这些方法中, 使用 MMD 进行微调的策略对核函数的选择非常敏感, 在面对不同设备时需要搜索与更换核函数来获取良好的攻击性能, 但很难找到最优核函数. 因此, 有必要深入研究在微调过程中核函数的寻优方法, 以提高 MMD 方法在不同环境中的应用能力. 其次, 在对抗迁移学习方案中, 在损失函数引入标签条件的外积操作会导致维度爆炸, 能否找到计算量小的平替计算方法. 同时, 在他们的方案中只讨论了局部对齐的方案, 该方案更适用于高分类准确率的领域. 对于 SCA 领域分类正确率是弃用的指标, 其数值也是极低的 (例如 ASCAD 数据集[21]的分类正确率仅为 1%), 引入标签条件可能导致负迁移效果. 因此, 有必要将全局对齐的方案纳入讨论与分析.

4) 随着新的应用场景不断出现, 静态密码逐渐不能满足当前安全需求. 例如全盘加密作为保护用户计算设备存储数据安全的重要手段, 不同磁盘扇区需采用不同的加解密算法, 这就要求分组密码提供除密钥之外的安全参数. 因此, 动态/可调分组密码被提出. 其中动态分组密码可分为组件动态与结构动态两种动态模式, 这些变化使得差分、线性攻击路径变化, 让传统密码分析难以切入. 可调分组密码无需重新密钥扩展, 仅更换 Tweak 便可达到更换密钥安全性. 目前, 仍未有研究全面而系统地分析 SCA 对这些算法的威胁性. 特别是, 基于迁移学习的 SCA 对动态/可调分组密码的可移植性问题. 利用迁移学习技术能够使得建模类 SCA 适应不同差异的场景. 因此, 利用迁移学习对不同可调/动态分组密码的可移植性场景进行分析是必要的, 该方向有助于研究者更全面地理解这些算法在实际应用中的安全性表现.

5) 在构建攻击的可移植性方案时, 迫切需要提出一个公开认可的设备相似度评估标准, 以引导攻击者在不同场景下精准地设计攻击方案. 在当前的研究中, 已有的一些方法如皮尔逊乘积矩相关系数、DTW、瓦瑟斯坦距离以及最大平均差异, 这些方法为设备差异的评估提供了一些基础. 然而, 目前研究者没有确认一个公开认可的评估标准. 未来的研究需要确认和完善设备相似度评估的标准. 该标准的制定需要充分考虑多个因素, 包括但不限于设备类型、算法实现、采集环境等, 还需要关注可重复性和可比性的问题. 此外, 评估标准应该具备一定的稳定性, 确保在不同的研究和实际应用中都能够得到一致的结果, 从而保证其实用性.

References

[1] Kocher PC. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Koblltz N, ed. 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] Le TH, Canovas C, Clédière J. An overview of side channel analysis attacks. In: Proc. of the 2008 ACM Symp. on Information, Computer and Communications Security. Tokyo: ACM, 2008. 33–43. [doi: 10.1145/1368310.1368319]

[3] Zhang TW, Zhang YQ, Lee RB. CloudRadar: A real-time side-channel attack detection system in clouds. In: Monrose F, Dacier M, Blanc G, Garcia-Alfaro J, eds. Proc. of the 19th Int'l Symp. on Research in Attacks, Intrusions, and Defenses. Paris: Springer, 2016. 118–140. [doi: 10.1007/978-3-319-45719-2_6]

[4] Moos T, Moradi A, Richter B. Static power side-channel analysis—An investigation of measurement factors. IEEE Trans. on Very Large Scale Integration (VLSI) Systems, 2020, 28(2): 376–389. [doi: 10.1109/tvlsi.2019.2948141]

[5] Longo J, De Mulder E, Page D, Tunstall M. SoC it to EM: Electromagnetic side-channel attacks on a complex system-on-chip. In: Güneysu T, Handschuh H, eds. Proc. of the 17th Int'l Workshop on Cryptographic Hardware and Embedded Systems. Saint-Malo: Springer, 2015. 620–640. [doi: 10.1007/978-3-662-48324-4_31]

[6] Baksi A, Bhasin S, Breier J, Jap D, Saha D. A survey on fault attacks on symmetric key cryptosystems. ACM Computing Surveys, 2022, 55(4): 86. [doi: 10.1145/3530054]

[7] Mangard S. A Simple Power-Analysis (SPA) attack on implementations of the AES key expansion. In: Lee PJ, Lim CH, eds. Proc. of the 5th Int'l Conf. on Information Security and Cryptology. Seoul: Springer, 2002. 343–358. [doi: 10.1007/3-540-36552-4_24]

[8] Kocher P, Jaffe J, Jun B. Differential power analysis. In: Wiener M, ed. 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]

[9] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model. In: Joye M, Quisquater JJ, eds. Proc. of the 6th Int'l Workshop on Cryptographic Hardware and Embedded Systems. Cambridge: Springer, 2004. 16–29. [doi: 10.1007/978-3-540-28632-5_2]

[10] Chen JC, Ng JS, Chong KS, Lin ZP, Gwee BH. A novel normalized variance-based differential power analysis against masking countermeasures. IEEE Trans. on Information Forensics and Security, 2021, 16: 3767–3779. [doi: 10.1109/tifs.2021.3093783]

[11] Chari S, Rao JR, Rohatgi P. Template attacks. In: Kaliski BS, Koc CK, Paar C, eds. Proc. of the 4th Int'l Workshop on Cryptographic Hardware and Embedded Systems. Redwood Shores: Springer, 2003. 13–28. [doi: 10.1007/3-540-36400-5_3]

[12] Schindler W, Lemke K, Paar C. A stochastic model for differential side channel cryptanalysis. In: Rao JR, Sunar B, eds. Proc. of the 7th Int'l Workshop on Cryptographic Hardware and Embedded Systems. Edinburgh: Springer, 2005. 30–46. [doi: 10.1007/11545262_3]

[13] Wu L, Perin G, Picek S. On the evaluation of deep learning-based side-channel analysis. In: Balasch J, O'Flynn C, eds. Proc. of the 13th Int'l Workshop on Constructive Side-channel Analysis and Secure Design. Leuven: Springer, 2022. 49–71. [doi: 10.1007/978-3-030-99766-3_3]

[14] Hospodar G, Gierlichs B, De Mulder E, Verbauwhede I, Vandewalle J. Machine learning in side-channel analysis: A first study. Journal of Cryptographic Engineering, 2011, 1(4): 293–302. [doi: 10.1007/s13389-011-0023-x]

[15] Belgiu M, Drăguţ L. Random forest in remote sensing: A review of applications and future directions. ISPRS Journal of Photogrammetry and Remote Sensing, 2016, 114: 24–31. [doi: 10.1016/j.isprsjprs.2016.01.011]

[16] Lerman L, Bontempi G, Markowitch O. A machine learning approach against a masked AES. Journal of Cryptographic Engineering, 2015, 5(2): 123–139. [doi: 10.1007/s13389-014-0089-3]

[17] Kohonen T, Oja E, Simula O, Visa A, Kangas J. Engineering applications of the self-organizing map. Proc. of the IEEE, 1996, 84(10): 1358–1384. [doi: 10.1109/5.537105]

[18] Maghrebi H, Portigliatti T, Prouff E. Breaking cryptographic implementations using deep learning techniques. In: Carlet C, Hasan MA, Saraswat V, eds. Proc. of the 6th Int'l Conf. on Security, Privacy, and Applied Cryptography Engineering. Hyderabad: Springer, 2016. 3–26. [doi: 10.1007/978-3-319-49445-6_1]

[19] Tang JX, Deng CW, Huang GB. Extreme learning machine for multilayer perceptron. IEEE Trans. on Neural Networks and Learning Systems, 2016, 27(4): 809–821. [doi: 10.1109/TNNLS.2015.2424995]

[20] Krizhevsky A, Sutskever I, Hinton GE. ImageNet classification with deep convolutional neural networks. Communications of the ACM, 2017, 60(6): 84–90. [doi: 10.1145/3065386]

[21] Benadjila R, Prouff E, Strullu R, Cagli E, Dumas C. Deep learning for side-channel analysis and introduction to ASCAD database. Journal of Cryptographic Engineering, 2020, 10(2): 163–188. [doi: 10.1007/s13389-019-00220-8]

[22] Zaid G, Bossuet L, Habrard A, Venelli A. Methodology for efficient CNN architectures in profiling attacks. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2020, 1: 1–36. [doi: 10.13154/tches.v2020.i1.1-36]

[23] Wouters L, Arribas V, Gierlichs B, Preneel B. Revisiting a methodology for efficient CNN architectures in profiling attacks. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2020, 3: 147–168. [doi: 10.13154/tches.v2020.i3.147-168]

[24] Hajra S, Chowdhury S, Mukhopadhyay D. EstraNet: An efficient shift-invariant Transformer network for side-channel analysis. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2024, 1: 336–374. [doi: 10.46586/tches.v2024.i1.336-374]

[25] Karayalçın S, Krček M, Wu LC, Picek S, Perin G. It's a kind of magic: A novel conditional GAN framework for efficient profiling side-channel analysis. In: Proc. of the 30th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Kolkata:

Springer, 2024. 99–131. [doi: 10.1007/978-981-96-0944-4_4]

[26] Schoos K, Meschkov S, Tahoori MB, Gnad DRE. JitSCA: Jitter-based side-channel analysis in picoscale resolution. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2023, 3: 294–320. [doi: 10.46586/tches.v2023.i3.294-320]

[27] Perin G, Wu L, Picek S. Exploring feature selection scenarios for deep learning-based side-channel analysis. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2022, 4: 828–861. [doi: 10.46586/tches.v2022.i4.828-861]

[28] Cagli E, Dumas C, Prouff E. Convolutional neural networks with data augmentation against jitter-based countermeasures: Profiling attacks without pre-processing. In: Fischer W, Homma N, eds. Proc. of the 19th Int'l Conf. on Cryptographic Hardware and Embedded Systems. Taipei: Springer, 2017. 45–68. [doi: 10.1007/978-3-319-66787-4_3]

[29] Cao P, Zhang C, Lu XJ, Gu DW, Xu S. Improving deep learning based second-order side-channel analysis with bilinear CNN. IEEE Trans. on Information Forensics and Security, 2022, 17: 3863–3876. [doi: 10.1109/tifs.2022.3216959]

[30] Masure L, Dumas C, Prouff E. A comprehensive study of deep learning for side-channel analysis. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2020, 1: 348–375. [doi: 10.13154/tches.v2020.i1.348-375]

[31] Renauld M, Standaert FX, Veyrat-Charvillon N, Kamel D, Flandre D. A formal study of power variability issues and side-channel attacks for nanoscale devices. In: Proc. of the Annual Int'l Conf. on the 2011 Theory and Applications of Cryptographic Techniques. Tallinn: Springer, 2011. 109–128. [doi: 10.1007/978-3-642-20465-4_8]

[32] Elaabid MA, Guilley S. Portability of templates. Journal of Cryptographic Engineering, 2012, 2(1): 63–74. [doi: 10.1007/s13389-012-0030-6]

[33] Lomné V, Prouff E, Roche T. Behind the scene of side channel attacks. In: Sako K, Sarkar P, eds. Proc. of the 19th Int'l Conf. on the Theory and Application of Cryptology and Information. Bengaluru: Springer, 2013. 506–525. [doi: 10.1007/978-3-642-42033-7_26]

[34] Hanley N, O'Neill M, Tunstall M, Marnane WP. Empirical evaluation of multi-device profiling side-channel attacks. In: Proc. of the 2014 IEEE Workshop on Signal Processing Systems (SiPS). Belfast: IEEE, 2014. 1–6. [doi: 10.1109/SiPS.2014.6986091]

[35] Kim K, Kim TH, Kim T, Ryu S. Black Hat Asia—AES wireless keyboard: Template attack for eavesdropping. 2018. https://i.blackhat.com/briefings/asia/2018/asia-18-Kim-AES-Wireless-Keyboard-Template-Attack-for-Eavesdropping.pdf

[36] Wang W, Zhang MH, Chen G, Jagadish HV, Ooi BC, Tan KL. Database meets deep learning: Challenges and Opportunities. ACM SIGMOD Record, 2016, 45(2): 17–22. [doi: 10.1145/3003665.3003669]

[37] van der Valk D, Picek S, Bhasin S. Kilroy was here: The first step towards explainability of neural networks in profiled side-channel analysis. In: Bertoni GM, Regazzoni F, eds. Proc. of the 11th Int'l Workshop on Constructive Side-channel Analysis and Secure Design. Lugano: Springer, 2021. 175–199. [doi: 10.1007/978-3-030-68773-1_9]

[38] Das D, Golder A, Danial J, Ghosh S, Raychowdhury A, Sen S. X-DeepSCA: Cross-device deep learning side channel attack. In: Proc. of the 56th Annual Design Automation Conf. Las Vegas: ACM, 2019. 134. [doi: 10.1145/3316781.3317934]

[39] Carbone M, Conin V, Cornélie MA, Dassance F, Dufresne G, Dumas C, Prouff E, Venelli A. Deep learning to evaluate secure RSA implementations. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2019, 2: 132–161. [doi: 10.13154/tches.v2019.i2.132-161]

[40] Wouters L, Van den Herrewegen J, Garcia FD, Oswald D, Gierlichs B, Preneel B. Dismantling DST80-based immobiliser systems. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2020, 2: 99–127. [doi: 10.13154/tches.v2020.i2.99-127]

[41] Wang A, Ge J, Zhang 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]

[42] Wu WB, Liu Z, Yang H, Zhang JP. Survey of side-channel attacks and countermeasures on post-quantum cryptography. Ruan Jian Xue Bao/Journal of Software, 2021, 32(4): 1165–1185 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6165.htm [doi: 10.13328/j.cnki.jos.006165]

[43] Wang YJ, Fan HP, Dai ZY, Yuan QJ, Wang XB. Advances in side channel attacks and countermeasures. Chinese Journal of Computers, 2023, 46(1): 202–228 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2023.00202]

[44] Picek S, Perin G, Mariot L, Wu LC, Batina L. SoK: Deep learning-based physical side-channel analysis. ACM Computing Surveys, 2023, 55(11): 227. [doi: 10.1145/3569577]

[45] Bhasin S, Chattopadhyay A, Heuser A, Jap D, Picek S, Shrivastwa RR. Mind the portability: A warriors guide through realistic profiled side-channel analysis. In: Proc. of the 2020 Network and Distributed System Security (NDSS) Symp. San Diego, 2020. 1–14. [doi: 10.14722/ndss.2020.24390]

[46] Zhang F, Shao B, Xu GR, Yang BL, Yang ZQ, Qin Z, Ren K. From homogeneous to heterogeneous: Leveraging deep learning based power analysis across devices. In: Proc. of the 57th ACM/EDAC/IEEE Design Automation Conf. San Francisco: IEEE, 2020. 1–6. [doi: 10.1109/DAC18072.2020.9218693]

[47] Cao P, Zhang C, Lu XJ, Gu DW. Cross-device profiled side-channel attack with unsupervised domain adaptation. IACR Trans. on

Cryptographic Hardware and Embedded Systems, 2021, 4: 27–56. [doi: 10.46586/tches.v2021.i4.27-56]

[48] Choudary O, Kuhn MG. Template attacks on different devices. In: Prouff E, ed. Proc. of the 5th Int'l Workshop on Constructive Side-channel Analysis and Secure Design. Paris: Springer, 2014. 179–198. [doi: 10.1007/978-3-319-10175-0_13]

[49] Choudary MO, Kuhn MG. Efficient, portable template attacks. IEEE Trans. on Information Forensics and Security, 2018, 13(2): 490–501. [doi: 10.1109/tifs.2017.2757440]

[50] Wang HY, Brisfors M, Forsmark S, Dubrova E. How diversity affects deep-learning side-channel attacks. In: Proc. of the 2019 IEEE Nordic Circuits and Systems Conf. (NORCAS): NORCHIP and Int'l Symp. of System-on-chip (SoC). Helsinki: IEEE, 2019. 1–7. [doi: 10.1109/NORCHIP.2019.8906945]

[51] Wu LC, Picek S. Remove some noise: On pre-processing of side-channel measurements with autoencoders. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2020, 4: 389–415. [doi: 10.13154/tches.v2020.i4.389-415]

[52] Yu HG, Wang M, Song XY, Shan HQ, Qiu HB, Wang JY, Yang KC. Noise2Clean: Cross-device side-channel traces denoising with unsupervised deep learning. Electronics, 2023, 12(4): 1054. [doi: 10.3390/electronics12041054]

[53] Wu LC, Won YS, Jap D, Perin G, Bhasin S, Picek S. Ablation analysis for multi-device deep learning-based physical side-channel analysis. IEEE Trans. on Dependable and Secure Computing, 2024, 21(3): 1331–1341. [doi: 10.1109/tdsc.2023.3278857]

[54] Paguada S, Batina L, Buhan I, Armendariz I. Playing with blocks: Toward re-usable deep learning models for side-channel profiled attacks. IEEE Trans. on Information Forensics and Security, 2022, 17: 2835–2847. [doi: 10.1109/tifs.2022.3196273]

[55] Rioja U, Batina L, Flores JL, Armendariz I. Auto-tune POIs: Estimation of distribution algorithms for efficient side-channel analysis. Computer Networks, 2021, 198: 108405. [doi: 10.1016/j.comnet.2021.108405]

[56] Thapar D, Alam M, Mukhopadhyay D. Transca: Cross-family profiled side-channel attacks using transfer learning on deep neural networks. Cryptology ePrint Archive, Paper 2020/1258, 2020.

[57] Liskov M, Rivest RL, Wagner D. Tweakable block ciphers. Journal of Cryptology, 2011, 24: 588–613. [doi: 10.1007/3-540-45708-9_3]

[58] Liu JJ, Sun B, Liu GQ, Dong XF, Liu L, Zhang H, Li C. New wine old bottles: Feistel structure revised. IEEE Trans. on Information Theory, 2023, 69(3): 2000–2008. [doi: 10.1109/tit.2022.3223139]

[59] Yu HG, Shan HQ, Panoff M, Jin YE. Cross-device profiled side-channel attacks using meta-transfer learning. In: Proc. of the 58th ACM/IEEE Design Automation Conf. (DAC). San Francisco: IEEE, 2021. 703–708. [doi: 10.1109/DAC18074.2021.9586100]

[60] Gohr A, Jacob S, Schindler W. CHES 2018 side channel contest CTF-solution of the AES challenges. Cryptology ePrint Archive, Paper 2019/094, 2019.

[61] Wang CG, Ninan M, Reilly S, Ward J, Hawkins W, Wang BY, Emmert JM. Portability of deep-learning side-channel attacks against software discrepancies. In: Proc. of the 16th ACM Conf. on Security and Privacy in Wireless and Mobile Networks. Guildford: ACM, 2023. 227–238. [doi: 10.1145/3558482.3590177]

[62] Seckiner S, Kose S. Preprocessing of the physical leakage information to combine side-channel distinguishers. IEEE Trans. on Very Large Scale Integration (VLSI) Systems, 2021, 29(12): 2052–2063. [doi: 10.1109/tvlsi.2021.3115420]

[63] Souissi Y, Nassar M, Guilley S, Danger JL, Flament F. First principal components analysis: A new side channel distinguisher. In: Rhee KH, Nyang D, eds. Proc. of the 13th Int'l Conf. on Information Security and Cryptology. Seoul: Springer, 2011. 407–419. [doi: 10.1007/978-3-642-24209-0_27]

[64] Mahmudlu R, Banciu V, Batina L, Buhan I. LDA-based clustering as a side-channel distinguisher. In: Hancke G, Markantonakis K, eds. Proc. of the 12th Int'l Workshop on Radio Frequency Identification and IoT Security. Hong Kong: Springer, 2017. 62–75. [doi: 10.1007/978-3-319-62024-4_5]

[65] Kizhvatov I. Side channel analysis of AVR XMEGA crypto engine. In: Proc. of the 4th Workshop on Embedded Systems Security. Grenoble: ACM, 2009. 8. [doi: 10.1145/1631716.1631724]

[66] Danial J, Das D, Golder A, Ghosh S, Raychowdhury A, Sen S. EM-X-DL: Efficient cross-device deep learning side-channel attack with noisy EM signatures. ACM Journal on Emerging Technologies in Computing Systems, 2021, 18(1): 4. [doi: 10.1145/3465380]

[67] Won YS, Hou XL, Jap D, Breier J, Bhasin S. Back to the basics: Seamless integration of side-channel pre-processing in deep neural networks. IEEE Trans. on Information Forensics and Security, 2021, 16: 3215–3227. [doi: 10.1109/tifs.2021.3076928]

[68] Ngo K, Dubrova E. Side-channel analysis of the random number generator in STM32 MCUs. In: Proc. of the 2022 Great Lakes Symp. on VLSI 2022. Irvine: ACM, 2022. 15–20. [doi: 10.1145/3526241.3530324]

[69] Le TH, Clédière J, Serviere C, Lacoume JL. Noise reduction in side channel attack using fourth-order cumulant. IEEE Trans. on Information Forensics and Security, 2007, 2(4): 710–720. [doi: 10.1109/TIFS.2007.910252]

[70] Coron JS, Kizhvatov I. Analysis and improvement of the random delay countermeasure of CHES 2009. In: Mangard S, Standaert FX, eds. Proc. of the 12th Int'l Workshop on Cryptographic Hardware and Embedded Systems. Santa Barbara: Springer, 2010. 95–109. [doi: 10.

1007/978-3-642-15031-9_7]
[71] Veyrat-Charvillon N, Medwed M, Kerckhof S, Standaert FX. Shuffling against side-channel attacks: A comprehensive study with cautionary note. In: Proc. of the 2012 Int'l Conf. on the Theory and Application of Cryptology and Information Security. Beijing: Springer, 2012. 740–757. [doi: 10.1007/978-3-642-34961-4_44]
[72] Wolf S, Hu H, Cooley R, Borowczak M. Stealing machine learning parameters via side channel power attacks. In: Proc. of the 2021 IEEE Computer Society Annual Symp. on VLSI (ISVLSI). Tampa: IEEE, 2021. 242–247. [doi: 10.1109/ISVLSI51109.2021.00052]
[73] Mateos E, Gebotys CH. A new correlation frequency analysis of the side channel. In: Proc. of the 5th Workshop on Embedded Systems Security. Scottsdale: ACM, 2010. 4. [doi: 10.1145/1873548.1873552]
[74] Golder A, Das D, Danial J, Ghosh S, Sen S, Raychowdhury A. Practical approaches toward deep-learning-based cross-device power side-channel attack. IEEE Trans. on Very Large Scale Integration (VLSI) Systems, 2019, 27(12): 2720–2733. [doi: 10.1109/tvlsi.2019.2926324]
[75] Rioja U, Batina L, Armendariz I. When similarities among devices are taken for granted: Another look at portability. In: Proc. of the 2020 Int'l Conf. on Cryptology in Africa. Cairo: Springer, 2020. 337–357. [doi: 10.1007/978-3-030-51938-4_17]
[76] Sudhan RH, Kumar MG, Prakash AU, Devi SAR, Sathiya P. Arduino ATMega-328 microcontroller. Int'l Journal of Innovative research in Electrical, Electronics, Instrumentation and Control Engineering, 2015, 3(4): 27–29. [doi: 10.17148/ijireeice.2015.3406]
[77] Weiss K, Khoshgoftaar TM, Wang DD. A survey of transfer learning. Journal of Big Data, 2016, 3(1): 9. [doi: 10.1186/s40537-016-0043-6]
[78] Wang P, Chen P, Luo ZM, Dong GF, Zheng MC, Yu NH, Hu HG. Enhancing the performance of practical profiling side-channel attacks using conditional generative adversarial networks. Cryptology ePrint Archive, Paper 2020/867, 2020. https://eprint.iacr.org/2020/867
[79] Li D, Li L, Ou Y. Side-channel analysis based on Siamese neural network. The Journal of Supercomputing, 2024, 80(4): 4423–4450. [doi: 10.1007/s11227-023-05631-3]
[80] Mukhtar N, Batina L, Picek S, Kong Y. Fake it till you make it: Data augmentation using generative adversarial networks for all the crypto you need on small devices. In: Proc. of the 2022 Cryptographers' Track at the RSA Conf. Springer, 2022. 297–321. [doi: 10.1007/978-3-030-95312-6_13]
[81] Ito A, Saito K, Ueno R, Homma N. Imbalanced data problems in deep learning-based side-channel attacks: Analysis and solution. IEEE Trans. on Information Forensics and Security, 2021, 16: 3790–3802. [doi: 10.1109/tifs.2021.3092050]
[82] Picek S, Heuser A, Perin G, Guilley S. Profiled side-channel analysis in the efficient attacker framework. In: Grosso V, Pöppelmann T, eds. Proc. of the 20th Int'l Conf. on Smart Card Research and Advanced Applications. Lübeck: Springer, 2022. 44–63. [doi: 10.1007/978-3-030-97348-3_3]
[83] Genevey-Metat C, Heuser A, Gérard B. Train or adapt a deeply learned profile? In: Proc. of the 2021 Int'l Conf. on Cryptology and Information Security in Latin America. Bogotá: Springer, 2021. 213–232. [doi: 10.1007/978-3-030-88238-9_11]
[84] Jia XD, Zhao M, Di Y, Yang QB, Lee J. Assessment of data suitability for machine prognosis using maximum mean discrepancy. IEEE Trans. on Industrial Electronics, 2018, 65(7): 5872–5881. [doi: 10.1109/tie.2017.2777383]
[85] Guntur H, Ishii J, Satoh A. Side-channel attack user reference architecture board SAKURA-G. In: Proc. of the 3rd IEEE Global Conf. on Consumer Electronics (GCCE). Tokyo: IEEE, 2014. 271–274. [doi: 10.1109/GCCE.2014.7031104]
[86] Cao P, Zhang HY, Gu DW, Lu Y, Yuan YD. AL-PA: Cross-device profiled side-channel attack using adversarial learning. In: Proc. of the 59th ACM/IEEE Design Automation Conf. San Francisco: ACM, 2022. 691–696. [doi: 10.1145/3489517.3530517]

附中文参考文献

[41] 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]
[42] 吴伟彬, 刘哲, 杨昊, 张吉鹏. 后量子密码算法的侧信道攻击与防御综述. 软件学报, 2021, 32(4): 1165–1185. http://www.jos.org.cn/1000-9825/6165.htm [doi: 10.13328/j.cnki.jos.006165]
[43] 王永娟, 樊昊鹏, 代政一, 袁庆军, 王相宾. 侧信道攻击与防御技术研究进展. 计算机学报, 2023, 46(1): 202–228. [doi: 10.11897/SP.J.1016.2023.00202]

作者简介

李迪, 博士生, CCF 学生会员, 主要研究领域为密码芯片功耗攻击与防御.
张裕鹏, 硕士, 主要研究领域为密码学应用.
汤宇锋, 博士, 主要研究领域为白盒密码的设计及其侧信道分析.
龚征, 博士, 教授, 主要研究领域为对称密码算法的设计与分析.