

多源融合信息泄漏检测方法

曹雨晨^{1,2}, 周永彬^{1,2*}

¹中国科学院信息工程研究所信息安全国家重点实验室 北京 中国 100093

²中国科学院大学网络空间安全学院 北京 中国 100049

摘要 密码设备的侧信息泄漏检测是侧信道分析中的重要技术环节,旨在客观地评估密码设备的物理安全性。不同类型的侧信息在密码设备运行过程中同时存在,仅仅从单源侧信息的视角进行信息泄漏检测难以全面反映密码设备的真实泄漏威胁情况。因此,发展基于多源侧信息的融合信息泄漏检测方法,建立综合利用多源侧信息的信息泄漏检测方法体系,以期实现对密码设备物理安全性更全面、更客观地评估,是一种现实技术需求。本文基于如何融合利用多个信道的侧信息提出了3种多源融合信息泄漏检测方案:多源简单融合信息泄漏检测、多源时频融合信息泄漏检测以及基于多元 T 检验的多源信息泄漏检测。其中,多源简单融合信息泄漏检测在时域上组合利用多个信道的侧信息;多源时频融合信息泄漏检测综合利用了多个信道侧信息的时域信息及频域信息;基于多元 T 检验的多源信息泄漏检测基于多元假设检验方案构造。对比单源的信息泄漏检测方案,模拟实验和真实实验结果表明本文提出的多源融合信息泄漏检测方案可以降低检测出泄漏所需的侧信息数量,提高泄漏检测的效率。

关键词 信息泄漏;多源融合;信息泄漏检测

中图分类号 TP309.2 DOI号 10.19363/J.cnki.cn10-1380/tn.2020.11.04

Multi-Channel Fusion Leakage Detection

CAO Yuchen^{1,2}, ZHOU Yongbin^{1,2*}

¹State Key Laboratory Of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

²University of Chinese Academy of Sciences, Beijing 100049, China

Abstract Leakage detection is an important part of side channel analysis, which can objectively evaluate the security of cryptographic devices. Different types of side channel exist simultaneously during the running of cryptographic devices, so leakage detection against mono-channel cannot give a fully evaluation about the security of cryptographic devices. The development of multi-channel fusion leakage detection which can achieve a more comprehensive and objective evaluation is a very urgent practical technology choice. In this paper, we propose 3 multi-channel fusion leakage detection methods based on how to utilize the side information of multi-channels. The multi-channel simple fusion leakage detection combine data of multi-channel in time domain. The multi-channel time-frequency fusion leakage detection uses the time domain information and frequency domain information on multi-channel. And the multi-channel leakage detection based on multivariate hypothesis testing technology. Simulated and practical experimental results show that the multi-channel fusion leakage detection methods proposed in this paper can reduce the number of side-channel leakage discovering leakages.

Key words information leakage; multi-Channel fusion; leakage detection

1 引言

侧信道分析(Side-Channel Analysis, SCA)是“攻击者通过密码算法执行过程中产生的额外信息泄漏对密码算法实现进行破解的攻击方式”^[1]。密码设备在运行过程中,由于自身运行环境、实现的密码算法以及当前运行状态等因素的影响,通常会呈现出某些特定的物理特征。这些特定的物理特征称之为“侧信息”。侧信息与密码设备执行算法时执行的操作以

及处理的数据相关。SCA就是一种利用侧信息与密码设备内部状态间的关联性来恢复密码设备秘密信息的密码分析手段。Kocher^[2]在1996年首次提出并成功实施计时攻击,此后学术界和产业界给予了SCA极大的关注。截至目前,已公开证实能够成功用于SCA的侧信息种类有十余种,包括密码设备的执行时间^[2]、能量消耗^[3]、电磁辐射^[4]、音频特征^[5]以及光谱特性^[6]等等。实际上,随着SCA技术的发展,完全可以预测将会有更多其他形式的侧信息被发现

通讯作者:周永彬,博士,研究员,Email:zhouyongbin@iie.ac.cn。

本课题得到国家自然科学基金(No.61632020, No. 61472416, No. 61602468)资助。

收稿日期:2018-12-27;修改日期:2019-02-15;定稿日期:2020-09-22

和利用。

与传统密码分析学将密码算法看作黑盒模型不同, SCA 场景下, 攻击者除了可以获得密码算法的输入与输出之外, 还可以采集到密码设备运行过程中与密码设备内部状态相关的侧信息。由于获取了密码设备执行过程中的中间数据, SCA 可利用的信息更多, 具有更强的分析能力。相比于传统密码分析, 后者刻画了密码设备在实际应用中的物理安全性。例如, 在传统密码分析中很难攻破的 AES-128 密码算法, 若以无保护的形式实现在微处理器上, 仅需 20 条能量迹就可以通过 SCA 得出正确密钥^[7], 整个能量迹采集以及 SCA 过程不会超过 5min。不难看出, SCA 颠覆了仅考虑密码算法数学安全性的传统, 给密码设备在实际中的安全使用带来了极大的威胁。因此实际应用中密码设备需要具备抵抗 SCA 的能力, 两大安全认证标准: 联邦信息处理标准(Federal Information Processing Standards, FIPS)以及通用准则(Common Criteria, CC)均强调了这一点。为了对密码设备抵抗 SCA 的能力进行刻画评估, 需要相应的信息泄漏检测方案。学术界及产业界现有的信息泄漏检测方案可以分为两种不同类型: 攻击依赖型检测(Evaluation-Style Testing)以及一致性检测(Conformance-Style Testing)。下面对这两种检测类型分别进行说明。

1.1 攻击依赖型检测

攻击依赖型检测^[8-11]基于实际 SCA 的结果对密码设备的抗 SCA 能力进行评估。CC 提出的检测标准^[12](ISO-15408)是典型的攻击依赖型检测。从检测信息泄漏的角度看, ISO-15408 要求利用多种 SCA 方法对密码设备进行分析(包括但不限于简单能量分析(Simple Power Analysis, SPA)、差分能量分析(Differential Power Analysis, DPA)、电磁分析(Electromagnetic Analysis, EMA)以及高阶差分能量分析(Higher-order Differential Power Analysis,)等), 并依据分析结果评估密码设备的物理安全性。利用攻击依赖型检测得出的结果直观, 但存在以下两点不足: 1)需要利用多种攻击方案进行攻击, 检测时间长; 2)利用的攻击方案有限, 检测给出的结果有条件限制, 结果不全面。

1.2 一致性检测

与 CC 不同, FIPS 的 1403 草案中提出一种典型的检测密码模块是否达到了必要的安全水平的一致性检测方案^[13]。这一类检测方法不依赖于 SCA 攻击方案以及具体的泄漏模型, 通过评估密码设备的实际信息泄漏量, 完成对密码设备物理安全性的评估。

2011 年美国国际标准技术研究院(National Institute of Standards and Technology, NIST)举办的 NIAT 研讨会上提出的测试向量泄漏评估方案(Test Vector Leakage assessment Methodology, TVLA)^[14-16]是一种典型的一致性检测, 也是目前泄漏检测领域的研究热点。

TVLA 基于学生 t 检验, 是一种 PASS / FAIL 测试, 通过比较密码设备在不同输入下侧信息的均值是否不同来检测是否存在信息泄漏。通常通过计算同一密码设备上利用同样采样参数分别采集的两组侧信息(一组侧信息具有固定密钥和固定明文, 另一组侧信息具有固定密钥和随机明文)在同一采样时刻的 t 值来进行泄漏检测。如果 t 值超过阈值(建议为 ± 4.5 ^[14]), 则认为测量结果包含数据依赖信息, 存在信息泄漏, 可能会被攻击者利用。反之, 则认为侧信息中不存在信息泄漏。这种测试的主要优点在于: 一方面只需要比较少量几组侧信息就可以完成检测, 降低了信息泄漏检测的耗时; 另一方面检测结果与分析方法无关, 检测结果客观全面。

TVLA 在学术界获得了极大的关注, 多项相关工作研究了 TVLA 在不同场景下的有效性。Mather 等人^[17]比较了 TVLA 与互信息(Mutual Information, MI)的检测效果及计算复杂性, 分析结果表明 TVLA 在大多数情况下优于 MI。Schneider 和 Moradi 等^[18]从高阶侧信息泄漏、多维侧信息泄漏、以及快速评估等角度对 TVLA 进行了深入的研究; Durvaux 等^[19]评估了 TVLA 检测泄漏点的有效性; Moradi 等^[20]利用 TVLA 对门限密码实现的高阶侧信息泄漏特征进行了评估。

为了提高 TVLA 的实用性及检测准确性, 学术界也有多项改进工作。Ding 等^[21]的相关工作指出, 由于侧信息中通常包含多个采样点, 若采用阈值 ± 4.5 进行是否有泄漏的判断, 可能会造成漏报, 他们提出了一种优化的 TVLA 阈值计算方案, 提高了对多点进行泄漏检测成功的概率。Durvaux 等人^[22]指出由于利用 TVLA 进行泄漏检测与具体攻击方案无关, 会检测出无法转化为有效攻击的泄漏点, 为解决这一问题 Durvaux 等提出了一种基于相关系数的 TVLA 方案, 使得检测出的泄漏点与选定的敏感中间值相关。Reparaz 等人^[23]基于示波器采样数据的特点, 提出了一种数据分块存储计算的 TVLA 快速计算方案, 大幅降低了 TVLA 数据存储空间并提高了计算效率。在进行高阶泄漏检测时, TVLA 需要对多个阶段的数据进行检测, 效率不高, 基于此, Moradi 等人^[24]提出了一种基于皮尔逊卡方检验的泄漏检测方法, 在进行高阶泄漏检测时, 基于皮尔逊卡方检验的泄漏检测方法与

TVLA 具有互补性, 联合两种检测方法进行泄漏检测可以大幅提高泄漏检测的效率。

需要注意的是, 以上提到的相关工作都是基于单个信道的侧信息进行信息泄漏检测的。然而, 不同类型的侧信息在密码设备运行过程中同时存在, 密码设备信息泄漏检测若仅从单个信道的视角进行难以全面反映密码设备的真实泄漏威胁情况。这种情况下, 发展基于多个信道的信息泄漏检测技术, 建立多源融合泄漏检测方法体系, 以期实现对密码设备物理安全性更全面、更客观的评估, 是一种现实技术选择。一方面, 基于多源融合的信息泄漏检测技术的研究有利于发现单信道信息泄漏检测中可能检测不出的泄漏; 另一方面, 基于多源融合的信息泄漏检测技术由于利用了多个信道的信息, 有可能会极大的降低泄漏检测所需的侧信息数量, 从而提高泄漏检测的效率和实用性。

面对建立多源信息泄漏检测的迫切需求, 本文基于如何融合利用多个信道的侧信息并提高信息利用率提出了 3 种多源融合信息泄漏检测方案: 多源简单融合信息泄漏检测, 多源时频融合信息泄漏检测以及基于多元 T 检验的多源信息泄漏检测。其中, 多源简单融合信息泄漏检测组合利用不同信道侧信息的时域信息, 是一种最直观的多源融合信息泄漏检测方案, 直观易实施, 本文的模拟实验和真实实验表明在被融合的信道具有相似的信噪比及泄漏函数的前提条件下, 该方案可以降低进行信息泄漏检测所需的侧信息数量; 多源时频融合信息泄漏检测综合利用了不同信道侧信息的时域信息及频域信息, 该方案有效的前提条件是被融合的信道具有相似的频谱分布; 基于多元 T 检验的多源信息泄漏检测基于多元假设检验构造, 具有成熟的理论基础, 在本文的多种实验场景下均可以大幅降低检测出泄漏所需的侧信息数量(本文模拟实验场景下, 最高可降至单信道信息泄漏检测所需侧信息数量的 43%), 提高信息泄漏检测的效率。

本文的主要结构如下: 第 2 章描述相关背景知识; 具体方案的构造在第 3 章中给出; 第 4 章利用模拟实验及真实实验验证了方案的性能; 最后一章总结全文。

2 背景知识

2.1 信息泄漏模型

密码设备的能量消耗以及电磁泄漏是两种常用的侧信息类型, 二者具有相似的泄漏模型, 见公式 1。其中, $\Psi(p, k)$ 是与明文 p (或密文)以及秘密信息 k

相关的敏感中间值。在实际分析中, 采集的侧信息通常包含很多测量点, 每条侧信息中包含的测量点数用 m 表示。这 m 个测量点中, 与敏感中间值相关的测量点称为特征点(Points of Interest, POI)。 L 表示特征点的侧信息。例如, 对于 AES 的物理实现来说, $\Psi(p, k)$ 可以取第一轮 S 盒的输出或最后一轮 S 盒的输入。函数 f 是敏感中间值到信息泄漏的转换函数, 常用的转换函数有汉明重量(Hamming Weight, HW)以及汉明距离(Hamming Distance, HD)等。 a 是常数系数, σ 是随机噪声, a, σ 以及函数 f 的选取均与具体的密码设备相关。

$$L = a * f(\Psi(p, k)) + \sigma \quad (1)$$

在公式(1)的泄漏模型假设下, 密码设备在特征点的信噪比(Signal-to-Noise Ratio, SNR)可以通过公式(2)计算, 其中 $Var(x)$ 表示变量 x 的方差。

$$SNR = \frac{a^2 * Var(f(\Psi(p, k)))}{Var(\sigma)} \quad (2)$$

2.2 TVLA

Goodwill 等^[14]基于学生 t 检验(Student T-test)提出了 TVLA 信息泄漏检测方案。学生 t 检验^[25]是用 t 分布理论来推论两组数据的均值有差异发生的概率, 从而比较两组数据的均值差异是否显著的假设检验。当侧信息中没有信息泄漏时, 侧信息的均值与密码设备中处理的数据无关; 反之, 侧信息的均值与密码设备中处理的数据相关。文献[14]提出了两种 TVLA: 特异型 TVLA(Specific TVLA)和非特异型 TVLA(Non-Specific TVLA)。二者的区别在于特异型 TVLA 的两组数据具有不同的假设泄漏(利用公式 $f(\Psi(p, k))$ 计算), 而非特异型 TVLA 的两组数据具有不同的明文。特异型 TVLA 需要有待测密码设备(Device Under Test, DUT)的先验知识, 若检测有泄漏, 该泄漏必定与选定的敏感中间值相关。非特异型 TVLA 又可以细分为两种形式: 1)一组数据具有随机明文固定密钥, 另一组数据具有固定明文固定密钥(Fixed-vs-Random TVLA); 2)两组数据均具有固定明文固定密钥, 但所选明文不同(Fixed-vs-Fixed TVLA)。利用非特异型 TVLA 进行检验时, 存在固定明文固定密钥产生的可能的假设泄漏与随机明文固定密钥产生的可能假设泄漏相同的场景, 因此需要检测多组数据(为了便于讨论, 本文不考虑这种场景)。利用 Fixed-vs-Random TVLA 对 DUT 进行检测的步骤是:

1) 对 DUT 采集 L_A 和 L_B 两组样本, 其中 L_A 是一组基于随机(均匀分布)明文及固定密钥的侧信息, L_B 是一组基于固定明文及固定密钥的侧信息。二者均为 $n * m$ 的矩阵, n 为侧信息数目, m 为每条侧信息包

含的采样点数量;

2) 建立假设 H_0 及备择假设 H_1 :

H_0 : 密码设备没有泄漏, 则 L_A 和 L_B 与明文密钥无关, 二者均值相等;

H_1 : 密码设备有泄漏, L_A 和 L_B 的均值不等;

3) 计算 t 值及自由度, 见公式(3)。其中, \bar{L}_A 是 L_A 的均值, S_A^2 是 L_A 的方差; \bar{L}_B 是 L_B 的均值, S_B^2 是 L_B 的方差。

$$t_u = \sqrt{\frac{n}{S_A^2 + S_B^2}} * (\bar{L}_A - \bar{L}_B) \quad (3)$$

$$v = (n-1) * \frac{(S_A^2 + S_B^2)^2}{(S_A^2)^2 + (S_B^2)^2}$$

4) 如果 $|t_u| \geq 4.5$, 则拒绝假设 H_0 , 认为存在信息泄漏。若否, 则接受 H_0 , L_A 和 L_B 来自于同一分布, 二者对应时刻的侧信息与 DUT 中运行的数据无关, 尚无证据支持侧信息中存在信息泄漏。

2.3 时频分析

时频分析的基本思想是: 设计一个时间和频率的联合函数, 该函数描述了信号在不同时间和频率的强弱, 提供了时间域和频率域的联合分布信息。本文利用短时傅里叶变换(Short-time Fourier Transform, STFT)^[26]来得到侧信息的时频联合信息。

STFT 是一种时频分析的常用方法, 它基于傅里叶变换, 利用一个滑动窗口, 可以确定信号局部频率。简单来说, 短时傅里叶变换就是先把一个函数和窗函数进行相乘, 然后再进行一维的傅里叶变换。并通过窗函数的滑动得到一系列的傅里叶变化结果, 将这些结果排开便得到一个二维的表象。离散短时傅里叶变换^[26]如公式(4)所示。

$$STFT[x[n]](m, \omega) = \sum_{n=-\infty}^{\infty} x[n] * w[n-m]e^{-j\omega n} \quad (4)$$

3 多源信息泄漏检测

对密码设备的两个信道 M_1 和 M_2 分别同时采集两组侧信息(可扩展至多个信道, 其中 M_1 和 M_2 可以选择能量消耗或电磁泄漏), M_1 上采集的两组侧信息记为 L_{A1} 和 L_{B1} , M_2 上采集的两组侧信息记为 L_{A2} 和 L_{B2} 。其中, L_{A1} 和 L_{A2} 基于一组随机明文(均匀分布)和固定密钥同时采集; L_{B1} 和 L_{B2} 基于一组固定明文和固定密钥同时采集。 L_{A1} , L_{A2} , L_{B1} 以及 L_{B2} 都是 $n*m$ 的矩阵, 其中 n 表示每组侧信息均有 n 条侧信息数据, 每条侧信息包含 m 个采样数据点。当两个信道具有相似的泄漏模型时(如能量迹与电磁迹), 两信道的泄

漏函数记为 L_1 和 L_2 , 如公式(5)。

$$L_1 = a_1 * f(\Psi(p, k)) + \sigma_1$$

$$L_2 = a_2 * f(\Psi(p, k)) + \sigma_2 \quad (5)$$

对多源信息进行信息泄漏检测, 有三种策略:

策略一: 分别对多源侧信息进行 TVLA 检验, 将检测结果融合得出最终的信息泄漏检测结果;

策略二: 将多源侧信息融合得到一组新的侧信息, 针对这一组新的侧信息进行 TVLA 检验;

策略三: 提出新的检测方法, 直接对多源侧信息进行泄漏检测。

其中, 利用**策略一**进行侧信息泄漏检测可能会存在以下三种问题:

1) 需要对每个信道的侧信息分别进行 TVLA 检验, 增加了犯 I 型错误(误报, 认为实际上没有泄漏的侧信息有泄漏)的概率;

2) 对每个信道分别进行 TVLA 检验, 忽略了各个信道侧信息泄漏间的相互联系;

3) 当对各信道进行 TVLA 检验的结果不一致时, 难以下一个综合的结论。

因此, 本文基于**策略二**和**策略三**建立多源信息泄漏进行检测方案。

3.1 多源简单融合信息泄漏检测

多源简单融合信息泄漏检测是基于**策略二**提出的一种多源融合信息泄漏检测方案。在多源简单融合信息泄漏检测中, 将 L_{A1} 和 L_{A2} 用函数 h 组合起来构成一组新的泄漏 L_A , 即 $L_A = h(L_{A1}, L_{A2})$, 将 L_{B1} 和 L_{B2} 用相同的函数 h 组合起来构成一组新的泄漏 L_B , 即 $L_B = h(L_{B1}, L_{B2})$ 。其中, 函数 h 可以选则使融合后的侧信息仍然满足正态分布的算法, 本文选择加法和带权重的加法进行对比分析。该方法要求不同信道对应同一敏感中间值的侧信息泄漏在时域上对齐, 否则对融合得到的多源侧信息进行信息泄漏检测可能会降低信息泄漏检测的准确性。

算法 1. 多源简单融合信息泄漏检测

输入: 能量消耗 L_{A1} 和 L_{B1} , 电磁泄漏 L_{A2} 和 L_{B2}

输出: 是否有泄漏

1: 将 L_{A1} 和 L_{A2} 组合计算得到一组新的基于随机明文的侧信息 $L_A = h(L_{A1}, L_{A2})$;

2: 将 L_{B1} 和 L_{B2} 组合计算得到一组新的基于固定明文的侧信息 $L_B = h(L_{B1}, L_{B2})$;

3: 利用 TVLA 对 L_A 和 L_B 进行检测计算得到 t_u ;

4: 比较 $|t_u|$ 与阈值 4.5, 返回是否有泄漏。

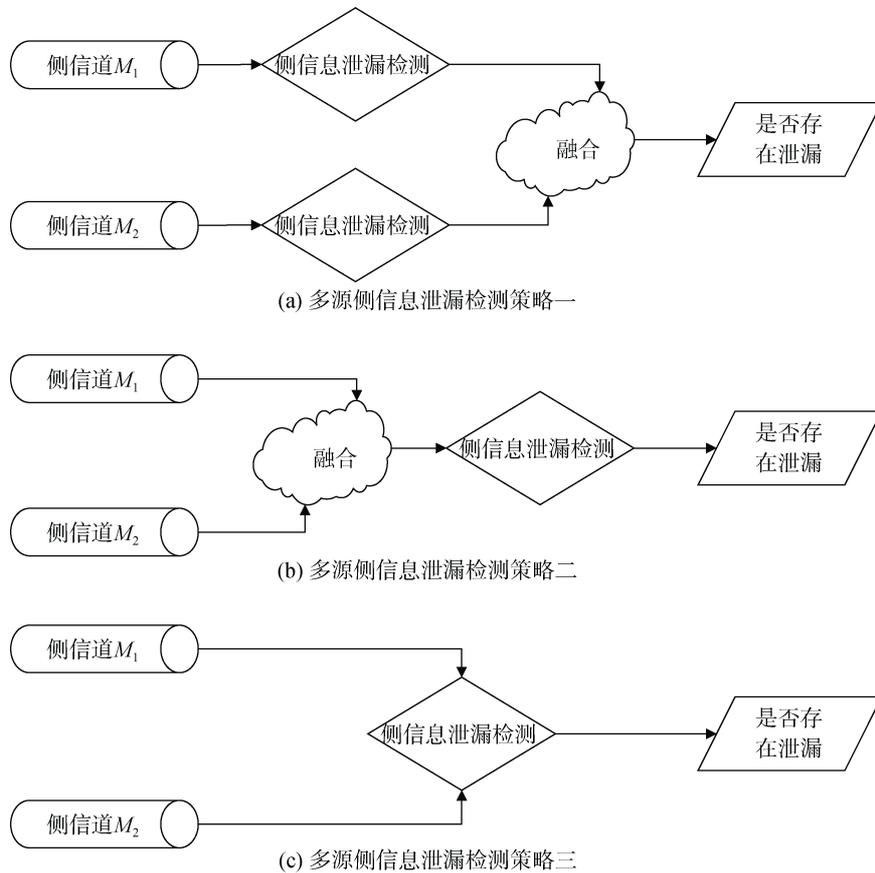


图 1 多源侧信息泄漏检测三种不同策略

Figure 1 Three Strategies of multi-channel fusion leakage detection methods

下面以 h 为加法函数来说明该方案的正确性:

假设信道 M_1 和 M_2 的泄漏模型分别为 $L_{M1} = a_1 * f(p, k) + \sigma_1$, $L_{M2} = a_2 * l(p, k) + \sigma_2$, 则将 M_1 与 M_2 信道利用加法函数 h 组合后可以得到 $L = a_1 * f(p, k) + a_2 * l(p, k) + \sigma_1 + \sigma_2$, L 符合高斯分布。当不存在侧信息泄漏, 即 $L_{A1}, L_{A2}, L_{B1}, L_{B2}$ 均与 DUT 中运行的数据无关时, $L_{A1}, L_{A2}, L_{B1}, L_{B2}$ 两两相互独立, L_{A1} 与 L_{B1} 同分布, L_{A2} 与 L_{B2} 同分布时, 因此 $L_{A1} + L_{A2}$ 与 $L_{B1} + L_{B2}$ 同分布, 此时利用 TVLA 对 L_A 和 L_B 检测同样检测不出信息泄漏。当存在侧信息泄漏, 即 $L_{A1}, L_{A2}, L_{B1}, L_{B2}$ 均与 DUT 中运行的数据有关时, L_A 与 L_B 具有不同的分布, 此时利用 TVLA 对 L_A 和 L_B 检测可以检测出信息泄漏。

3.2 多源时频融合信息泄漏检测

多源时频融合信息泄漏检测需要待融合的侧信道具有相似的假设形式, 如能量消耗以及电磁泄漏。根据公式 3 对含有泄漏 l 以及噪声 σ 的侧信息进行短

时傅里叶变换, 变换后可得公式(6)。

$$STFT(l + \sigma) = STFT(l) + STFT(\sigma) \quad (6)$$

能量或电磁侧信息中的泄漏 l 部分是由电路中数据或操作的变化引起的, 而噪声 σ 部分是由于环境、元器件间的相互影响以及元器件自身的特性引起的。由于产生原因不同, l 和 σ 的频率组成差异较大。因此, 对侧信息进行 STFT 变换后, 时频图中泄漏 l 与噪声 σ 分布在不同的频率分量上。例如, 对 FPGA 实现的无保护 AES-128 同时采集能量迹和电磁迹, 并对电磁迹和能量迹分别做 STFT 处理得到其时频图, 结果如图 3 所示。可以看到能量迹中有效信息的频率和电磁迹中有效信息的频率分布相似, 都集中在低频部分。其中, 电磁迹的时频图中可以清晰的看出 AES-128 密码算法的 10 轮计算过程。基于这一特点, 提出算法 2。当两个侧信道的侧信息具有相似的频谱分布特征时, 将两个信道的侧信息 STFT 变换后的结果进行点乘操作, 可以进一步增大泄漏 l 与噪声 σ 之间的差异。

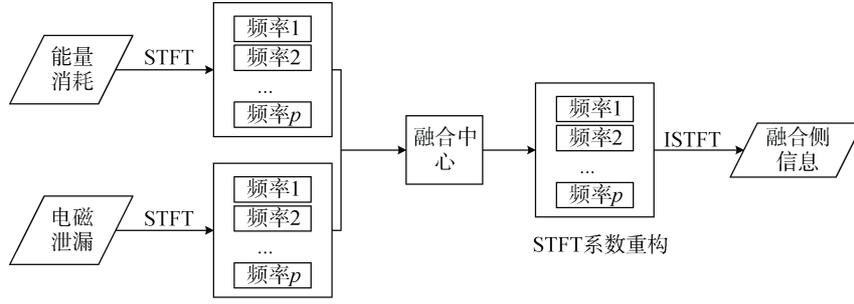


图 2 多源时频融合信息泄漏检测融合

Figure 2 Multi-channel time-frequency fusion leakage detection

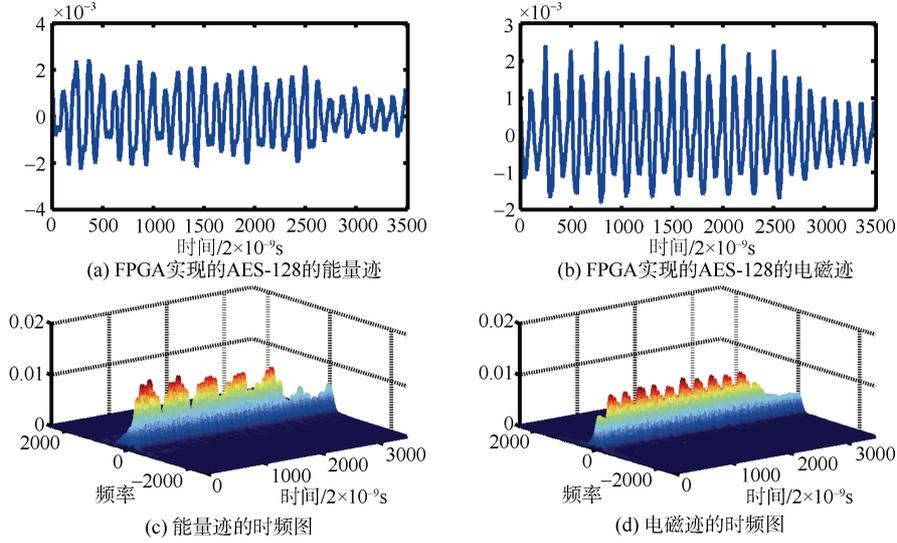


图 3 FPGA 实现 AES-128 能量迹及电磁迹的时频图

Figure 3 Time-frequency maps of the power traces and the EM traces of AES-128 implemented on FPGA

算法 2. 多源时频融合信息泄漏检测

输入: 能量消耗 L_{A1} 和 L_{B1} , 电磁泄漏 L_{A2} 和 L_{B2}

输出: 是否有泄漏

1: 对侧信息数据 L_{A1} , L_{A2} , L_{B1} , L_{B2} 分别做短时傅里叶变化:

$$L_{A1}' = STFT(L_{A1}); L_{A2}' = STFT(L_{A2});$$

$$L_{B1}' = STFT(L_{B1}); L_{B2}' = STFT(L_{B2});$$

2: 计算 L_{A1}' 和 L_{A2}' 点乘, 以及 L_{B1}' 和 L_{B2}' 的点乘:

$$L_1' = abs(L_{A1}') * abs(L_{A2}');$$

$$L_2' = abs(L_{B1}') * abs(L_{B2}');$$

3: 分别对 L_1' 和 L_2' 进行逆短时傅里叶变换得到两组融合后的侧信息:

$$L_1'' = ISTFT(L_1');$$

$$L_2'' = ISTFT(L_2');$$

4: 对 L_1'' 和 L_2'' 进行 TVLA 检验;

5: 返回是否有泄漏。

3.3 基于多元 T 检验的多源信息泄漏检测

本文提出了一种基于 Hotelling T^2 检验的多源信息泄漏检测方法。Hotelling T^2 检验^[27]是一种学生 t 检验在多元假设检验场景下的扩展。不同于学生 t 检验对两组单元变量的均值进行检验, Hotelling T^2 检验对两组多元变量的均值向量进行检验。本文基于 Hotelling T^2 检验提出一种多源信息泄漏检测。

3.3.1 Hotelling T^2 检验

有两个 p 维正态总体 $N_p(\mu, \Sigma)$ 和 $N_p'(\mu_0, \Sigma_0)$, 对这两个正态总体的均值向量进行检测, 检测二者是否相等, 检测步骤为:

从两个正态总体中分别抽取 n 个样本(本文仅考虑抽取的两组样本数量相同的情况), 即 $X_{(a)} = (X_{a1}, X_{a2}, \dots, X_{ap})'$, $a=1, 2, \dots, n$; 以及 $Y_{(b)} =$

$(Y_{b1}, Y_{b2}, \dots, Y_{bp})', b=1, 2, \dots, n$ 。

1) 建立假设 H_0 及备择假设 H_1 :

H_0 : 两组 p 维数据的均值向量相等 $\mu = \mu_0$;

H_1 : 两组 p 维数据的均值向量不等 $\mu \neq \mu_0$;

2) 令 $Z_i = X_i - Y_i$ 。则 $\bar{Z} = \frac{1}{n} \sum_{i=1}^n Z_i = \bar{X} - \bar{Y}$,

$S = \sum_{i=1}^n (Z_i - \bar{Z})(Z_i - \bar{Z})'$ 。假设 H_0 成立时, 构造检验统

计量 $F = \frac{(n-p)n}{p} \mathbf{Z} \mathbf{S}^{-1} \mathbf{Z}' \square F_{\alpha}(p, n-p)$, 其中 p 为正

态总体的维度, n 为样本数量。计算出 F 值后, 根据 F 分布计算出 $F(p, n-p)$ 在检验水准为 α 时的分位数 F' 。若 F 大于 F' , 则拒绝假设 H_0 , 接受 H_1 , 认为二者的均值向量有差异; 否则, 认为二者的均值向量没有差异。

3.3.2 基于 Hotelling T^2 检验的信息泄漏检测

与经典 TVLA 不同, 多源信息泄漏检测将多个侧信道在某一个时刻的值分别看作该时刻侧信息的不同维度, 即密码设备执行过程中某一时刻的侧信息是一个多维向量。具体方案如下(两个侧信道以能量消耗和电磁泄漏为例进行说明):

1) 随机生成两组明文密钥 A 和 B , 每组中均有 n 明文密钥对, 其中 A 明文随机密钥固定, B 明文和密钥都固定;

2) DUT 分别运行 A 和 B 两组数据, 并在运行过程中利用同样的采样参数同时采集能量消耗和电磁泄漏, 则得到 4 组数据 P_A, P_B 以及 E_A 和 E_B , 其中 P_A 表示明文随机的能量迹组, P_B 表示明文固定的能量迹组, E_A 表示明文随机的电磁迹组, E_B 表示明文固定的电磁迹组。每一条侧信息中均有 m 个采样点, 即 P_A, P_B, E_A 和 E_B 中每一个点可以表示为 $P_{Ai}^j, P_{Bi}^j, E_{Ai}^j, E_{Bi}^j, i=1, 2, \dots, n, j=1, 2, \dots, m$;

3) 将 P_A 与 E_A 在某一时刻的泄漏看做该时刻泄漏的不同维度, 若将 P_A 与 E_A 组合以 L_A 表示, 其中 $L_{Ai}^j = [P_{Ai}^j, E_{Ai}^j], i=1, 2, \dots, n, j=1, 2, \dots, m$, 同理将 P_B 与 E_B 组合以 L_B 表示, 则 L_B 每一时刻的泄漏为 $L_{Bi}^j = [P_{Bi}^j, E_{Bi}^j], i=1, 2, \dots, n, j=1, 2, \dots, m$;

4) 对 L_A 和 L_B 中的 m 个点分别做 Hotelling T^2 检验, 并根据检验结果判断是否接受假设 H_0 。具体算法如算法所示。

算法 3. 基于 Hotelling T^2 检验的多源信息泄漏检测

输入: 能量消耗 P_A 和 P_B , 电磁泄漏 E_A 和 E_B

输出: 是否有泄漏

1: 将 P_A 和 E_A 对应时刻上的泄漏组合起来, 构成一组新的基于随机明文和固定密钥的侧信息泄漏 L_A , 其中 $L_A^j = [P_A^j, E_A^j], j=1, 2, \dots, m$;

2: 将 P_B 和 E_B 对应时刻上的泄漏组合起来, 构成一组新的基于固定明文和固定密钥的侧信息泄漏 L_B , 其中 $L_B^j = [P_B^j, E_B^j], j=1, 2, \dots, m$;

3: 利用 Hotelling T^2 检验对 L_A 和 L_B 的均值向量进行检测, 并比较检测结果是否超过阈值;

4: 返回是否有泄漏。

4 实验分析

4.1 模拟实验

4.1.1 模拟实验配置

进行模拟实验时, 选择两个侧信道进行多源融合信息泄漏检测, 并考虑了两种实验场景:

1) 两个侧信道 M_1 和 M_2 具有相同的泄漏模型(实验中均选择 AES-128 第一轮 S 盒输出的汉明重量模型, 见公式(7))。

$$L_1 = a_1 * HW(\Psi(p, k)) + \sigma_1 \quad (7)$$

$$L_2 = a_2 * HW(\Psi(p, k)) + \sigma_2$$

实验中, 随机选取 a_1 和 a_2 (其中 $a_1=1$, 随机生成 $a_2=0.7$), 生成一组均匀分布的随机明文 P_1 和一组固定明文 P_2 以及固定密钥 K 。 σ_1 和 σ_2 是均值为 0 的高斯噪声, M_1 和 M_2 的信噪比取值均为 $[0.0625, 0.125, 0.25, 0.5, 1, 2]$, 对于 M_1 和 M_2 信噪比的不同取值, 共有 36 组参数。实验中对每一组参数, 分别进行多次实验计算检测出泄漏所需侧信息的最少数量, 并取均值作为该参数下的最终结果。

2) 两个侧信道 M_1 和 M_2 具有不同的泄漏模型(实验中, 一个侧信道的泄漏模型为 AES-128 第一轮 S 盒输出的汉明重量模型, 另一个侧信道的泄漏模型为 AES-128 第一轮 S 盒输入与输出的汉明距离模型, 信道 M_1 和 M_2 的泄漏模型见公式(8))。

$$L_1 = a_1 * HW(Sbox(p \oplus k)) + \sigma_1 \quad (8)$$

$$L_2 = a_2 * HW(Sbox(p \oplus k) \oplus (p \oplus k)) + \sigma_2$$

实验中, 随机选取 a_1 和 a_2 (其中 $a_1=1$, 随机生成 $a_2=0.7$), 生成一组均匀分布的随机明文 P_1 和一组固定明文 P_2 以及固定密钥 K 。 σ_1 和 σ_2 是均值为 0 的高斯噪声。 M_1 和 M_2 的信噪比取值均为 $[0.0625, 0.125, 0.25, 0.5, 1, 2]$ 。实验中, 对于每一组参数, 分别进行多

次实验计算检测出泄漏所需侧信息的最少数量, 并取均值作为该参数下的最终结果。

两组实验中, 利用 $TVLA(M_1)$, $TVLA(M_2)$, $SFTVLA-(W)SUM$ 以及 $MCTVLA$ 进行信息泄漏检测。其中, $TVLA(M_1)$ 和 $TVLA(M_2)$ 分别表示基于 M_1 的侧信息和 M_2 的侧信息进行经典 TVLA 检测; $SFTVLA-(W)SUM$ 表示对 M_1 和 M_2 进行多源简单融合信息泄漏检测, 使用的组合函数分别为加法和带权重的加法(M_1 的权重为 0.3 和 M_2 的权重为 0.7); $MCTVLA$ 表示进行基于多元 T 检验的多源信息泄漏检测。实验结果中以 $N(\text{Exp}_{SNR})$ 表示在信噪比为 SNR 时, 信息泄漏检测方案 Exp 检测出泄漏所需的侧信息数量。

4.1.2 模拟实验结果分析

1) M_1 和 M_2 具有相同的泄漏模型时, 泄漏检测所需侧信息数量如图 4 所示。可以看出, 随着信噪比的提高, $TVLA(M_1)$ 和 $TVLA(M_2)$ 检测出泄漏所需的侧信息数量逐步减少。当 M_1 和 M_2 的信噪比相同时, $TVLA(M_1)$ 检测出泄漏需求的侧信息数量远大于 $TVLA(M_2)$ 检测出泄漏需求的侧信息数量, 说明 TVLA 的检测效率不仅与侧信息的信噪比相关, 也与侧信息的泄漏模型有关。 $SFTVLA-(W)SUM$ 在不同的信噪比条件下表现差异较大。在实验场景中, 当 $SNR(M_2) \geq SNR(M_1)$ 时, $SFTVLA-WSUM$ 检测出泄漏时所需侧信息的数量小于 $SFTVLA-SUM$ 所需侧信息的数量; 反之, $SFTVLA-WSUM$ 检测出泄漏需要更多的侧信息。图 4 的 6 幅子图中均可以看出, 当 $SNR(M_1)$ 和 $SNR(M_2)$ 相差较大时, $SFTVLA-(W)SUM$ 检测出信息泄漏所需的侧信息数量位于 $TVLA(M_1)$ 或 $TVLA(M_2)$ 之间, 说明 $SFTVLA$ 的检测出泄漏所需侧信息的数量与 M_1 和 M_2 间的信噪比相关。图 4 中, 不论两个侧信道的信噪比取值如何, $MCTVLA$ 检测出泄漏所需侧信息的数量总是远少于 $TVLA(M_1)$, $TVLA(M_2)$ 及 $SFTVLA-(W)SUM$, 说明在 M_1 和 M_2 具有相同的泄漏模型时, $MCTVLA$ 可以降低泄漏检测所需侧信息的数量(实验中, 最高可降至单信道信息泄漏检测所需侧信息数量的 43%, 该数据通过

$$\frac{N(MCTVLA_{SNR(M_1), SNR(M_2)})}{\min(N(TVLA(M_1)_{SNR(M_1)}), N(TVLA(M_2)_{SNR(M_2)}))}$$
 计算得出), 提高信息泄漏检测效率。

2) M_1 和 M_2 具有不同的泄漏模型时, 泄漏检测所需侧信息数量如图 5 所示。可以看出, 随着信噪比的提高, $TVLA(M_1)$ 和 $TVLA(M_2)$ 检测出泄漏需求的侧信息数量逐步减少。当 M_1 和 M_2 的信噪比相同时, $TVLA(M_2)$ 检测出泄漏需求的侧信息数量远

大于 $TVLA(M_1)$ 检测出泄漏需求的侧信息数量, 例如图 5(a) 中 $N(TVLA(M_2)_{SNR(M_2)=0.0625}) = 21760$, 而对侧信道 M_1 有 $N(TVLA(M_2)_{SNR(M_1)=0.0625}) = 10190$, 在实验所选固定明文条件下 HW 模型的侧信息泄漏比 HD 模型的侧信息泄漏更容易检测出来。另外, 图 5 和图 4 具有相似的结论, 当 $SNR(M_1)$ 和 $SNR(M_2)$ 相差较大时, $SFTVLA-(W)SUM$ 检测出信息泄漏所需的侧信息数量位于 $TVLA(M_1)$ 以及 $TVLA(M_2)$ 所需侧信息数量之间, 此时利用这两种方案进行多源融合泄漏检测没有必要。而不论 $SNR(M_1)$ 和 $SNR(M_2)$ 的取值如何, $MCTVLA$ 检测出泄漏所需侧信息的数量总是远少于其余 4 种泄漏检测方案(实验中, 最高可降至单信道信息泄漏检测所需侧信息数量的 45%)。说明在 M_1 和 M_2 具有不同的泄漏模型时, $MCTVLA$ 可以有效减少信息泄漏检测所需的侧信息数量。

4.2 真实实验

4.2.1 真实实验配置

进行真实实验时, 选择能量消耗和电磁泄漏两个信道进行多源融合信息泄漏检测, 并考虑了有保护和无保护两种实验场景。

1) 检测目标是 SAKURA-X FPGA 板上实现的无保护 AES-128, 密码算法工作频率是 20 MHz, 同时采集加密算法执行全过程的能量消耗和电磁泄漏, 采样率均为 5 GHz, 采样点数为 3500。采集过程中, 基于固定明文固定密钥以及随机明文固定密钥采集能量迹和电磁迹。针对采集得到的 4 组数据进行 $TVLA(\text{Power})$, $TVLA(\text{EM})$, $SFTVLA-(W)SUM$, $TFFTVLA$ 和 $MCTVLA$ 泄漏检测实验。

2) 检测目标是 SAKURA-X FPGA 板上实现的受一阶布尔掩码保护的 AES-128。密码算法工作频率是 20 MHz, 同时采集算法最后 3 轮(最后一轮存在二阶泄漏)执行过程中的能量消耗和电磁泄漏, 采样率均为 5 GHz, 采样点数为 800。对受一阶布尔掩码保护的 AES-128 进行二阶泄漏检测, 首先对数据进行预处理, 将采样点进行两两组合以降低掩码的影响, 对于采集的 800 个采样点共有 320400 种组合形式。实验中使用的组合方式是标准绩, 即 L' 通过
$$L' = \left| L^i - \overline{L^i} \right| \cdot \left| L^j - \overline{L^j} \right|$$
 计算得出, 其中 $i \in [1, m-1]$, $j \in [i+1, m]$ 。针对预处理后的数据分别进行二阶泄漏检测实验, 实验方案为 $TVLA(\text{EM}-2nd)$, $TVLA(\text{Pow}-2nd)$, $TFFTVLA-2nd$, $SFTVLA-(W)SUM-2nd$ 和 $MCTVLA-2nd$ 。

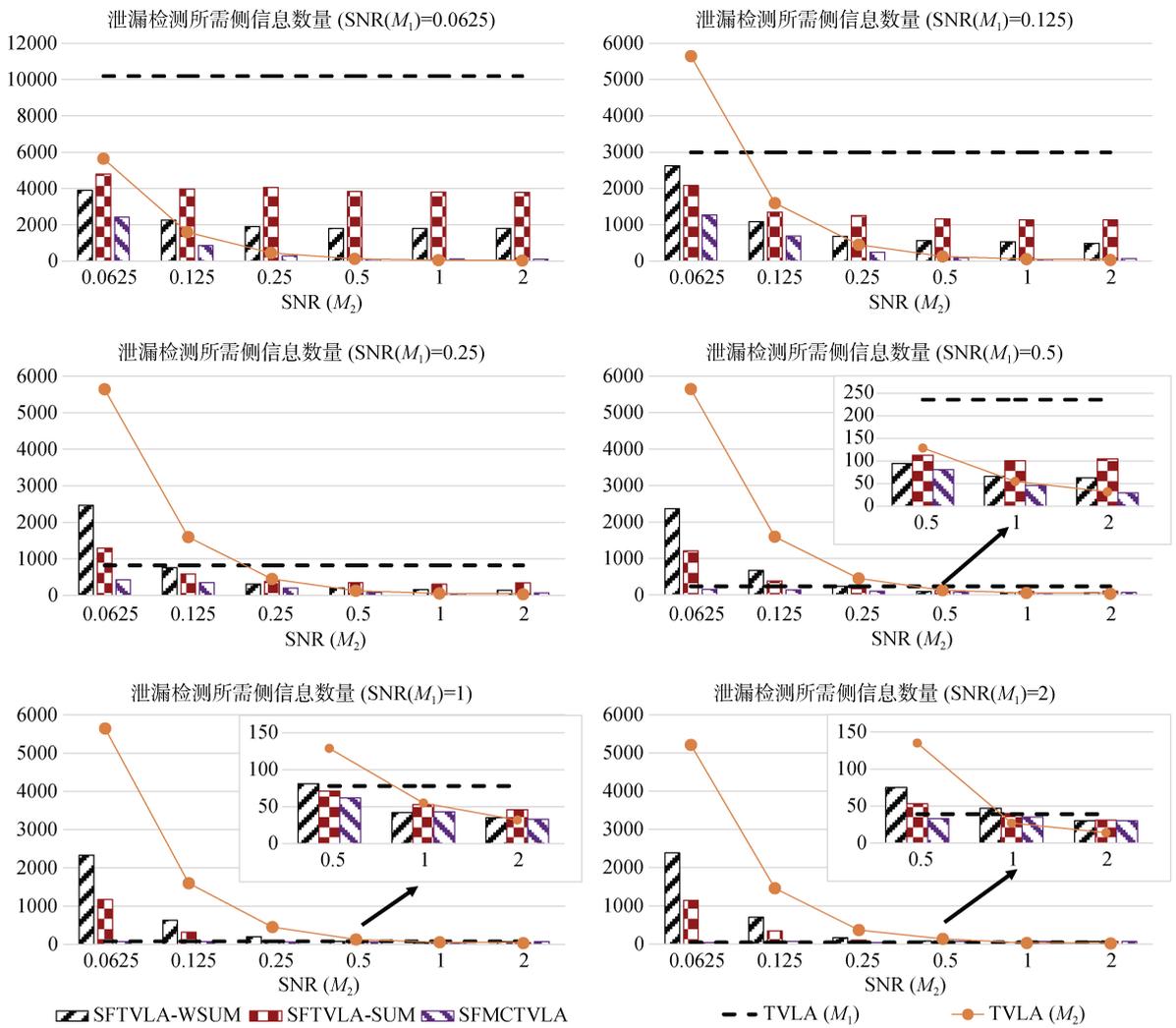
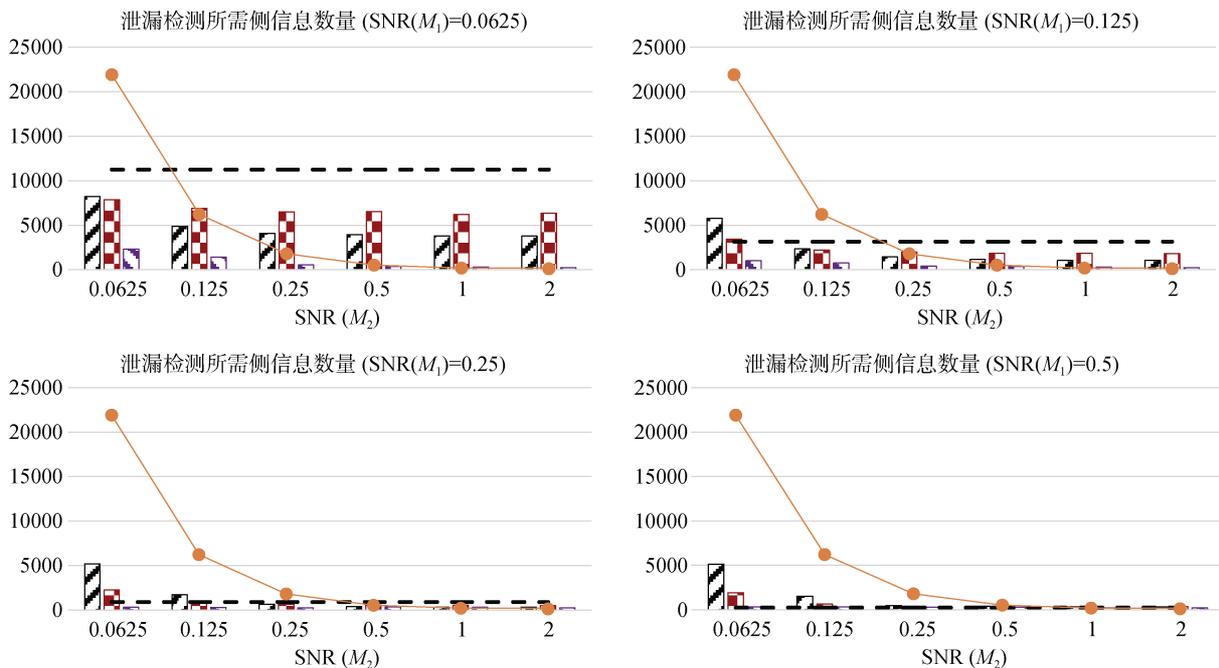


图 4 M_1 和 M_2 具有相同的泄漏模型, 泄漏检测所需侧信息数量与 $SNR(M_1)$ 和 $SNR(M_2)$ 间的关系

Figure 4 The relationship between the amount of side information needed for leakage detection and $SNR(M_1)$ and $SNR(M_2)$ when M_1 and M_2 have the same leakage model



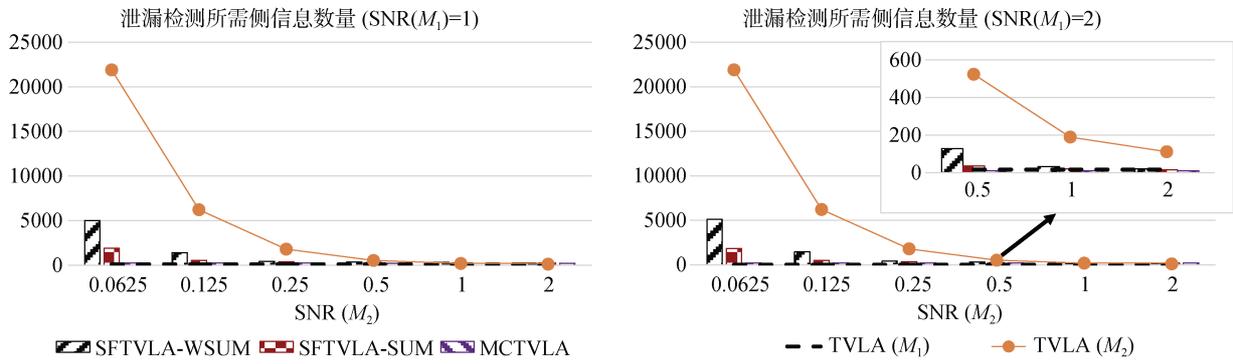


图 5 M_1 和 M_2 具有不同的泄漏模型, 泄漏检测所需侧信息数量与 $\text{SNR}(M_1)$ 和 $\text{SNR}(M_2)$ 间的关系

Figure 5 The relationship between the amount of side information needed for leakage detection and $\text{SNR}(M_1)$ and $\text{SNR}(M_2)$ when M_1 and M_2 have the same leakage model

4.2.2 真实实验结果分析

1) 对 SAKURA-X 上实现的无保护 AES-128 泄漏检测结果如图 6 和图 7 所示。从图 7 中可以看出, 在各组数据均为 1000 条时, 6 种泄漏检测方案均可以检测出泄漏, 且检测出的泄漏点位置大致相同。然而当侧信息数量降至 200 条时, $TVLA(Power)$ 不能检测出泄漏, $TVLA(EM)$ 和 $SFTVLA-(W)SUM$ 仅能检测出一个泄漏点, 而 $TFFTVLA$ 和 $MCTVLA$ 仍然能检测出

多个泄漏位置的信息泄漏。两幅图对比, $TFFTVLA$ 检测出的泄漏点位置并没有因为侧信息数量的减少有较大变化。真实实验结果说明 $TFFTVLA$ 和 $MCTVLA$ 可以提高信息泄漏检测的效率, 降低泄漏检测所需侧信息数量。而 $SFTVLA-(W)SUM$ 的表现也可以利用模拟实验说明, 只有当待融合的多个侧信道信噪比相差不大时, 利用 $SFTVLA-(W)SUM$ 可以减少泄漏检测所需的侧信息数量。

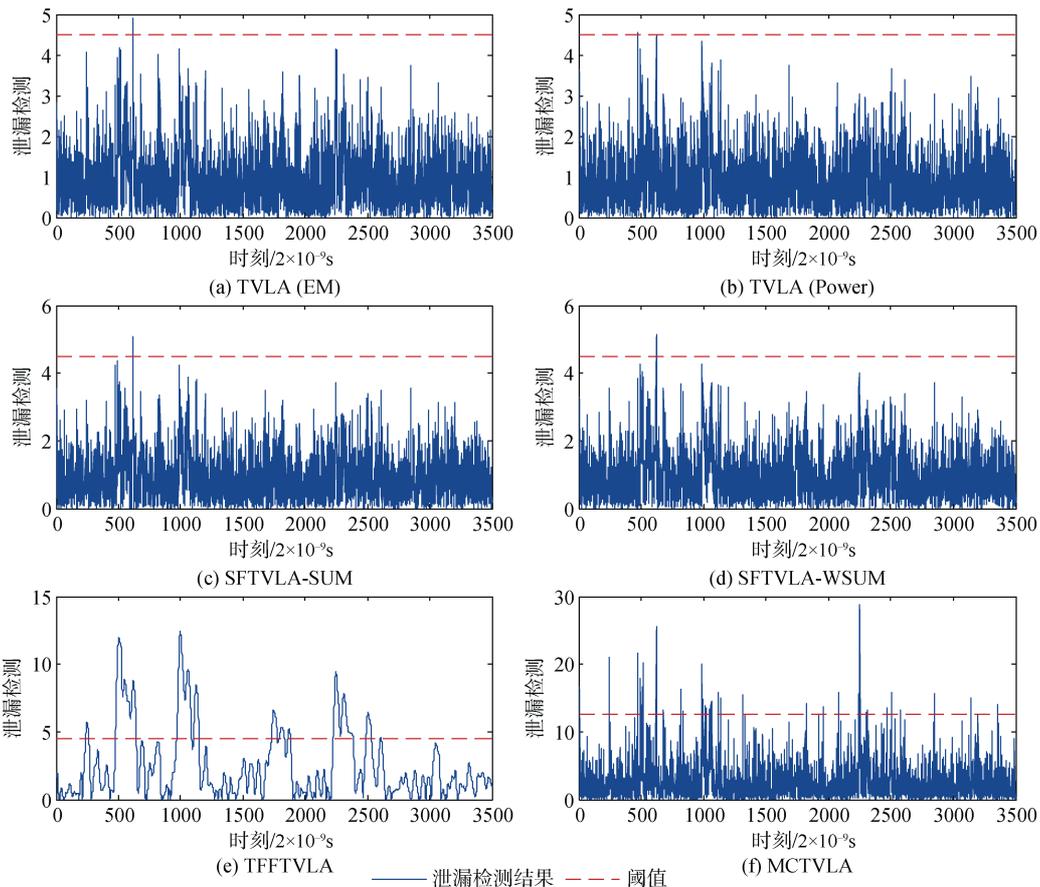


图 6 SAKURA-X 实现的无保护 AES-128 泄漏检测结果(各组电磁迹、能量迹均为 200 条)

Figure 6 Results of leakage detection against unprotected AES-128 implemented on SAKURA-X (each group has 200 EM traces and 200 power traces)

2) 对 SAKURA-X 上实现的一阶布尔掩码保护的 AES-128 泄漏检测结果如图 8 所示。从图中可以看出, 在能量迹和电磁迹均有 10000 条的情况下, 只有 *MCTVLA* 检测出了泄漏, 且检测出了 133 种存在泄漏的数据组合。已知利用基于一致性检验的泄漏检测检测出的泄漏并不一定能够转化为已知的有效攻击^[22], 为了验证检测出的泄漏是否有效, 对检测出的 133 种数据组合分别进行 2 阶电磁相关分析(2nd CEMA)进行攻击。针对 SAKURA-X 平台, 选择的假设电磁泄漏为最后一轮 S 盒的输入

与相应的密文间的汉明距离(最后一轮需要考虑行移位)。2nd CEMA 攻击结果如图 9 所示, 其中有 20 种数据组合可以成功恢复密钥, 说明利用 *MCTVLA* 可以检测出二阶泄漏。图 8 和图 9 说明在实验场景下, *MCTVLA* 可以提高信息泄漏检测的效率, 降低泄漏检测所需侧信息数量, 而 *SFTVLA-(W)SUM* 和 *TFFTVLA* 并不能检测出有效泄漏。*TFFTVLA* 在实验中不能减少泄漏检测所需侧信息数量可能是由于密码实现的能量消耗和电磁泄漏的频率分布间差异造成的。

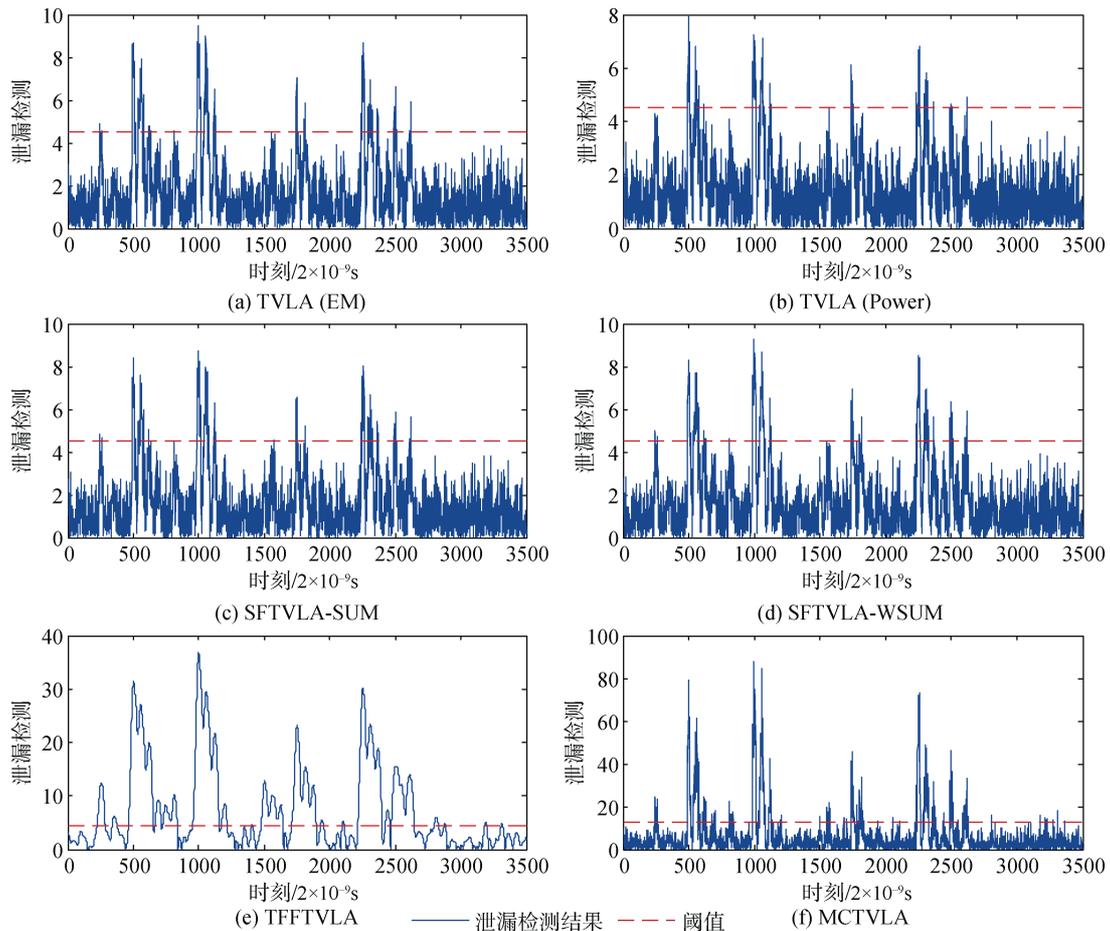


图 7 SAKURA-X 实现的无保护 AES-128 泄漏检测结果(各组电磁迹、能量迹均为 1000 条)

Figure 7 Results of leakage detection against unprotected AES-128 implemented on SAKURA-X (each group has 1000 EM traces and 1000 power traces)

5 结束语

本文为了实现多源泄漏场景下对密码设备物理安全性更全面、更客观的评估, 提出了 3 种多源融合信息泄漏检测方案。据笔者所知, 这是目前首项针对多源泄漏场景下如何综合利用多个信道侧信息进行信息泄漏检测的工作。与单信道的信息泄漏检测相比, 多源融合信息泄漏检测具有天然的优势: 一方面, 多

源融合信息泄漏检测技术由于利用了多个信道的信息, 可以降低泄漏检测所需的侧信息数量, 从而提高泄漏检测的效率和实用性。另一方面, 多源融合信息泄漏检测同时检测多个信道的侧信息, 有利于发现单信道信息泄漏检测中可能检测不出的泄漏。实验结果显示 *MCTVLA* 可以大幅提高信息泄漏检测的效率, 减少泄漏检测所需侧信息的数量(与单信道 TVLA 相比, *MCTVLA* 最多可将所需侧信息数量降至 43%)。真实

实验中, *TFFTVLA* 针对无保护实现可以大幅减少泄漏检测所需的侧信息数量, 提高了泄漏检测的效率。与 *MCTVLA* 相比, *SFTVLA* 和 *TFFTVLA* 虽然有具体适用场景, 但更容易扩展至其他类型的泄漏检测, 如文献[23]和[25]中提出的泄漏检测方案。对于 *SFTVLA* 和 *TFFTVLA*, 在进行信息融合时, 可能会存在其他效果

更好的融合函数, 值得进行更深入的探讨。

需要注意的是, 通过多源融合信息泄漏检测测出的泄漏并不能确定是哪个信道泄漏的信息。如果需要定位到具体是哪个信道泄漏的信息进而设计相应的防护措施时, 需要利用单信道的信息泄漏检测进行具体的定位工作。

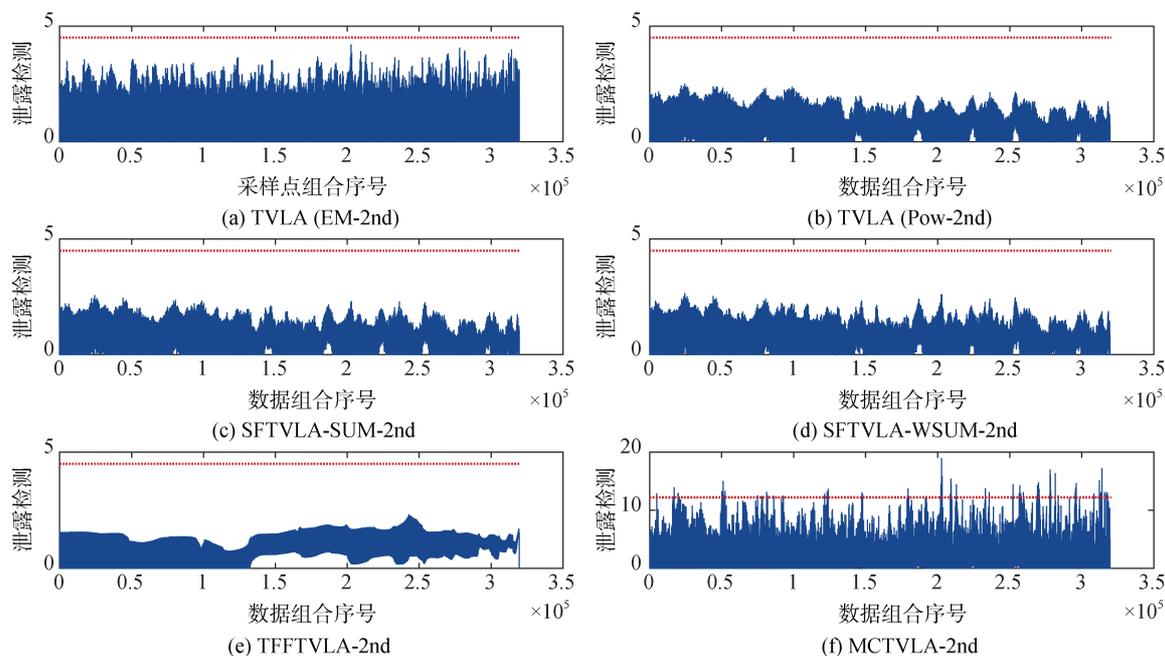


图 8 SAKURA-X 实现的一阶布尔掩码保护的 AES-128 泄漏检测结果(各组电磁迹、能量迹均为 10000 条)
Figure 8 Results of leakage detection against AES-128 protected by 1st order boolean mask implemented on SAKURA-X (each group has 10000 EM traces and 10000 power traces)

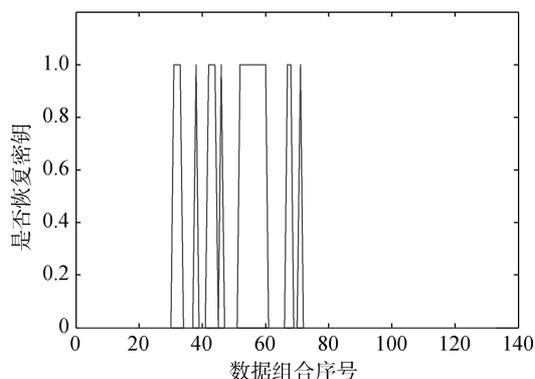


图 9 MCTVLA-2nd 检测出的泄漏点是否可以利用 2nd CEMA 恢复正确密钥

Figure 9 Leakage points detected by MCTVLA-2nd can be used to recover correct key using 2nd CEMA

参考文献

[1] Kelsey J, Schneier B, Wagner D, et al. Side Channel Cryptanalysis of Product Ciphers[M]. *Computer Security — ESORICS 98*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998: 97-110.

[2] Kocher P C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other Systems[M]. *Advances in Cryptology — CRYPTO '96*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996: 104-113.

[3] Kocher P, Jaffe J, Jun B. Differential power analysis[C]. *Annual international cryptography conference*. Springer, Berlin, Heidelberg, 1999: 388-397.

[4] Gandolfi K, Mourtel C, Olivier F. Electromagnetic Analysis: Concrete Results[M]. *Cryptographic Hardware and Embedded Systems—CHES 2001*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001: 251-261.

[5] Halevi T, Saxena N. Keyboard Acoustic Side Channel Attacks: Exploring Realistic and Security-sensitive Scenarios[J]. *International Journal of Information Security*, 2015, 14(5): 443-456.

[6] Skorobogatov S P, Anderson R J. Optical Fault Induction Attacks[M]. *Cryptographic Hardware and Embedded Systems - CHES 2002*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003: 2-12.

[7] Mangard S, Oswald E, Popp T. Power analysis attacks: Revealing the secrets of smart cards[M]. Springer Science & Business Media,

- 2008.
- [8] Lomné V, Maurine P, Torres L, et al. Evaluation on FPGA of triple rail logic robustness against DPA and DEMA[C]. *2009 Design, Automation & Test in Europe Conference & Exhibition*. IEEE, 2009: 634-639.
- [9] Standaert F X, Malkin T G, Yung M. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks[M]. *Advances in Cryptology - EUROCRYPT 2009*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009: 443-461.
- [10] Moradi A, Barengi A, Kasper T, et al. On the Vulnerability of FPGA Bitstream Encryption Against Power Analysis Attacks: Extracting Keys from Xilinx Virtex-II FPGAs[C]. *the 18th ACM conference on Computer and communications security*, 2011: 111-124.
- [11] Whitnall C, Oswald E. A Comprehensive Evaluation of Mutual Information Analysis Using a Fair Evaluation Framework[M]. *Advances in Cryptology - CRYPTO 2011*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 316-334.
- [12] ISO/IEC 15408, Information technology-Security techniques-Evaluation criteria for IT security. <https://www.iso.org/standard/50341.html>
- [13] FIPS 1403 DRAFT Security Requirements for Cryptographic Modules (Revised Draft). http://csrc.nist.gov/publications/drafts/fips1403/reviseddraftfips1403_PDFzip_documentannexAtoannexG.zip.
- [14] Gilbert Goodwill B J, Jaffe J, Rohatgi P. A testing methodology for side-channel resistance validation[C]. *NIST non-invasive attack testing workshop*. 2011, 7: 115-136.
- [15] Schneider T, Moradi A. Leakage Assessment Methodology[M]. *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015: 495-513.
- [16] Cooper J, DeMulder E, Goodwill G, et al. Test vector leakage assessment (TVLA) methodology in practice[C]. *International Cryptographic Module Conference*. 2013, 20.
- [17] Mather L, Oswald E, Bandenburg J, et al. Does my Device Leak Information? an a Priori Statistical Power Analysis of Leakage Detection Tests[M]. *Advances in Cryptology - ASIACRYPT 2013*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013: 486-505.
- [18] Schneider T, Moradi A. Leakage assessment methodology[J]. *Journal of Cryptographic Engineering*, 2016, 6(2): 85-99.
- [19] Francois Durvaux, Francois-Xavier Standaert and Nicolas Durvaux F, et. al. How to certify the leakage of a chip?[C]. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 2014: 459-476.
- [20] Moradi A, Wild A. Assessment of Hiding the Higher-Order Leakages in Hardware[M]. *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015: 453-474.
- [21] Ding A A, Zhang L W, Durvaux F, et al. Towards Sound and Optimal Leakage Detection Procedure[M]. *Smart Card Research and Advanced Applications*. Cham: Springer International Publishing, 2018: 105-122.
- [22] Durvaux F, Standaert F X. From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces[M]. *Advances in Cryptology - EUROCRYPT 2016*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016: 240-262.
- [23] Reparaz O, Gierlichs B, Verbauwhede I. Fast Leakage Assessment[M]. *Lecture Notes in Computer Science*. Cham: Springer International Publishing, 2017: 387-399.
- [24] Moradi A, Richter B, Schneider T, et al. Leakage detection with the χ^2 -test[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018: 209-237.
- [25] Welch B L. The Generalization of 'Student's' Problem when Several Different Population Variances are Involved[J]. *Biometrika*, 1947, 34(1/2): 28.
- [26] Allen J. Short Term Spectral Analysis, Synthesis, and Modification by Discrete Fourier Transform[J]. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 1977, 25(3): 235-238.
- [27] Hotelling H. The Generalization of Student's Ratio[M]. *Springer Series in Statistics*. New York, NY: Springer New York, 1992: 54-65.



曹雨晨 于 2013 年在中国科学院大学信息工程研究所信息安全专业获得工学硕士学位。现在中国科学院信息工程研究所攻读博士学位。研究领域为侧信道分析。研究兴趣包括: 信号处理、安全性检测等。Email: caoyuchen@iie.ac.cn



周永彬 于 2004 年 3 月获得计算机应用技术专业博士学位。现任中国科学院信息工程研究所研究员。研究领域为信息安全理论及技术。研究兴趣密码学、密码工程、网络安全、数据安全与隐私保护等。Email: zhuyongbin@iie.ac.cn