中国科学院大学
University of Chinese Academy of Sciences

博士学位论文

密码芯片侧信道分析与检测技术研究

作者姓名：杨　威

指导教师：焦建彬　教授

中国科学院大学

学位类别：工学博士

学科专业：计算机应用技术

研 究 所：电子电气与通信工程学院

二〇一七年十月

Study on Side-Channel Analysis and Detection for Cryptographic Chips

By

Wei Yang

A Dissertation Submitted to
University of Chinese Academy of Sciences
in Partial Fulfillment of the Requirement
for the Degree of
Doctor of Philosophy

School of Electronic, Electrical and Communication Engineering
University of Chinese Academy of Sciences

October, 2017

中国科学院大学直属院系
研究生学位论文原创性声明

本人郑重声明：所呈交的学位论文是本人在导师的指导下独立进行研究工作所取得的成果。尽我所知，除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的研究成果。对论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明或致谢。

作者签名：

日　　期：

中国科学院大学直属院系
学位论文授权使用声明

本人完全了解并同意遵守中国科学院有关保存和使用学位论文的规定，即中国科学院有权保留送交学位论文的副本，允许该论文被查阅，可以公布该论文的全部或部分内容，可以采用影印、缩印或其他复制手段保存、汇编本学位论文。

涉密的学位论文在解密后适用本声明。

作者签名：　　导师签名：

日　　期：　　日　　期：

摘　要

侧信道攻击通过利用密码芯片的物理信息泄漏（如能量泄漏、电磁辐射等）来恢复密钥信息，对密码芯片的物理安全性构成了严重威胁。因此，针对密码芯片进行侧信道分析与检测十分重要且必要。

目前面向密码芯片的侧信道分析与检测技术的研究主要是在密码芯片侧信息泄漏充足及侧信息泄漏不足两个场景下展开。前一个场景下分析者能够实施成功的侧信道攻击或准确刻画密码芯片侧信息泄漏水平；后一个场景下分析者获取的侧信息泄漏不足以实施成功的侧信道攻击或无法准确刻画密码芯片侧信息泄漏水平。实际中，在对密码芯片进行侧信道分析与检测之前，通常需对泄漏信号进行预处理。因此本文首先研究了预处理中较为重要的泄漏信号对齐问题。之后在侧信息充足场景下，本文分别研究了多信道融合攻击、泄漏评估与泄漏检测问题。最后，本文对侧信息不足场景下的密钥枚举及密钥排序问题进行了研究。论文的主要工作及贡献如下：

1. 泄漏信号对齐. 绝大多数侧信道攻击正常工作的前提是采集所得泄漏信号在时域上严格对齐。然而实际中，常由于触发信号不精确、隐藏防御策略等因素的影响，采集到的泄漏信号在时域上不能严格对齐，导致侧信道攻击效率大幅将低，甚至失效。因此在攻击前对齐泄漏信号极其重要。而目前关于泄漏信号对齐的研究，或者会丢失部分依赖于密钥的泄漏信息，或者会引入冗余信息，对侧信道攻击效率的提升有限。本文着眼于此，根据信息利用方式的不同，将泄漏信号对齐技术分为局部对齐技术和全局对齐技术两类，并提出两种泄漏对齐方法，即基于 shotgun 距离的局部泄漏信号对齐算法以及基于加权编辑距离的全局泄漏信号对齐算法。与已有方法相比，二者能在保留依赖于密钥的泄漏信息的同时，避免引入冗余信息，从而能更大程度地提高侧信道攻击效率。实际实验验证了这一点。此外，实验结果还表明本文方法的抗噪声性能也都优于对比方法。

2. 多信道融合攻击. 与传统单信道攻击相比，多信道融合攻击同时利用多个侧信道的泄漏进行攻击。因此一个多信道攻击若实施恰当，应能更有效地利用侧信道泄漏信息，对密码芯片的侧信道安全性分析也应较单信道攻击全面。然而，现有相关研究较少且不成系统。针对一个密码实现，现有研究很难为如何进行高效的多信道融合攻击提供帮助。鉴于此，本文从融合的角度出发，将多信道融合攻击分为三类——数据级、特征级及决策级融合攻击，并在此框架下提出了六种融合攻击方法，考察了不同种类多信道融合攻击在同一密码算法的不同实现下的性能表现，以及不同融合方式对多信道融合攻击效率的影响。实验表明本文所提方法性能优于对比方法。此外，本文提出了一种基于偏相关分析的多信道融合度量标准，用于判断不同信道泄漏是否宜于融合。

该度量标准相比以往同类标准，无需知道密钥，且易于计算。该标准的有效性通过了实际实验验证。本文对多信道融合攻击研究较为系统，能够针对不同密码实现，为多信道融合攻击提供建议。

3. 泄漏评估与泄漏检测. 因为密码芯片的真实泄漏分布通常未知，所以对密码芯片进行泄漏评估较为困难。现有方法分非参数估计和参数估计两类。前者效率较高但精度不高，后者则需大量数据来保证精度，导致实际可操作性不强。为综合二者优点，本文建立了侧信道的通信信道模型，并使用通信信道的平均互信息及信道容量来分别估计密码芯片的泄漏量及其上界。实验显示，在不同的噪声类型下，本文所提方法性能总是优于所对比的非参数和参数估计方法。另外，本文结合侧信道通信信道模型的信道特性及参数一致性检验工具，得到一种新的泄漏检测方法。相比以往的泄漏检测方法，该方法对泄漏信号的采集没有特殊要求，且检测出的泄漏特征点能直接用于相关分析攻击。

4. 密钥枚举及密钥排序. 目前的密钥枚举研究不能提升密钥排序位置，效率始终受限。本文结合真实密钥排序位置随泄漏信号数目变化的曲线积分，提出两种可以提升真实密钥排序位置的算法，能从根本上提高密钥枚举的效率。在对密钥排序技术的研究中，本文利用子密钥候选值的位置排序来估计真实主密钥的排序位置，应用信号多抽样率抽取及插值技术提高一种已有的密钥排序算法的精度，并基于子密钥相关性，提出一种能评估最坏情况下密码芯片安全水平的密钥排序算法。实际实验验证了所提方法的有效性。

关键词：侧信道分析与检测；泄漏信号对齐；多信道融合；泄漏评估与泄漏检测；密钥枚举与密钥排序

Study on Side-Channel Analysis and Detection for Cryptographic Chips

Wei Yang (Computer Application Technology)
Directed by Jianbin Jiao

Side Channel attacks (SCAs) recover secret information of a crypto chip by exploiting its physical leakages, e.g. power consumption, electromagnetic emission, etc. SCAs have been a realistic serious threat to crypto chips. Therefore, it is quite important and necessary to analyze and detect the SCAs resilience of crypto chips.

The research of side channel analysis and detection focuses on two scenarios, i.e. the scenario that the acquired leakages are sufficient to mount a successful attack or accurately evaluate the total leakage amount of a crypto chip, and the scenario that the leakages are insufficient to mount an attack or evaluate the chip's leakage amount. In practice, signal preprocessing is generally necessary for side channel analysis and detection. Hence we firstly investigate side channel leakage alignment, which is an important topic of leakage signal preprocessing. Afterward, we respectively study multi-channel fusion attacks, leakage evaluation and leakage detection in the first scenario. In the final, key enumeration and rank estimation are respectively investigated in the second scenario. Our work and contributions are shown as follows:

Leakage alignment. For most SCAs to achieve good performance, the measured leakages are often desired to be well aligned. However, due to some reasons such as inaccurate measurements or carefully designed countermeasures, temporal misalignment of leakages frequently occurs in practice. Misalignment significantly reduces the efficiency of SCAs, or even makes them fail. Therefore, the alignment process towards misaligned traces is enormously helpful for SCAs. However, the previous work may lose some leakage information related to the key, or introduce some redundancy. To address the issues, this thesis divides leakage alignment into two groups according to the way of information use, i.e. local and global alignment. And accordingly, we propose two methods, i.e. a local alignment based on shotgun distance and a global alignment based on weighted edit distance. As compared to previous methods, the proposed methods are capable of keeping the secret dependant leakages, while not introducing any redundant information. Therefore, the proposed methods are more efficient than the compared methods. The analysis is also verified by practical experiments. Besides, the experiments also show that the proposed methods are more anti-noise than the compared methods.

Multi-channel fusion attacks. Multi-channel fusion attacks (MCFAs) utilize multi-channel leakages simultaneously. As compared to mono-channel attacks, MCFAs have higher potential

leakage utilization. They can evaluate the physical security of crypto chips more comprehensively if well-implemented. However, previous research about MCFAs is scarce. MCFAs have not been studied systematically. According to the existing research, it is hard to select MCFAs strategies properly and perform MCFAs efficiently. In light of this, we classify MCFAs into three groups from the view of fusion, i.e. data-level, feature-level and decision-level fusion attacks. Accordingly, we construct six MCFAs and study their applicable scopes and different performance of MCFAs with different fusion activities. Experiments show that the proposed methods outperform the previous methods. In addition, we also characterize a partial correlation analysis based fusion metric to select the channels which are suitable for combination. The metric is easier to calculate and does not need the knowledge of the key compared to the existing metrics. Its effectiveness is also verified by practical experiments. Our work systematically investigates MCFAs and it can offer advice on MCFAs against different implementations of a crypto algorithm.

Leakage evaluation and detection. Leakage evaluation is usually difficult because the real leakage distribution of a crypto device is unknown. Commonly, there are two ways to estimate the leakage distribution of a device, i.e. non-parametric ones and parametric ones. The former is generally more efficient, but may bring a big error since the leakage model is not accurate. The latter is more precise since it can profile the leakage model, but may be infeasible in practice. To combine the merits of these two estimation ways, we analyze the side-channel as a communication channel, and we use the average mutual information and the channel capacity of the communication channel to estimate a crypto's leakage amount and its upper bound, respectively. The experiments with different types of noise show that the proposed method always outperforms the compared methods. Furthermore, based on the communication channel characteristic, we find that if we do consistency check for the channel parameters, a leakage detection method can be developed. As compared to the known methods, there is no specific requirement for the acquirement of leakages, and the points found by the proposed method can be used to mount correlation analysis attack directly.

Key enumeration and rank estimation. The past work of key enumeration has a limited performance since the real key rank cannot be improved. According to the integral of the curve, which reflects the change of the real key rank with the variational trace number, we propose two methods which can improve the real key rank and the efficiency of key enumeration fundamentally. In addition, we estimate the rank of the real key according to ranks of all subkey guesses, and we improve the accuracy of an existing key enumeration method via multi-rate sampling and interpolation. We also propose another method based on the correlations of subkey to evaluate the worst-case security level of a crypto chip. Practical experiments show

that the proposed methods are effective.

Keywords: Side channel analysis and detection; Leakage alignment; Multi-channel fusion attacks; Leakage evaluation and leakage detection; Key enumeration and key rank estimation

目　录

图目录

表目录

第一章　引言

1.1　研究背景与意义

密码模块是一种将密码算法以软件程序或者硬件逻辑电路的形式实现的物理模块。其中，密码芯片作为一种最典型的密码模块形式，是一类重要的基础安全功能单元，在实际工作和生活中应用十分广泛，近几年需求迅速增长。例如，欧洲智能卡协会EuroSmart于2017年5月发布的2010-2017年全球密码芯片出货量统计与预测数据（如图 1.1 所示 *）显示，2015年及2016年全球售出的密码芯片总量分别为93.2亿个、96.1亿个，预计全球2017年密码芯片的售货量将达到99.4亿个。这些密码芯片广泛应用于各行各业，覆盖了电信、政府医疗、金融服务、设备制造等诸多领域。密码芯片的应用形式和场景多种多样，如电信SIM卡、银行IC卡、身份证件、USB Key、POS机、智能手机、近场通信、共享单车、城市交通、移动多媒体广播电视、物联网、税收、社保和医疗保健等，已经密切融入人们的工作与生活之中。

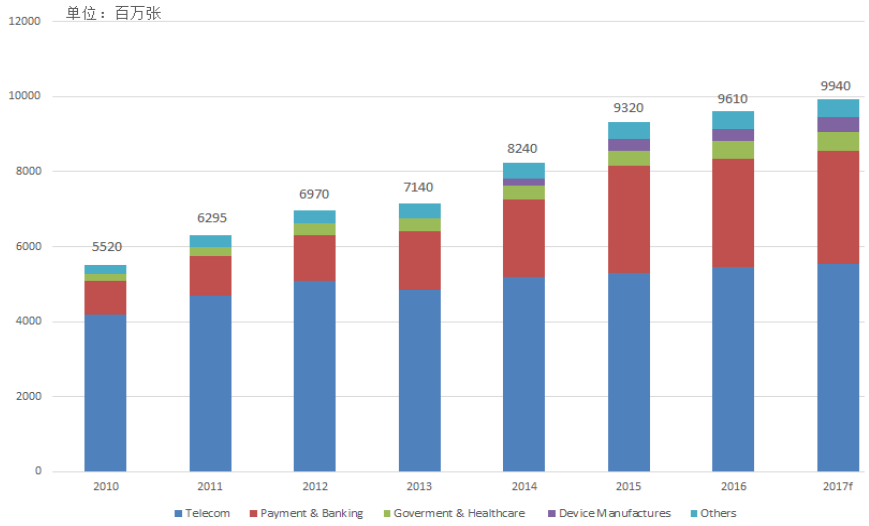


图 1.1　2010-2016年全球安全芯片出货量统计及2017年出货量预测

在我国，密码芯片凭借着高便捷性与安全性，需求增长强烈，正加速应用于与国计民生息息相关的行业中。仅以智能卡为例，据国家金卡工程办公室统计 †，我国现已成为世界上最大的智能证卡应用市场之一，近年来共发行135亿张智能卡，包括近60亿张电信SIM卡、24亿张银行IC卡、14亿张第二代居民身份证、8.6 亿张社会保障卡及近7.5亿张城市交通与各种公用事业缴费卡。其中，电信SIM卡用户规模在2015年就已

* 数据来源：http://www.eurosmart.com/facts-figures.html

† 数据来源：http://www.chinagoldencard.com/nd.jsp?id=4122&_jcp=4_57

达13.6亿，而且随着通讯网络升级及智能手机市场的不断增长，电信SIM卡市场在可预见的未来增长潜力依然巨大。另外，根据中国银联公布的统计数据，可以发现2015年中国市场金融IC卡发行与交易增速均居于全球领先，发卡量比2014年超出近亿张（如图 1.2 所示*）。预计2016年全国全年金融IC卡相比2015年增加的发卡量将超过8亿张。目前，智能卡已经应用在社会保障、公共交通、医疗卫生等7大类28个领域中，覆盖公共服务、社会保障、医疗卫生、文化教育、城市管理、生活服务、企业服务等多个领域，应用场景达百余个，有效创新了公共服务手段，开创了普惠服务民生的新局面，促进了行业信息化与城市信息化的结合。

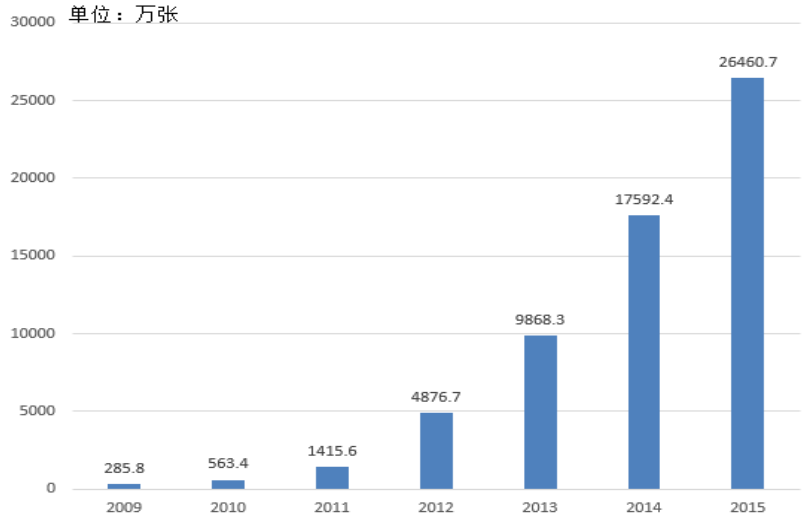


图 1.2　2009-2015年全国金融IC卡发卡量统计

可以预见，由于国内外持续呈现对搭载便利性和安全性的高端技术解决方案的强劲需求，密码芯片的应用需求将会持续增加，应用领域将会继续扩展。密码芯片负责为内嵌密码芯片的设备与系统提供基础安全功能，其安全性直接关系着设备与系统的信息保护是否可靠。密码芯片的安全性不仅包括所使用的密码算法的理论安全性，还包括算法实现的物理安全性。本文在假设密码芯片算法安全的基础上考虑一个重要的问题：一个密码芯片的物理安全性究竟如何？

要回答这个问题，需对密码芯片在实际应用中的物理安全性进行准确分析与检测。针对密码芯片物理安全性分析与检测的手段很多，通过攻击进行安全分析与检测一直是最直接、最有效的评估手段。通常对密码芯片物理安全性威胁较大的三类攻击方式为非入侵式攻击、半入侵式攻击与入侵式攻击。其中，具有广泛代表性的是非入侵式攻击方式中的侧信道攻击技术。

实际应用中，密码芯片运行时会以某种物理形式（如执行时间 [1]、能量消耗 [2]、电磁辐射 [3]、声音 [4]、光学辐射 [5–7] 等）泄漏其内部状态信息——这些与密码芯片

* 数据来源：http://www.chyxx.com/data/201603/393933.html

所使用密钥相关的信息被称为侧信息。侧信息泄漏可被分析者用以实施针对密码芯片的攻击，获取密码芯片所使用的密钥信息。此类攻击统称为侧信道攻击。图 1.3*以能量分析攻击为例，介绍了一个典型的侧信道攻击流程。从图中可以看出，分析者首先采集密码芯片运行中的能量泄漏信号，并根据能量泄漏模型，得到密码芯片运行中某个与密钥相关的中间值的假设能量泄漏，然后借助某种统计工具对实测能量泄漏和假设能量泄漏进行分析，从而恢复出密钥。

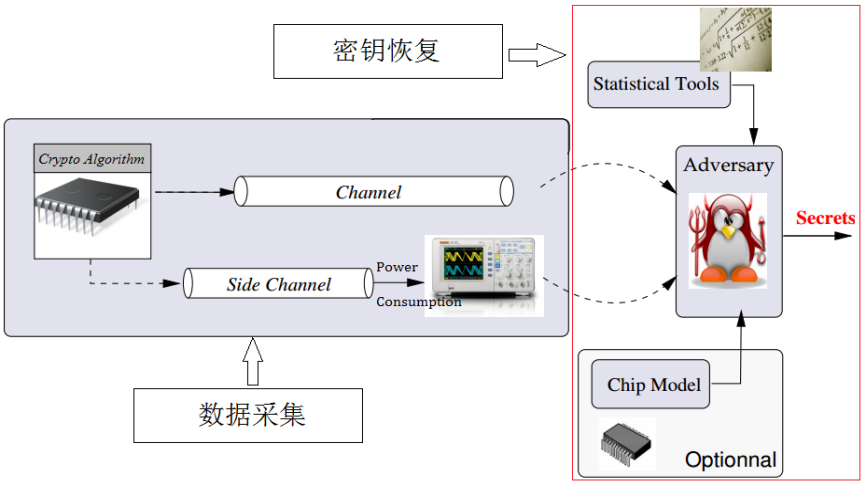


图 1.3 侧信道攻击流程示意图

侧信道攻击的存在给密码芯片的实际安全性带来了极大的安全威胁。事实上，国际密码学者与密码芯片产业界早就认识到了密码芯片物理安全的重要性，然而相比传统密码分析较为清晰的安全性定义及评估方法 [8,9]，密码芯片的物理安全性与设备高度相关 [10]，针对其安全性的定义及评估工作落后于实际需求。经过近二十年的研究与应用实践，对密码芯片自身的安全性逐步形成了严格而清晰的技术需求，并形成了相应的国际与国家技术标准。例如，美国国家标准技术局（NIST）制定并由美国联邦政府自1994年开始颁布的FIPS 140系列标准 [11]就是密码模块安全要求事实上的国际标准，旨在规范密码模块的设计、实现、使用及销毁过程涉及的技术与流程。在我国，国家密码管理局分别于2012年11月22日和2014年2月13颁布了《安全芯片密码检测准则》及《密码模块安全技术要求》 [12]，旨在为选择满足应用与环境安全要求的密码芯片提供依据，并为密码芯片的研制提供指导。上述国际与国家标准制定的指导思想与技术细节略有差异，但都要求密码芯片对密钥和敏感信息提供保护。

在密码芯片众多安全要求中，具有优良的侧信道安全性是密码芯片的一项共性技术要求。然而与严格而清晰的安全需求现实相比，密码芯片的侧信道安全性分析与检测技术研究面临着严峻的科学方法与巨大的工程技术挑战。

* 该图是在Thomas Roche （机构：French Network and Information Security Agency (ANSSI), Email: thomas.roche@ssi.gouv.fr) 画出的侧信道攻击示意图的基础上修改而成。

针对密码芯片的侧信道安全性分析与检测包括密码芯片的抗侧信道攻击能力分析，以及密码芯片的泄漏水平或安全水平评估两个方面 [13,14]。其中，侧信道分析技术考察的是密码芯片的抗侧信道攻击能力，而侧信道检测技术考察的则是密码芯片的泄漏水平或安全水平。目前面向密码芯片的侧信道分析方法与检测技术的研究主要是在密码芯片侧信息泄漏充足及侧信息泄漏不足两个场景下展开，其技术框架如图 1.4 所示。前一个场景下分析者能够实施成功的侧信道攻击或准确刻画密码芯片侧信息泄漏水平；后一个场景下分析者获取的侧信息泄漏不足以实施成功的侧信道攻击或无法准确刻画密码芯片侧信息泄漏水平。

在分析者能够获取充足的密码芯片侧信息泄漏的场景下，如果从侧信道分析所利用的侧信道数目的角度出发，那么可以发现侧信道分析研究主要沿着两个技术路线发展：单信道分析和多信道分析 [15]。单信道分析的技术思路是发现并利用单个侧信道泄漏，如声 [4]、光 [5–7]、电磁 [3]等，目前发展已相当成熟。不过，传统单信道分析只是孤立地利用密码芯片某一形式的物理泄漏，只能有限程度地反映密码芯片的侧信道安全性，无法满足现实分析与检测需求。与单信道分析相比，多信道分析综合利用多个侧信道的泄漏，以期超出单信道分析局限、提高分析效率 [15]。随着现在测量手段越来越先进，有关多信道融合攻击的研究越来越迫切，然而目前此方面的研究较少，难以为全面、深刻地分析密码芯片的侧信道安全性提供技术支撑 [16]。

在分析者能获取充足的密码芯片侧信息泄漏的场景下，侧信道检测技术考察的是密码芯片的泄漏水平，即密码芯片的泄漏量大小。而密码芯片泄漏量的大小可通过两个方面评估，即密码芯片泄漏信号中与密钥相关的泄漏点的泄漏量大小，及这些泄漏点数目的多寡。因此，侧信道检测技术可分为泄漏评估及泄漏检测技术两大类。其中，泄漏评估技术考察的是密码芯片泄漏信号中与密钥相关的泄漏点的泄漏量大小，泄漏检测技术考察的则是这些泄漏点数目多寡。不过，已有的泄漏评估与检测技术难以兼得精度与效率 [17,18]，亟需进一步发展。

而在分析者获取的密码芯片侧信息泄漏较为匮乏的场景下，侧信道分析技术主要分为两类：代数侧信道攻击 [19]和密钥枚举技术 [20]。代数侧信道攻击需要根据具体算法列代数方程组求解，效率较低，且容错性差。密钥枚举技术则对密码算法的依赖性小，灵活性及容错性较强。鉴于此，本文将主要关注密钥枚举技术的研究。密钥枚举技术考察了在对密码芯片进行侧信道分析后，得到真实密钥所需的枚举次数。因此，密钥枚举技术适用的前提是真实密钥在所有密钥候选值中的排序位置未超出分析者的计算能力。若真实密钥在所有密钥候选值中的排序位置超出了分析者的计算能力，要分析密码芯片的侧信道安全性，只能使用密钥排序技术 [14,21]。密钥排序技术属于侧信道检测技术，考察了密码芯片的安全水平——该指标刻画了真实密钥在所有密钥候选值排序中处于某一位置的可能性。密钥枚举与密钥排序技术的密码算法依赖性不大、适用性广，近年来得到越来越多的研究 [21]。但现有密钥枚举算法皆是在不改变真实

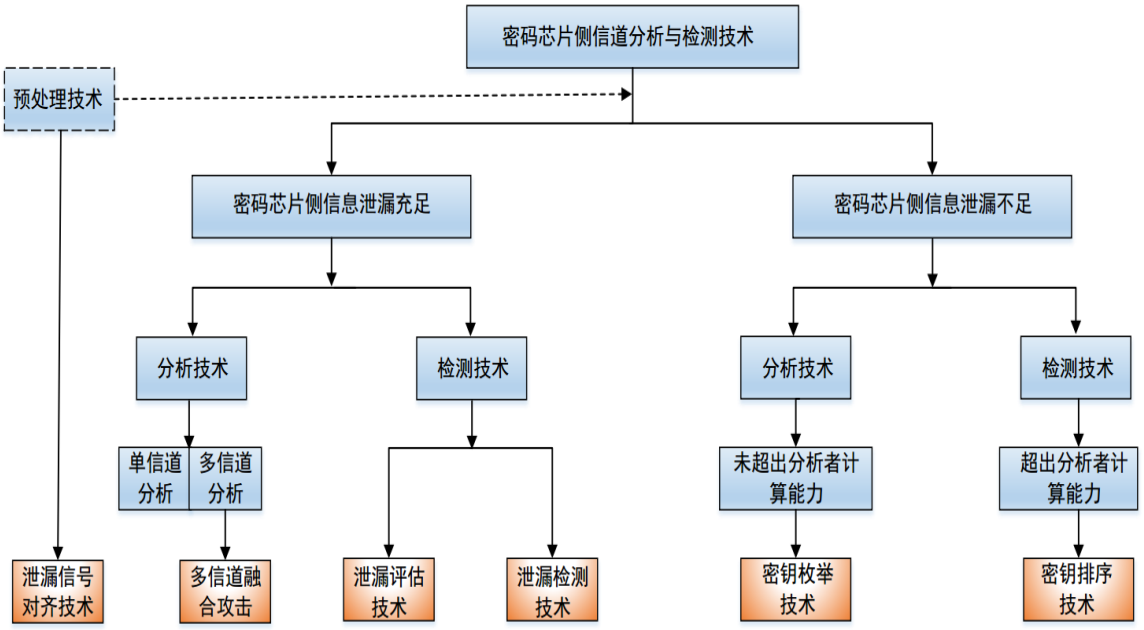


图 1.4 本文研究框架及研究内容示意图

密钥排序位置的前提下，优化密钥枚举的计算效率及存储结构的，并未从根本上改变密钥枚举的效率。而有关密钥排序的研究则大多按密钥后验概率排序，效率较低，且未考虑子密钥相关性的影响，需待发展。

此外，实际采集到的密码芯片侧信道泄漏信号常常因诸如采集时芯片噪声较大或加入了防御对策 [23–31]等因素影响，不宜直接用于侧信道分析与检测，否则可能会极大降低侧信道分析与检测效率 [10]，甚至使之变为不可能。所以在针对密码芯片进行侧信道分析与检测之前，需对泄漏信号进行预处理，以提高侧信道分析与检测效率 [10]。影响密码芯片侧信道分析与检测效率的两大常见因素是噪声及泄漏信号失调（即密码实现运行中同一操作的同一侧信道泄漏在各条泄漏信号中不在同一时刻发生） [32,33]。对于前者，可利用成熟的信号处理技术来抑制噪声、提高信噪比。而对于后者，需利用泄漏信号对齐技术处理，但该方面的研究尚不充分 [32,34]，有待进一步发展。

本论文拟从以上两个场景出发，围绕面向密码芯片的侧信道分析与检测的关键技术，重点研究泄漏信号对齐技术、多信道融合攻击技术、泄漏评估与泄漏检测技术，以及密钥枚举与密钥排序技术等方面的内容。本文研究旨在为开展面向密码芯片的分析与检测实践提供方法手段与技术支撑，提升密码芯片的分析与检测技术水平。该项研究不仅具有重大的学术价值和现实意义，而且由于密码芯片物理安全分析与检测技术的高度敏感性，同时具有重要的战略意义。

1.2 国内外研究现状

本章节将详细介绍侧信道分析与检测领域中，有关泄漏信号对齐、多信道融合攻击、泄漏评估与泄漏检测，以及密钥枚举与密钥排序等重要问题的国内外研究现状。

1.2.1 泄漏信号对齐

大部分侧信道攻击技术因沿着时间轴对每个时刻的泄漏信号逐个进行统计分析，故需保证每条泄漏信号中对应于同一依赖于秘密信息的中间值是在同一时刻产生的。其中非建模类技术，例如DPA类攻击技术，利用与秘密信息相关的敏感中间值的泄漏来进行统计分析，从而获得秘密信息。如果每条泄漏信号中与敏感数据相关的泄漏点不是在同一个时刻采集的，就会引入无关噪声信号，从而降低DPA类攻击技术的分析效率，甚至使该类攻击不可行。而建模类攻击技术，如模板攻击，其攻击前需准确刻画泄漏模型 [35]，更要求与敏感数据相关的泄漏点在时域上严格对齐。否则就需要使用大量的泄漏信号来满足精度要求，计算代价会急剧增加，甚至使分析失去实际可操作性。同样地，如果密码芯片的泄漏信号失调，也会严重影响侧信道检测的准确性。

然而在实际中，密码芯片可能会因触发信号不能与时钟信号保持精确同步，导致采集到的侧信道泄漏信号在时间轴上发生随机时延 [10,36]；或者因采用了针对时间维度防护的隐藏技术，如乱序（将运算中的操作打乱，并不高效，且对并行实现无意义）[28,37]、随机插入伪操作（Random Process Interrupts，简写为RPIs，即在运算中加入无意义的随机延迟或随机伪操作） [10,38,39] 和随机变化芯片工作时钟频率（随机变化加解密运算过程中的时钟频率） [40–42] 等，从而使得采集到的泄漏信号在时域上无法对齐。因此，在实施侧信道攻击前，很有必要对采集到的侧信道泄漏信号进行对齐预处理，以降低计算代价，提高侧信道分析效率与检测准确度。

一般来说，根据泄漏信号的信息利用方式不同，可将现有研究提出的泄漏信号对齐技术分为两类：局部对齐技术和全局对齐技术 [34]。其中，局部对齐技术通过提取泄漏信号所共有或相似的模式或特征部分，并依据相似性来匹配、对齐这些模式或特征部分。例如，静态对齐就是一种典型的局部对齐技术 [10]。静态对齐技术可用来消除触发信号不同步带来的泄漏信号不对齐的影响。它首先选取参考泄漏信号，并从中截取一个对应于某一加密或解密操作的信号段作为模式，然后在其它泄漏信号中依次寻找最相似的信号段来匹配，再移动这些信号段并对齐 [43]。显然静态对齐的精度取决于所选择的模式，但在噪声较大的环境下选择模式可能非常困难。这时需要先对泄漏信号进行滤波等处理，以凸显模式特征。然而，当密码芯片时钟频率过高时，泄漏信号中会包含大量电子、算术及量化噪声，几乎不可能通过常规的滤波技术选择一个正确的模式。这种情况下，文献 [44] 使用一个对相位变化敏感的检测器，对原始未对齐泄漏信号滤波，以增强泄漏信号中的模式特征并使之显现。文献 [45]使用互相关分析来检测泄漏信号中可区分及重复的模式，从而将插入了随机伪操作的密码实现的泄漏信号对齐。文献 [46]同样利用了模式匹配技术，将密码实现中的一些连续操作的汉明重量转化为字符串表示，然后使用字符串匹配技术检测并消除随机插入伪操作带来的影响。文献 [47]则提出了水平对齐技术，能够消除因芯片工作时钟变化所造成的泄漏

信号失调的影响。该技术通过搜寻POIs (Point of Interests)，并匹配这些点组成的模式来对齐。文献 [48,49] 在此基础上进行了改进提高。另一些基于时频分析的对齐方法也相继提出。例如，文献 [50]基于小波变换寻找参考泄漏信号及待对齐泄漏信号中的POIs，之后通过拉伸或压缩操作来对齐这些点。文献 [51]则根据信号时移对应相移这一性质，提出了基于短时傅里叶变换的技术来对齐泄漏信号。而文献 [52]提出了另一种基于加窗信号能量谱密度的策略，能够有效去除随机插入伪操作的影响。不过，局部对齐方法的主要缺点是易丢失部分与密钥相关的泄漏信息，且严重依赖人工参与，比如经验性地选择模式 [10]，不同的设备需要重复调节复杂的算法参数 [47]等等。这使得局部对齐算法在实际中可能较难实施。

相较之下，全局对齐技术直接利用泄漏信号的全局结构模式或特征来对齐泄漏信号。从这个角度看，一些直接在原始泄漏信号上进行处理的算法，例如滑窗DPA对齐 [53]及整合攻击 [10,54]等等，可归属于全局对齐一类。其中滑窗DPA对齐通过使用一个滑动窗口将泄漏信号多个点整合为一个点，来减轻泄漏信号失调对DPA攻击的影响。整合攻击类似滑窗DPA对齐，也能有效减轻泄漏信号时域失调对侧信道攻击的影响。文献 [36]改进了整合攻击，提出了一种基于四阶累积量的方法来减弱泄漏信号失调的影响。因高斯随机过程的二阶以上累积量为0，所以该方法还能有效消除高斯噪声。其它类似的方法还有诸如基于卷积的对齐 [10]等等。虽然以上这些方法在实际中简单易行，能够提高侧信道分析效率，但是它们会丢失部分泄漏信息，只能在有限程度上消除泄漏信号时域失调的影响 [10]。另外一些研究则换了视角，在频域上对齐泄漏信号，如信号经离散傅里叶变换后，利用信号幅度谱与时移无关或信号相移与时移对应的性质，分别发展出基于幅度相关 [55,56,59,60,62]和相位相关的泄漏对齐技术 [50,55,57,58,61]。这些技术在频域对泄漏信号处理后，将频域的相关信息反变换到时域上获得对齐信号。然而这些方法并未充分利用泄漏信号的信息，要么只利用了泄漏信号的幅度谱，要么只利用了泄漏信号的相位谱。而且，所有的这些频域对齐技术可行的前提是泄漏信号序列内呈现周期性特征。这很大程度上限制了它们的适用范围。此外，文献 [63]为了攻击采用了随机变化时钟频率防御对策的智能卡，提出了基于小波变换去噪、再使用模拟退火技术对齐的方法。不过该方法可能会丢失部分与密钥相关的泄漏信息，进而影响信号对齐后侧信道攻击效率的提升。而且，模拟退火算法可能会严重影响对齐算法的计算效率。文献 [32]则独辟蹊径，提出了基于动态时间规整（Dynamic Time Warping，简写为DTW）的对齐技术，用来避免对齐过程中泄漏信息的损失，不过却会引入冗余信息，导致计算代价较大。

1.2.2 多信道融合攻击

侧信道攻击技术已经得到学术界及产业界极大关注。相应地，多种类型的侧信道攻击方法被提出来，例如多元高斯模板攻击 [35]、多元差分攻击 [64]、代数侧信道攻击

[19,65–70]、组合攻击 [71,72]及多信道融合攻击 [15]等等。其中，多信道融合攻击同时利用多个信道的侧信息泄漏来进行侧信道分析。相比单信道攻击，多信道融合攻击具有很高的潜在信息利用率，具有将侧信道分析效率提高到单信道攻击无法达到的水平的可能性。一个恰当实施的多信道融合攻击应能充分利用多个侧信道的泄漏信息，从而比单信道攻击性能更优越、更具威胁性。随着检测手段越来越先进，多信道泄漏采集变得愈加容易（如现在的示波器可以同时采集密码芯片总体能量消耗以及不同位置的电磁泄漏），相应分析技术的研究需求也越来越迫切。发展多信道融合攻击技术，有利于更全面、客观地研究密码芯片的侧信道安全性，满足更深层次的现实分析需求。

然而现有的侧信道攻击多是利用单个侧信道泄漏信息进行分析，关于多信道融合攻击的研究很少，且既有研究基本是从攻击的角度出发，根据经验尝试，较为零散，并没有建立起一个统一的框架进行系统性的研究，导致在不同应用场景下很难指导分析者如何进行高效的融合攻击，不利于全面而深入地评估密码芯片的安全水平。为了在一个统一框架下系统研究和深入理解多信道融合攻击，我们从融合本身而不是攻击的角度出发，借鉴图像融合的分类方法 [73]，将多信道融合攻击方法分为三类：数据级融合攻击方法，特征级融合攻击方法，以及决策级融合攻击方法 [16]。其中，数据级融合攻击方法是指通过某种计算或操作（如串联、相加等）合并不同信道的侧信息泄漏信号，产生一个新的侧信息泄漏信号，然后对其实施单信道攻击。特征级融合攻击方法是指首先提取不同信道的侧信息泄漏信号中与密钥信息相关的泄漏特征集，然后再使用这些特征集实施单信道攻击。这些特征集可以由所有侧信道的侧信息泄漏信号的联合特征组成，也可以通过合并提取自单个信道的与密钥相关的侧信息泄漏特征集获得。决策级融合攻击方法则是指那些分别从不同信道发动单信道攻击，再综合所有单信道攻击结果得出最终攻击结果的一类融合攻击方法。

目前的研究中, 文献 [15]提出了两种数据级多信道融合攻击方法。这两种融合攻击方法简单地将多个侧信道的泄漏信号串接构成新的泄漏信号，并分别进行单信道DPA攻击和单信道模板攻击。然而，这两种方法要求对应于同一敏感中间值的多个信道的泄漏必须同时发生。文献 [74]则提出了另一种数据级融合攻击方法。该方法首先使用同一个探针放在FPGA芯片上多个相连的位置，测量实现在FPGA上的椭圆曲线标量乘法对应的电磁（Electromagnetic, 简写为EM）泄漏。之后，对这些不同电磁通道泄漏进行主成分分析提取主成分，然后组合在一起实施攻击，以提高基于聚类的非建模类攻击算法的效率。接着，文献 [75]做了类似的工作，只不过使用了多个不同直径的电磁探针同时探测不同电磁通道的泄漏。该方法属于特征级融合攻击方法。在文献 [76]中，两个分别基于主成分分析和线性判别分析的特征级融合攻击方法被提了出来。这两种融合攻击方法首先使用主成分分析或线性判别分析处理能量泄漏和电磁泄漏信号，随后将处理过的两个泄漏信号集合串联构成一个新的集合，再实施单信道模板攻击。文献 [77]最早介绍了一种决策级融合攻击方案。该方法同时联合RSA实现的能量泄

漏和时间信息来分析RSA。而文献 [78]则提出了另外两种决策级融合攻击算法。这两种融合攻击方法（本文分别标记它们为Max_FA和Sum_FA）先分别在多个电磁泄漏通道，通过相关系数区分器计算一个假设密钥在这些单信道电磁攻击中得到的分值，之后选择这些分值中的最大值（Max_FA）或这些分值的和（Sum_FA）作为该假设密钥的最终分值。在计算出所有假设密钥的分值后排序，取分值最大的假设密钥作为密钥猜测。

此外，另一个与多信道融合紧密相关的研究——泄漏融合判别标准研究，目前仅极少数工作涉及。多信道泄漏融合判别标准的作用是判断两个信道的泄漏是否适于融合，属于多信道融合攻击前的工作。文献 [15]和 [78]中提出过这类度量标准，它们分别使用信噪比和概率来刻画两个信道是否可以联合，不过要计算这两个指标，需要预先知道密码算法所用的密钥并进行刻画，然后才能计算指标值以进行判断。

1.2.3 泄漏评估与泄漏检测

现在侧信道攻击已经对密码芯片的物理安全性构成了严重威胁 [79–81]，对一个密码芯片的侧信道安全性进行分析和检测变得愈来愈重要且必要。上两个小节介绍的泄漏信号对齐及多信道融合攻击属于侧信道分析技术，考察的是密码芯片的抗侧信道攻击能力，亦即分析者利用密码芯片泄漏的能力。而在分析者能获取充足的密码芯片侧信息泄漏的场景下，侧信道检测技术考察的是一个密码芯片的侧信息泄漏量。密码芯片泄漏量的大小评估包括密码芯片泄漏信号中与密钥相关的泄漏点的泄漏量大小，及这些泄漏点数目多寡两个方面。这两个方面的评估可分别使用泄漏评估及泄漏检测技术来处理。下面分别介绍泄漏评估技术及泄漏检测技术的发展现状。

泄漏评估技术考察的是密码芯片泄漏信号中的与密钥相关的泄漏点的泄漏量大小。目前已经有大量与侧信道泄漏评估相关的研究 [13,14,25,82–86]。已有的密码芯片泄漏信息量度量标准包括信噪比（Signal-to-Noise Ratio，简写为SNR） [87]、相关系数 [88,89]、标准化类内方差 [90,91]、矩相关DPA [25,92]、感知信息 [89,93]、互信息（Mutual Information, 简写为MI） [82]及本质上和互信息等价的条件熵 [13]，等等。在这些度量标准中，互信息因为具有清晰明确的信息论含义而被广泛用来度量密码芯片的侧信息泄漏量。然而，实际中分析者对一个密码芯片侧信道泄漏的真实分布很难了解清楚，使得计算密码芯片的互信息较难进行，继而导致对密码芯片侧信息泄漏进行评估比较困难 [94]。此时，需要近似估计密码芯片的侧信道泄漏分布。一般地，两类方法常被用来估计密码芯片的泄漏分布，即参数类估计方法和非参数类估计方法。非参数类估计方法通过假设密码芯片的泄漏模型，如汉明重量、汉明距离、比特模型 [95]等等，然后使用非参数类方法（例如直方图和核密度估计 [94,96]）估计出密码芯片的侧信息泄漏分布。在很多情况下，非参数估计方法效率较高，但会因泄漏模型假设不准确等因素带来比较大的假设误差 [89]。参数类估计方法则通过一些参数估计方法来刻画密码芯片的侧信息泄漏分布，例如高斯模板 [89]、回归模型 [94]、指数修正的高斯模

板和转移广义对数正态模板 [18]等等。参数类估计方法需要大量侧信道泄漏信号来刻画密码芯片的泄漏分布，精度较高，但在实际场景中可操作性不强。

泄漏检测考察的是密码芯片泄漏信号中的与密钥相关的泄漏点数目多寡，是侧信道检测研究中的一个重要内容。目前来看，侧信道泄漏检测技术大体上可分为两类：基于攻击的泄漏检测技术与基于统计的泄漏检测技术。基于攻击的检测技术利用侧信道攻击来寻找与秘密信息相关的泄漏特征点，跟密码算法密切相关；基于统计的检测技术则只依赖于所使用的统计工具和采集到的泄漏样本点，与密码算法关系不大，适用性更强，因此近年来得到重点研究。现在基于统计的泄漏检测技术研究多是建立在T-test检测基础上。这一大类方法将采集到的密码芯片的两个侧信道泄漏信号集合看作两个正态分布的样本总体，然后通过T-test假设检验来考察它们之间是否存在显著差异，而存在显著差异的时刻所对应的样本点即被认为包含可被利用的依赖于秘密信息的泄漏 [17,97–102]。这一类方法一般对做T-test假设检验的两个侧信道泄漏集合的采集有特殊要求，如需要知道密钥 [97]，或者要求两个侧信道泄漏集合中相应信号对应的密码算法输入一个固定、一个随机 [101]，或者两组输入都相同 [98]等等。而且，T-test假设检验适用于正态分布总体，只考虑了样本的均值和方差，所以基于T-test的泄漏检测技术一般检测出的可能包含秘密信息泄漏的样本点，数目较大且大多无益于攻击。鉴于此，文献 [17]提出了一种基于相关系数和交叉验证的泄漏检测方法，能够检测出可用于相关分析的POIs，但该方法要求侧信道泄漏信号数目较多且对应的输入必须遍历所有可能的取值。文献 [90,91]提出了基于标准化类内方差的泄漏检测技术，该技术只依赖明文或密文，通过每个时刻的泄漏信号的总方差来找到与某个敏感变量相关的泄漏特征点。该方法不需要对密码芯片泄漏分布进行刻画，但包含参数较多，需要人工精细调节，较为繁琐 [103–105]，而且该方法本质上与基于T-test的泄漏检测技术是等价的 [106]。文献 [101]则提出了一种基于互信息的泄漏检测技术。该方法需要知道子密钥。还有一些研究，例如文献 [95]提出的基于方差的泄漏检测技术，对泄漏信号的采集并无特殊要求。该技术通过对比不同密码算法输入的侧信道泄漏信号的均值的方差来检测泄漏。该方法能够找到泄漏信号中的POIs。不过因其只利用了泄漏信号的均值和方差信息，故而无法找到全部的POIs，且会引入少量对攻击无用的样本点。

1.2.4 密钥枚举与密钥排序

一般侧信道攻击（如DPA [107]、模板攻击 [35]、互信息分析 [84]、线性回归 [108]等）都是基于分治的策略来恢复密钥 [13,82]，即在采集到密码芯片的侧信道泄漏信号（如能量泄漏、电磁泄漏等）之后，每次单独地使用一个侧信道区分器计算出所有子密钥可能值对应的分数，降序排列后分别选择排在第一位的值作为子密钥的猜测值，然后联合所有的子密钥猜测值得到完整密钥的猜测值 [109]。当分析者获取的侧信道泄漏量足够多时，如果将区分器计算出的所有子密钥猜测值按其分数降序排列，此

时真实子密钥应该排在第一位，从而使得完整的真实密钥在所有密钥可能值排序中排在第一位 [53,85,87,110–114]。

但是，如果分析者获得的侧信道泄漏信息不足以实施一次成功的攻击，例如受设备限制只能采集少部分侧信道泄漏信号，或者一些子密钥受保护而导致无法由攻击获得 [14,23–31]，等等。此时真实密钥对应的区分器分数不是最高，但较某一些密钥候选值高些，导致真实密钥排在所有密钥候选值中间某一位置。这种情况下，就需要借助其它技术，利用密码算法结构及实现等有关信息进行密钥枚举，并使用明密文对验证，来寻找真实密钥。目前针对侧信息不足时侧信道分析技术的研究主要集中在两大部分：一是代数侧信道攻击技术；二是密钥枚举技术。

代数侧信道攻击是指在侧信道攻击获取的有限的秘密信息的基础上，利用密码算法的结构及实现信息，找出以密钥比特为变量的方程组，并通过解方程的方法来恢复密钥，如传统代数侧信道攻击 [65,68,70]、软分析代数侧信道攻击 [19,69]、立方攻击 [66,67]等等。然而，代数侧信道攻击的效率取决于其所构建的方程组的准确程度。在实际攻击场景中，由于实测的侧信道泄漏都是有噪的，导致方程组并不精确，求解所得的结果并不可靠。虽然现有的研究考虑到了代数侧信道攻击中的容错性问题，但整体看它们的容错性依然非常弱。而且代数侧信道攻击技术与密码算法联系紧密，具体算法需要具体分析，列代数方程组的工作比较繁重，灵活性差。密钥枚举技术则是在对从侧信道攻击中得到的各个子密钥候选值的分数排序后，直接从子密钥排序着手，研究如何高效地枚举主密钥候选值，从而恢复出真实主密钥 [20]。该方法除了在使用明密文对验证密钥猜测是否正确时需要涉及密码算法外，其它步骤基本不涉及密码算法，可移植性好、灵活性强，近几年逐渐成为重要研究内容 [115]。鉴于此，本文将主要关注密钥枚举技术的研究。

目前已有的密钥枚举算法大都与最优密钥枚举算法 [20]有关系。最优密钥枚举算法首先计算每个子密钥所有候选值的分数并降序排序，利用贝叶斯定理将不同子密钥候选值分数转化为后验概率，在假设任意两个子密钥独立的前提下，将不同子密钥候选值后验概率相乘，得到主密钥候选值的后验概率，并按其降序枚举，同时使用明密文对验证，直至恢复出主密钥。由于需要按概率从大到小一一枚举主密钥候选值，该算法需要占用大量的内存，实际应用时效率很低。特别是在分析者所获取的侧信道泄漏信号噪声较多时，该算法运行时间和内存需求会急剧增长。从概率论角度来看，相较之前的密钥枚举算法 [116–118]，最优密钥枚举算法的效率是最优的。在最优密钥枚举算法提出之后，为提高其实用性，有关研究开始转向于如何提高最优枚举算法的运行效率，并减少算法内存需求。例如，文献 [119]提出了一种基于子密钥候选值分数排序的密钥枚举算法。从主密钥概率分布来看，该算法是一种次优枚举算法，但其运行时所需内存及所用时间都比最优枚举算法小，在时间及内存资源受限的场景下尤为实用。而文献 [22]则另辟蹊径，使用卷积计算来加速最优枚举算法。其思路是：因为假设

各个子密钥独立，所以主密钥的概率密度函数是各个子密钥概率密度函数的乘积，对其取对数则变为求和关系。由统计知识可知，多个独立离散随机变量和的概率分布函数是这些随机变量和的概率分布函数的卷积和。于是密钥枚举问题就转化为了一个迭代求卷积和的问题。又由于计算机卷积的求解一般基于傅里叶变换，速度远远超过最优密钥枚举算法中使用的启发式算法 [20]，大大提高了最优枚举算法的计算效率，且内存需求更少，更加实用。文献 [115]结合了文献 [22]中的密钥枚举技术和文献 [119]中并行密钥枚举算法的优点，进一步提高了密钥枚举效率。据作者了解，该算法是目前密钥枚举算法中效率最高的。文献 [86,120]则将密钥枚举问题转化为寻找计数背包问题解的个数的问题，并结合图论将后者转化为寻找有向无环图的关键路径数目问题。为了提高枚举计算的时间和空间效率，该算法采用了并行枚举技术，并使用树的数据结构存储数据。此外，文献 [121]提出了一种次最优的密钥枚举算法，采用分层方法，将子密钥候选值分成不同的层，以层为单位进行密钥搜索。该层次化方法通过不断缩小每一次密钥枚举的范围，从而有效缩小密钥枚举的复杂度，尤其适用于内存受限的场景。作者同时给出了主密钥猜测熵的界，讨论了该枚举算法的次最优性。

不过，密钥枚举技术适用的前提是分析者的计算能力（以现在的计算能力而言，约为2^{40}～2^{50} [21]）足以枚举出真实密钥。如果真实密钥的排序位置较为靠后，超出了分析者的计算能力，密钥枚举就会变得不可行。例如，假设真实密钥在所有密钥候选值排序中排在第2^{80} 位，那么我们就无从得知密码芯片的安全水平到底是2^{51}还是2^{120}。此时上述密钥枚举技术不再适用，密码芯片的安全水平如何描述就会成为一个问题。在这种场景下，要估计密码芯片的安全水平，只能使用密钥排序技术 [21]。

密钥排序是在已知真实主密钥的前提下，联合各个子密钥在其相应候选值中的排序，估计出真实主密钥在所有主密钥候选值中的排序。密钥排序与密钥枚举非常接近，但除了需要知道真实主密钥之外，密钥排序不必枚举出在真实主密钥排序位置前的所有主密钥候选值，只需估计出真实主密钥的排序位置即可。最早研究密钥排序技术的是文献 [14]。其提出的密钥排序算法基于最大似然估计原则，以各个子密钥所有候选值的后验概率（降序排列）为输入，并组合子密钥构成密钥搜索空间，通过不断迭代，寻找经过真实主密钥排序位置的凸曲线，从而将密码芯片安全水平的评估问题转化为了凸优化问题。然而该密钥排序算法的收敛性不好，受密钥空间组合方式的影响较大，只能得出一个有关密码芯片安全水平的上下界。且当真实密钥在所有密钥候选中排序较为靠后时，该算法便无法使用 [22]。例如对密钥长度为128-bit的高级加密标准算法（Advanced Encryption Standard, 简写为AES-128） [122]而言，当其真实密钥排序位置超过2^{80}时，该密钥排序算法就会失效。而文献 [22]中提出的密钥枚举算法，同样可变化为密钥排序算法，并且远比文献 [22]中的算法高效、实用，能够得到一个收敛的密码芯片安全水平估计。文献 [115]中的密钥枚举算法是文献 [22]中所提方法的改进版本，也同样适用于密钥排序，而且效率和精度更高。文献 [123]同样改进了文献 [14]提

出的密钥排序算法，并给出了一个与密钥芯片安全水平上下界有关的置信度区间。此外，文献 [123]还提出了一种基于多项式乘法的密钥排序算法。该算法是一种非迭代的算法，可通过预置参数来调节估计精度。文献 [124]在此基础上，稍作变化，提出了另一种基于弱最大似然概率的密钥排序算法。与基于最大似然概率的算法 [14]取每个子密钥所有候选值用来主密钥排序不同，文献 [124]中的算法只取每个子密钥一部分候选值，以使主密钥的恢复成功率达到或超过某个预设值为条件限制，以枚举次数最小化为目标，将密码芯片安全水平评估问题转化为一个优化问题。而文献 [25]提出的算法与文献 [124]中的算法相反，是以枚举次数最小化为条件限制，以最大化主密钥的恢复成功率为目标，相比文献 [124]更合理。不过该算法为了提高效率，使用了基于均匀采样的降采样技术，要求每次得到的密钥成功率与枚举次数之间的曲线平滑且单调递增，否则可能采样失真，影响评估精度。而文献 [86]所提出的基于计算背包问题的密钥枚举算法同样可转化为密钥排序算法，而且适当调节参数可得到精度较高的结果。文献 [21]则第一次将已有的密钥排序算法分类并对比，然后组合各类算法进行对比、验证。该工作可视为文献 [14,86,123]中工作的延伸。此外，文献 [125]提高了文献 [86]中密钥排序算法的精度，并对密钥排序位置所服从的分布进行了理论刻画。

1.3 存在的问题

本节将对目前有关泄漏信号对齐、多信道融合攻击、泄漏评估与泄漏检测，以及密钥枚举与密钥排序等研究存在的问题进行总结。

1.3.1 泄漏信号对齐

目前关于对齐技术的研究存在的主要问题是对齐过程中容易造成部分依赖于密钥的泄漏信息丢失（如文献 [10]），或者会引入冗余信息（如文献 [32,63]）。其它的问题还有诸如一些方法抗噪声性能差（如静态匹配技术 [10]），参数调节繁琐（如文献 [47–49]中方法需要仔细选择大量参数），对泄漏信号的性质有很强限制（如文献 [50,55–62]要求泄漏信号必须是周期信号），只能较小程度地消除泄漏信号失调的影响（如滑窗DPA对齐 [53]及整合攻击 [10,54]）等等。这些问题影响了现有泄漏对齐技术消除泄漏信号失调影响的效率，从而影响了侧信道分析与检测效率的进一步提升。

1.3.2 多信道融合攻击

可以看出，以前的多信道融合攻击研究不但较少，而且皆从具体的攻击出发，并未在一个统一的研究框架下进行，较为散乱。此外，已有研究工作仅仅只是构造了某一种特定类型的多信道融合攻击方法，攻击针对的也只是某种密码算法的一种特定实现。因此，根据现有研究，面对一个密码算法的不同实现，很难在如何选择高效的多信道融合攻击策略这一问题上，找到解决思路。另外，已有融合攻击方法或多或少存在改进的余地。例如，文献 [15]中的多信道DPA要求对应于同一敏感中间值的多个信道

的泄漏点在时间上必须同时发生，文献 [76] 提出的建模类特征级融合攻击方案在实际场景中可操作性差，而文献 [78]提出的两个融合攻击方法Max_FA和Sum_FA并未充分考虑不同信道的贡献，无法充分利用每个单信道攻击结果，等等。

进一步地，以前多信道融合攻击方法采取的皆是第一类融合方式，没有一种方法采用了第二类融合方式。也就是说，以往的研究并未考虑到不同融合方式对多信道融合攻击效率的影响。除此之外，目前仅有的两个多信道泄漏融合判别标准 [15,78]，计算时需要知道密码算法所用的密钥，在实际中可能不可行。

1.3.3 泄漏评估与泄漏检测

目前用于侧信道泄漏评估的两种常用方法是参数类估计方法和非参数类估计方法。非参数类估计方法因为在估计密码芯片的侧信息泄漏分布之前，需要假设密码芯片的泄漏模型，所以常会带来比较大的假设误差 [89]。而参数类估计方法通过刻画密码芯片的侧信息泄漏分布达到较高精度，但需采集大量侧信道泄漏信号，实际可操作性差。

此外，基于攻击的泄漏检测技术需要知道密钥或大量泄漏信号，跟密码算法密切相关，受限较大；而多数基于统计的检测技术只利用了泄漏信号的均值和方差信息。这些技术大多会检测出大量无益于攻击的泄漏点，且对泄漏信号的采集要求较多。

1.3.4 密钥枚举与密钥排序

目前密钥枚举算法多基于最优密钥枚举算法 [20]发展而来，即依据最大似然原则得到相应主密钥候选值的后验概率，然后按照后验概率大小依次枚举主密钥候选值。从概率角度来看，最优密钥枚举算法是最优的。然而，当完成一个特定侧信道攻击后，真实主密钥在所有主密钥候选值中的排序位置业已确定，最优密钥枚举算法只是在优化存储结构、加快计算效率上下功夫，并没有改变真实主密钥在所有主密钥候选值中的排序。而真实主密钥在所有主密钥候选值中的排序位置才是决定密钥枚举次数的根本因素。但是目前并没有关于提升真实密钥排序位置的研究。

在真实密钥在所有密钥候选值中的排序位置超出了分析者的计算能力时，利用子密钥候选值的位置排序来估计真实主密钥位置，与利用子密钥候选值的后验概率排序来估计真实主密钥位置是有区别的。在已知真实密钥的情况下，按前者评估密码芯片的安全水平往往比后者更高效 [21,25,124]。目前仅有文献 [25,124]是按子密钥候选值的位置排序来估计真实主密钥位置的，然而文献 [124]中的假设不如文献 [25]合理，而后者精度有待提高。此外，以前的密钥排序算法都是建立在各个子密钥相互独立的假设基础上，并未考虑子密钥相关时如何评估密码芯片的安全水平。

1.4 研究内容

本文研究内容包括泄漏信号对齐技术、多信道融合攻击技术、泄漏评估与泄漏检测技术，以及密钥枚举与密钥排序技术四个方面。下面分别简要介绍。

1.4.1 泄漏信号对齐

首先，本文将从信息利用方式的角度，对泄漏信号对齐技术进行分类，并在此框架下讨论、分析对齐技术。其次，鉴于目前关于对齐技术的研究中存在的主要问题，本文将在保证既不丢失与密钥相关的泄漏信息，也不引入冗余信息的前提下，研究对齐效率较高的泄漏信号对齐技术，以期能较彻底地消除泄漏信号失调的影响，提升侧信道分析效率与检测准确度。在此基础上，对已有对齐方法中存在的其它问题，诸如抗噪性差、参数调节繁琐、对泄漏信号性质限制强等等，本文也希望能有所改进。

1.4.2 多信道融合攻击

鉴于目前多信道融合攻击研究存在的问题，本文将根据多信道融合攻击中所利用的侧信道泄漏信息形式及方式的不同，首先将多信道融合攻击分类，然后在此统一框架下进行研究。本文除了将在不同应用场景下验证不同种类多信道融合攻击的效率外，还将考虑不同融合方式是否会对多信道融合攻击产生显著影响。我们希望通过对多信道融合攻击的研究，可以为针对不同密码实现采用何种高效的多信道融合攻击提供建议，从而能更全面、深刻地研究密码芯片的侧信道安全性。最后，本文还将重点关注多信道泄漏融合判别标准的研究，以便构造出一个无需知道密钥便可进行计算的度量标准，并保证该度量标准在实际中的计算是高效可行的。

1.4.3 泄漏评估与泄漏检测

鉴于目前用于侧信道泄漏评估的参数类估计方法和非参数类估计方法各自的优缺点，本文希望能够联合这两类估计方法的优点，找到一种方法，既像非参数估计方法一样实际可操作性强，也像参数估计方法一样精度高。另外，本文希望构造一个基于统计的泄漏检测技术，能充分利用泄漏信号的信息，以期检测出的可直接用于攻击的POIs尽可能的多，同时检测出的对攻击无用的泄漏样本点尽可能的少。

1.4.4 密钥枚举与密钥排序

由于目前的密钥枚举算法并没有改变真实主密钥在所有主密钥候选值中的排序，本文将研究侧信息不足时，如何提升真实主密钥在所有主密钥候选值中排序位置，以期从根本上提升密钥枚举的效率。本文也将关注基于子密钥候选值位置排序的密钥排序算法研究，并考虑子密钥相关性时如何进行密钥排序和评估密码芯片的安全水平。

1.5 论文结构

本文以下部分内容安排如下：第二章介绍泄漏信号对齐相关内容，第三章介绍多信道融合攻击相关内容，第四章介绍泄漏评估与泄漏检测技术，第五章介绍密钥枚举与密钥排序技术，第六章进行总结和展望。

第二章　泄漏信号对齐

如前所述，本文将泄漏信号对齐技术分成两类：局部泄漏信号对齐技术和全局信号对齐技术。本章节主要介绍作者所提出的两种基于距离的泄漏信号对齐算法：基于*shotgun*距离的局部泄漏信号对齐算法和基于加权编辑距离的全局泄漏信号对齐算法[34]。其中，基于*shotgun*距离的局部泄漏信号对齐算法利用泄漏信号的局部特征进行对齐，而基于加权编辑距离的全局泄漏信号对齐算法则根据泄漏信号的全局结构进行对齐。这两种方法可以消除随机插入伪操作、随机延迟，以及芯片工作时钟频率变化等引发的泄漏信号失调的影响，从而提高侧信道攻击效率。

2.1　预备知识

介绍本章方法之前，首先介绍本章方法涉及的相关知识，包括加权编辑距离、多序列对齐、信号非均匀量化及相关能量分析等四方面内容。

2.1.1　加权编辑距离

编辑距离表示的是一个字符串变换成另一个字符串所需要的最小编辑操作数目[126]，度量了两个字符之间的相似性，广泛应用于各领域，如拼写检查、计算生物学、机器翻译、信息提取及语音识别等等 [127,128]。编辑距离使用的字符串操作有三种，分别是单个字符的插入、删除操作，以及单个字符置换成另一字符的置换操作。两个字符串间的编辑距离通常使用自底而上的动态规划算法求解 [126]。例如，将字符串“WITTEN”变换为另一个字符串“BITTING”只需3个编辑操作，分别是将“W”置换为“B”，将“E”置换成“I”，以及在“WITTEN”最后插入“G”，所以“WITTEN”与“BITTING”的编辑距离是3。

如果考虑到三个编辑操作的重要性不同，分别分配给每个编辑操作一个非负权值，编辑距离就被扩展为加权编辑距离（Weighted Edit Distance，简写为WED） [126]。显然，编辑距离可看作三个编辑操作权重为1的加权编辑距离。加权编辑距离的求解同样使用自底而上的动态规划算法，求解过程如附录 A.1.1 中算法 13 所示。加权编辑距离也度量了两个字符串之间的差异程度，因此稍作变化，只需在计算两个字符串之间的WED 后，利用回溯算法 [126]计算两字符串的加权编辑距离的代价矩阵，即可对齐任意两个字符串。下面以字符串“WITTEN”和“BITTING”为例介绍回溯算法，来展示如何对齐任意两个字符串。

假设以“BITTING”为参考字符串，首先使用算法 13 计算字符串“WITTEN”和“BITTING”的WED代价矩阵，如附录 A.1.2 中表 A.1 所示。从表格中右下角开始沿着左侧或右侧的单元格回溯，每次回溯一个单元格，直至左上角为止。那么，这些单

元格（表中高亮标记）组成了回溯路径。由此回溯路径可得到字符串“WITTEN”和“BITTING”的一个最优对齐的字符串对。附录 A.1.3 中算法 14 给出了对齐字符串S和字符串T的一般过程。

这里得到的对齐字符串对为

```
W I T T E N _
: | | | : |
B I T T I N G
```

上述字符串对中，“:”表示将上面字符替换为下面相应位置的字符，“_”表示插入或删除相应字符，“|”表示上下字符相同，即不做任何编辑操作。

2.1.2 多序列对齐

由两个字符串对齐很容易推广到多个字符串序列对齐 [129]，即对多个字符串序列同时使用动态规划求编辑距离并对齐。显然，这样直接将WED 代价矩阵的计算从2维提升到多维，计算代价极高。一个改进的方案是渐进对齐算法，其分别对多个序列两两求编辑距离，然后取总的编辑距离之和最小的那个序列作为参考序列并对齐 [129]。进一步地，我们可以通过指定参考序列来加速对齐。例如，我们要对齐三个字符串序列“WITTEN”，“BITTING”和“KITTIWAGE”，首先选择“BITTING”作为参考序列，对齐它和另外两个字符串，得到两组对齐后的字符串对，即

```
W I T T E N _      K I T T I W A G E
: | | | : |      : | | | |   : |
B I T T I N G      B I T T I _ N G _
```

然后，向第一个字符串对中的“BITTING”中的相应位置插入符号“_”，以与第二个字符串对中的“BITTING”保持一致。最后调整第一个字符串对中的“WITTEN”中的字符，相应位置添加符号“_”，完成三个字符串的对齐。对齐结果为

```
W I T T E _ N _ _
K I T T I W A G E
B I T T I _ N G _
```

三个以上的字符串序列对齐思想及做法类似，不再赘述。

2.1.3 信号非均匀量化

在实际中，常需要将具有连续取值的信号（即连续时间信号）近似为有限多个离散值的信号（即离散时间信号），或者将具有大量取值的离散时间信号近似为具有较少取值的离散时间信号。上述过程，在数字信号处理领域称为“量化”。在侧信道分析领域，最常见的量化例子是连续泄漏信号的采集。这期间，需要使用示波器以一定的采样率抽取连续泄漏信号的样本点，并根据存储深度再次量化信号，组成新的离散时间

信号。信号的量化方式一般分为均匀量化（或线性量化）和非均匀量化（或非线性量化）两种。

均匀量化是将输入信号的值域按等间隔划分，并给落在每个区域内的信号统一分配一个规定值。均匀量化简单易行，但缺点显著：信号动态范围将受到较大的限制，而且无论信号大小如何，量化间隔都相等，从而使量化噪声功率固定不变，当信号较弱（如侧信道泄漏信号）时，量化后信噪比很小，部分信息会丢失，影响后续信号处理质量。为了克服均匀量化的缺点，实际中往往采用非均匀量化。

非均匀量化根据信号的不同区间来确定不等的量化间隔，量化噪声功率基本上与信号抽样值成比例。对于小信号，量化间隔变小，使量化噪声功率下降，量化信噪比提高；对于大信号，量化间隔增大，使量化噪声功率提高，但因信号功率比较大，故量化后信号信噪比可以保持恒定。因此，量化噪声对大、小信号的影响大致相同，即改善了小信号量化后的信噪比，在增强小信号的同时，保留了小信号的细节。相比均匀量化，非均匀量化更好地反映了信号小尺度内细微变化，能够减少或避免因线性量化造成的小信号信息丢失。非均匀量化常常通过一个非线性函数对信号进行压缩或扩展，然后再进行均匀量化实现。

2.1.4　相关能量分析简介

相关能量分析（Correlation Power Analysis, 简写为CPA） [88]基于分治策略恢复所有子密钥并藉此组合得到主密钥，是一种简单、强大、应用广泛的侧信道攻击方法。使用CPA进行侧信道攻击有一个前提假设，即分析者认为密码芯片在密码算法运行中，与子密钥相关的操作的实际能量泄漏与分析者所假设的能量泄漏值成线性关系。因此，当当子密钥猜测正确时，假设泄漏与实际泄漏的相关系数取得最大值。可以看出，CPA攻击假设简单、流程简洁。图 2.1 以无保护AES-128算法实现为例，介绍了一个标准的CPA攻击流程。

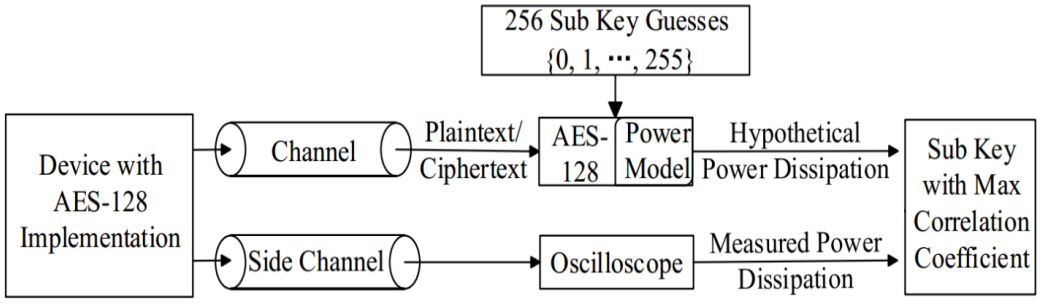


图 2.1　CPA攻击无保护的AES-128实现流程示例

2.2　基于*shotgun*距离的局部泄漏信号对齐算法

该对齐算法受基于匹配思想的静态对齐算法 [10]启发而得。静态对齐算法在密码芯片的侧信道泄漏信号中选定某一个模式，并进行匹配、对齐，其它与模式无关信息

不再考虑。这使得静态对齐算法选择匹配模式时严重依赖攻击者的经验，且可能会损失部分信息 [34]。为了克服这两个缺点，基于*shotgun* 距离的局部泄漏信号对齐算法利用完整的泄漏信号信息，将泄漏信号分段，然后根据一个匹配标准，让每段子信号相互匹配，找到最合适的匹配时停止。因其过程类似文献 [127,130]中的基于基因测序思想的*shotgun* 距离算法，故以此命名。该方法简洁、有效，不需要人工辅助选取特征模板进行匹配，且能够在保留泄漏信号的原始信息的同时，无冗余引入，可以视为对静态对齐方法的扩展。下面详细介绍该对齐方法。

假设有一个密码芯片，采集到的它的侧信道泄漏信号（如能量迹、电磁迹等）在时域上是未对齐的。假设采集了m条长度为n的侧信道泄漏信号，并将泄漏信号集合表示为Q，则有:

$$Q = \bigcup_{i=1}^{m} \{Q_i\} . \tag{2-1}$$

上式中Q_i表示密码芯片的第i条侧信道泄漏信号。

在对齐泄漏信号之前，首先从Q中随机选择一条参考信号S，并使用一个长度为L的矩形窗将其平均分为一串不重叠的子序列。若n/L不是整数，S所均分的最后一段的子序列长度将小于L, 无法进行对齐处理。为了保留原始数据点以避免信息损失，且不引入冗余信息，此时可将S尾部填充0，以保证n/L是整数。同时，为了消除不同泄漏信号在振幅维度上的偏移及尺度差别的影响 [131]，一般需要对这些子序列进行数据标准化处理，如最大最小标准化、零均值标准化等。假设经过数据标准化处理后的子序列组成的集合为S_w，则其可表示为

$$S_w = \bigcup_{j=1}^{n/L} \{S_w(j)\}, \tag{2-2}$$

其中，

$$S_w(j) = Min\_max(S((j-1) \times L + 1 : j \times L)), \tag{2-3}$$

$S((j-1) \times L + 1 : j \times L)$表示$S$中第$(j-1) \times L + 1$个到第$j \times L$个点的集合, Min_max代表最大最小标准化操作。之后，将S_w中的每个子序列分别沿着另外一条待匹配的泄漏信号，按一定步长逐一滑动匹配，直至找到最优匹配信号段并对齐。

为了保证精度，参考信号子序列沿着待匹配泄漏信号的滑动步长设置为1。整个匹配过程所依据的原则是：若某条泄漏信号中的某段信号与参考信号的某个子序列是最优匹配，则相比前者与参考信号的其它子序列而言，二者之间拥有最小的欧氏距离。该距离我们称之为*shotgun*距离（Shotgun Distance，简写为SD）。若使用符号*sDist*表示两个序列之间的SD，则SD可定义如下：

$$sDist = min\{Dist(S_w(j), Q_i'(k)) | k \in Label\}, \tag{2-4}$$

其中，

$$Q_i'(k) = Min\_max(Q_i(k : k + L - 1)), \tag{2-5}$$

$Label = \{1, 2, \ldots, n - L + 1\}$，$Dist$ 表示对两个序列$S_w(j)$及$Q_i'(k)$求欧式距离，而j_{min}则表示$sDist$对应的指标。显然，这里的$Q_i(j_{min} : j_{min} + L - 1)$应该与$S((j-1) \times L + 1 : j \times L)$对齐。为了防止参考序列的两个子序列与同一个子序列匹配，每次计算得到的j_{min}值都会被剔除出j所在的集合。最后，重复上述操作至泄漏信号集合Q中的所有泄漏信号都完成匹配、对齐为止。

该对齐算法可消除随机插入伪操作和随机延迟带来的泄漏信号失调的影响。它需要调节的参数只有子序列的长度L，不必再像静态对齐算法那样要求选取特征明显的匹配模式，使得攻击者不必花费大量时间寻找合适的模式，大大增强了算法的实际可操作性及普适性。相比静态对齐算法，该方法只是将原有泄漏信号分段匹配，在对齐泄漏信号后依然保留了原有泄漏信号信息，避免了与密钥相关的泄漏信息丢失的可能性。算法 1 给出了基于*shotgun*距离的局部泄漏信号对齐算法（Local Alignment Based on Shotgun Distance，简写为LA_SD）的具体步骤。

可以看出，对一条泄漏信号而言，计算*shotgun*距离的计算复杂度为$O(n^2 - nw)$，匹配对齐步骤的计算复杂度是$O(n)$，所以对于m条泄漏信号而言，该对齐算法总的计算复杂度是$O(m(n^2 - nw))$。如果w取值接近于n，则该对齐算法总的计算复杂度趋近于欧式距离的计算复杂度；若w取值极小，则$O(m(n^2 - nw))$趋近于$O(n^2)$，接近于基于动态时间规整的对齐算法 [32]的复杂度。

2.3 基于加权编辑距离的全局泄漏信号对齐算法

上一小节提出的基于*shotgun*距离的局部泄漏信号对齐算法利用的是泄漏信号的局部特征来进行对齐，而本小节将提出一种利用泄漏信号的全局特征进行对齐的算法——基于加权编辑距离的全局泄漏信号对齐算法。该全局对齐算法基本思路是：如果将密码芯片的每条侧信道泄漏信号视为一个离散信号序列，并将其转化为一个相应的符号序列，这样泄漏信号的对齐问题就转化为符号序列的对齐问题。两个符号序列的对齐可以使用加权编辑距离对齐算法，而多个符号序列的对齐可在两两符号序列对齐的基础上使用多序列对齐算法 [129]处理。当泄漏信号集合对应的多个符号序列对齐时，泄漏信号也就完成了对齐。下面详细介绍该全局对齐算法。

首先，需要将密码芯片的侧信道泄漏信号转化为一个符号序列。而将一条泄漏信号转化为一个符号序列需要两个步骤：一是将泄漏信号量化为一个数字信号序列，二是将该数字信号序列转化为符号序列。在第一个步骤中，由于离散信号精度高于数字信号，如果直接选择均匀量化，必然会造成量化误差。不过若对离散时间信号进行非均匀量化处理，适当地选择非线性扩展函数，则可以中和量化误差的负面影响。此外，

Algorithm 1 基于*shotgun*距离的局部泄漏信号对齐算法

输入： 未对齐的密码芯片侧信道泄漏信号集合Q及矩形窗长度L

输出： 对齐后的泄漏信号集合RQ

$RQ \leftarrow Q$
从 Q 中随机选择一条泄漏信号作为参考信号S，并计算集合S_w
for $i = 1, 2, \ldots, m$ **do**
    $j_{min} = [\,], Label = 1, 2, \ldots, n - L + 1$
    for $j = 1, 2, \ldots, n/L$ **do**
        $sDist = +\infty$
        for $k = 1, 2, \ldots, n - L + 1$ **do**
            $Label \leftarrow Label \setminus \{j_{min}\}$
            if $sDist > Dist(S_w(j), Q'_i(k))$ **then**
                $sDist = Dist(S_w(j), Q'_i(k))$
                $j_{min} \leftarrow [j_{min}; k]$
            end if
        end for
        $RQ_i((j-1) \times L + 1 : j \times L) = Q_i(j_{min} : j_{min} + L - 1)$
    end for
end for
返回： 对齐后的泄漏信号集合RQ

根据文献 [33] 的研究，密码算法实现中加解密操作的泄漏信号总是导致泄漏信号的整体幅度变大，同时与秘密信息相关的泄漏信号本身相对于总的泄漏信号相对较小。也就是说，侧信道攻击利用的是泄漏信号的细节特征。所以这里我们对泄漏信号进行非线性量化，将其转化为具有较少取值的离散信号。非线性量化时，我们选择应用成熟的A-律或μ-律 [34]扩展函数来对原始泄漏信号进行扩展，使得在增强泄漏信号的同时，保留与密钥相关的泄漏信号特征，进而提高量化信噪比，从而间接地中和下一步数据均匀量化带来的误差。

与基于*shotgun*距离的局部泄漏信号对齐算法一样，为消除不同泄漏信号在振幅维度上的偏移及尺度差别的影响，需要在进行非线性扩展之前，对原始泄漏信号进行数据标准化处理。假设x表示经过最大最小标准化预处理后的泄漏信号，则经过A-律扩展函数处理过的泄漏信号如下：

$$y = \begin{cases} \dfrac{sgn(x)(1 + lnA)x}{A}, & |x| < \dfrac{1}{(1 + lnA)} \quad (2\text{-}6a) \\ \dfrac{sgn(x)e^{((1+lnA)x-1)}}{A}, & \dfrac{1}{(1 + lnA)} \le |x| \le 1\,. \quad (2\text{-}6b) \end{cases}$$

经过μ-律扩展处理过的泄漏信号如下：

$$y = \frac{sgn(x)((1+\mu)^{|x|}-1)}{\mu}, \qquad |x| \le 1\ . \tag{2-7}$$

式 2-6 及 2-7 中

$$sgn(x) = \begin{cases} 1, & x \ge 0 \quad (2\text{-}8a) \\ -1, & x < 0 \quad (2\text{-}8b) \end{cases}$$

是符号函数，A和μ是扩展系数。之后，将经过A-律或μ-律非线性扩展后的信号的取值范围均匀划分为K个区间，并根据最近邻原则，将落在不同区间内的离散信号值量化为其所在区间的左端点或右端点的值，由此完成将原始泄漏信号转化为数字信号序列的步骤。该过程可描述如下：

$$y_i = \begin{cases} M_0, & \text{if } y_i = min\{y\} \quad (2\text{-}9a) \\ M_i, & \text{if } y_i \ne min\{y\} \text{ and } y_i \in (M_{i-1}, M_i], \quad (2\text{-}9b) \end{cases}$$

其中，$y = \{y_i\}$表示经非线性扩展后的信号序列，M_{i-1}, M_i分别为第i个区间的左端点值和右端点值，且$M_{i-1} < M_i$，$i = 1, 2, \ldots, K$。随后，只需给每个M_i分配一个唯一的符号，即可把得到的数字信号序列转化为符号序列。

在将Q中的每一条泄漏信号都转化为相应的符号序列后，从这些符号序列中随机选定一个符号序列作为参考序列，使用WED算法将参考符号序列和其余符号序列分别两两对齐，并利用渐进对齐算法对得到的两两对齐序列对进行多序列对齐。注意，原始多序列对齐算法使用的参考序列是与其它所有符号序列编辑距离之和最小的符号序列。显然，该算法计算复杂度是$O(C_n^2) = O(n^2)$，而我们的算法则随机选择一个参考序列，其计算复杂度是$O(n)$。当泄漏信号数目足够大时，算法运算量将大大减少。实际中，这样做仅仅可能会多一些编辑操作，不会对原始泄漏信号的信息产生不良影响。

最后，根据每条原始泄漏信号数据与多序列对齐后的符号集合的一一映射关系，得到对齐后的泄漏信号。为了避免如文献 [32]中方法一般在对齐过程中引入冗余，我们需要删除每个对齐后的符号序列中对应于删除及插入编辑操作的符号（记作“_”），并剔除相应的原始泄漏信号数据。这同时有助于减少算法运算量。算法 2 给出了基于加权编辑距离的全局泄漏信号对齐算法（Global Alignment Based on Weighted Edit Distance，简写为GA_WED）的细节。

我们知道，噪声及泄漏信号时域失调是影响侧信道攻击效率的常见的两大因素[32,33]。目前多数研究只是致力于消除其中一方面的影响，提出的技术只关注提升泄漏信号信噪比或对齐泄漏信号某一方面，如文献 [33]所提出的算法能够有效减少噪声对侧信道攻击的影响，而文献 [32]所提出的算法则可降低泄漏信号时域失调的影响。我们提出的全局对齐算法则综合了文献 [33]及 [32]所提出的算法的优势，不仅能通过非线性扩展减少量化误差，而且也弱化了噪声的影响，同时克服了泄漏信号对齐技术中

Algorithm 2 基于加权编辑距离的全局泄漏信号对齐算法

输入： 未对齐的密码芯片侧信道泄漏信号集合Q，A-律或μ-律非线性扩展系数P，非均匀量化阶数K，加权编辑距离算法中删除操作权重w_{del}，插入操作权重w_{ins}及置换操作权重w_{sub}

输出： 对齐后的泄漏信号集合RQ

1: 对未对齐的泄漏信号集合Q进行非线性量化并将之转换为符号序列集合

1.1: 对Q中的每条泄漏信号数据进行最大最小标准化预处理

1.2: 对数据标准化后的泄漏信号使用A-律或μ-律进行非线性信号扩展

1.3: 根据最近邻原则，将非线性扩展后的泄漏信号值均匀分到K个区间

1.4: 给每个区间分配一个唯一的符号，每个区间内的所有信号值分配同一个符号

1.5: 获得原始泄漏信号集合Q的符号化表达SQ

2: 对SQ中的序列使用WED算法进行两两对齐

2.1: 随机从SQ中选择一条符号序列作为参考符号序列

2.2: 使用WED算法，将该参考符号序列与SQ中的其余符号序列两两对齐，得到一个新的两两对齐的符号序列对组成的集合PSQ

3: 对PSQ使用渐进对齐算法，得到一个多序列对齐的符号集合MSQ

4: 根据MSQ对齐原始泄漏信号Q

4.1: 找到Q中每条泄漏信号中数据与MSQ中每条符号序列中符号的一一映射关系

4.2: 找到对应于非“_”的符号索引值集合，并根据得到的泄漏信号数据与符号映射关系，选择对应于该符号的原始泄漏信号数据

4.3: 将Q中每条原始泄漏信号中被选择的数据与参考符号序列所对应的原始泄漏信号中被选择的数据一一对齐

5: **返回：** 对齐后的泄漏信号集合RQ

常见的信息丢失及冗余引入的问题。

可以看出，对一条泄漏信号而言，加权编辑距离算法的计算复杂度为$O(n^2)$，多序列对齐算法及匹配对齐步骤的计算复杂度均为$O(n)$；所以对于m条泄漏信号而言，该对齐算法总的计算复杂度是$O(mn^2)$。

2.4 算法性能评估

这里我们以典型的AES-128加密算法的常见实现方案（包括智能卡实现、8-bit单片机实现及FPGA实现方案）为例，针对由常见原因（不精确的触发信号、随机插入伪操作及变化芯片工作时钟频率）引起的密码芯片侧信道泄漏信号时域失调现象，通过采集不同实现方案运行过程中的能量泄漏信号，并在泄漏信号对齐后使用相关能量分析计算一阶成功率 [13,132]，来检验、分析本章节所提出算法的有效性。

2.4.1 实验设置及参数

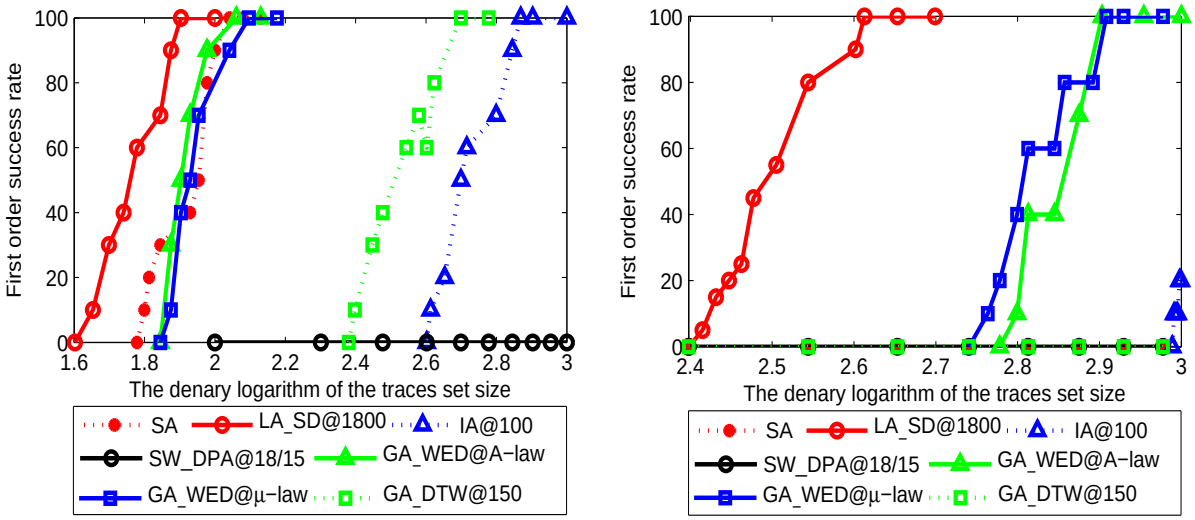
本章节的实验以典型的AES-128加密算法为例，将其分别在三种常见芯片类型上实现，并分别采集了一组能量泄漏信号。这三种芯片类型分别包括一张商业智能卡（ATmega163），一个8位8051架构的单片机（Microcontroller Unit，简写为MCU）及一个FPGA (Xilinx Kintex-7)。其中，AES-128加密算法的智能卡及8-bit MCU实现方案运行过程中的能量泄漏可近似认为是汉明重量泄漏（Hamming Weight，简写为HW），AES-128的FPGA实现方案可近似认为是汉明距离泄漏（Hamming Distance，简写为HD）。针对前两种AES-128实现，我们分别采集它们在输入1000条、2000条随机明文时所对应的能量泄漏信号，且选择这两种实现的第一轮S盒输出作为攻击目标。针对AES-128的FPGA实现，我们采集其在输入90,000条随机明文时所对应的能量泄漏信号，并选择该实现的最后一轮S盒输入及输出的异或作为攻击目标。在AES-128的这三种不同的实现方案中，由于智能卡中的AES-128实现触发信号与时钟信号不能精确同步、8-bit MCU中的实现使用了随机插入伪操作的防护措施，以及AES-128的FPGA实现使用了三种不同的工作时钟（分别是2.5MHz，5MHz和20MHz），采集得到的三组能量泄漏信号在时域上都是未对齐的。

为了比较本章节所提出的两种对齐方法的性能，这里同时对比了一些经典的、有代表性的对齐方法，包括静态对齐（Static Align，简写为SA） [10]、滑窗DPA 对齐（Slide Window DPA，简写为SW_DPA） [53]、整合攻击（Integrated Attack，简写为IA） [36]，以及基于DTW的全局对齐算法（Global Alignment Based on DTW，简写为GA_DTW） [32]。由于SA算法并不适合用于消除随机插入伪操作及变化时钟引起的能量泄漏信号失调 [10]，故这里SA只用于消除智能卡触发信号不精确引发的能量泄漏信号失调。而其它对比方法都将用于降低或消除智能卡触发信号不精确及8-bit MCU随机插入伪操作引发的能量泄漏信号失调的实验中。此外，只有GA_DTW和GA_WED算法能消除变化FPGA工作时钟频率所造成的能量泄漏信号失调的影响。

不失一般性，在以上方法中，我们都选择三组能量泄漏信号集合中的第一条信号作为参考信号。三个实验的结果如图 2.2(a)，2.3(a) 和 2.4(a) 所示。图中也给出了实验中各个算法所选取的参数信息。例如，LA_SD@230表示LA_SD算法的窗长是230，IA@8表示IA对齐算法的窗长是8，SW_DPA@18/15则表示SW_DPA算法所选时钟周期长度参数是18，并且将15个样本点数目累加为1个点。此外，三个实验中GA_DTW算法的半径总是设置为150，GA_WED算法的量化阶数选择10，A-律或μ-律非线性扩展系数总选为10或25，而且删除、插入及替换三个编辑操作的权重系数总设为5，1，1。

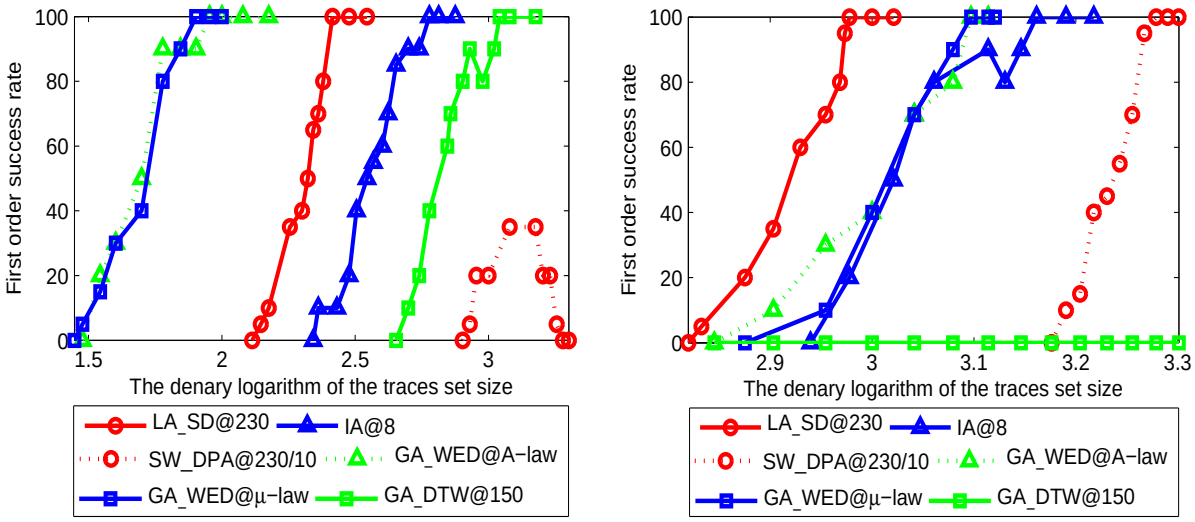
最后，为了考察不同噪声水平下本章节所提出算法的稳健性，我们在原有能量泄漏信号中添加了不同大小的噪声之后*，使用各个对齐算法处理并进行CPA攻击、计算

* 即将原始信号视为“纯净”信号，在原始泄漏信号的基础上，按一定“信噪比”添加噪声。



(a) SNR=+∞ (b) SNR=32dB

图 2.2 各对齐算法消除智能卡触发信号不精确影响后CPA攻击效果对比



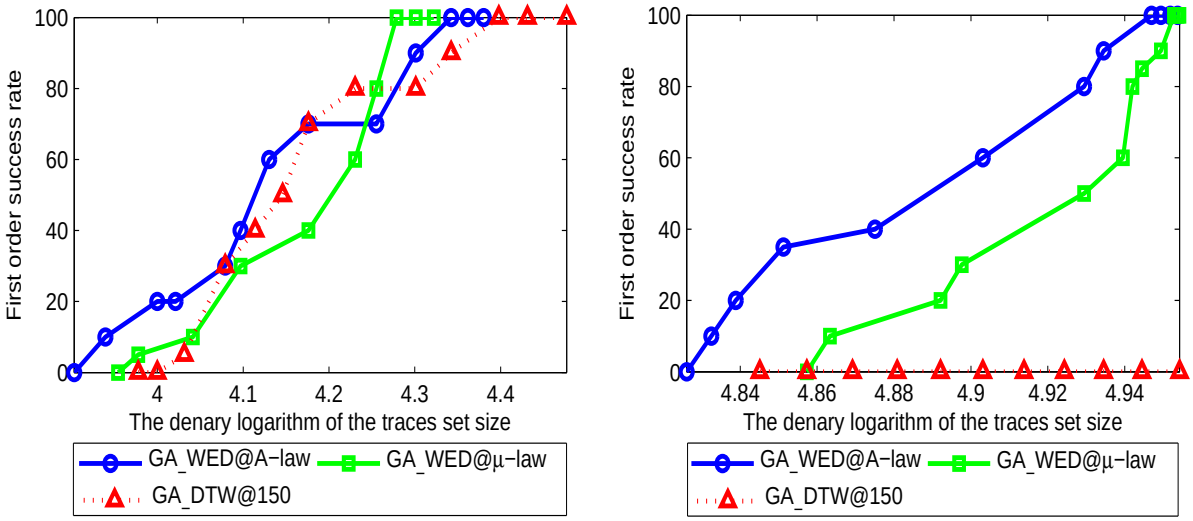
(a) SNR=+∞ (b) SNR=32dB

图 2.3 各对齐算法消除RPIs影响后CPA攻击效果对比

成功率，实验结果如图 2.2(b), 2.3(b) 和 2.4(b) 所示。

2.4.2 实验结果及分析

图 2.2, 2.3 和 2.4 显示了各个对齐算法消除常见原因引发的能量泄漏信号失调影响后的CPA攻击结果。其中，从图 2.2(a) 可以看出，SA算法在信噪比很大的情况下，因为能在泄漏信号中轻易选出S盒输出所对应的泄漏部分作为模式匹配，所以其结果在所有的对齐算法中几乎是最理想的。而本章所提出的LA_SD算法作为SA算法的扩展，完全保留了SA算法的优点，甚至对齐后的攻击效果比后者还要好。这也间接说明，相对于原始泄漏信号，经SA算法对齐后的泄漏信号还是损失了少部分信息。另外，本章所提出的GA_WED与SA算法相比，效果亦难分伯仲。相比之下，SW_DPA 算法完全失效，



(a) SNR=+∞　　(b) SNR=32dB

图 2.4　各对齐算法消除工作时钟变化影响后CPA攻击效果对比

GA_DTW 算法对齐泄漏信号后攻击成功率达到100%需要500条能量迹之多，而IA算法甚至在700条能量迹时依然无法使得攻击成功率达到100%。

在噪声强度较大的场景下，可以从图 2.2(b) 看出，本章所提出的LA_SD算法表现优异，性能依然稳健。同样地，本章所提出的GA_WED算法性能表现同样稳健。而SA算法则由于噪声干扰，无法根据泄漏信号模式特征有效提取S盒输出所对应的泄漏信号段，从而导致算法失效。此外，IA算法在使用接近1000条能量迹的情况下，对齐后攻击只达到了20%的成功率，SW_DPA及GA_DTW算法则完全失效。

本章所提出的两种对齐算法在消除8-bit MCU随机插入伪操作引起的能量泄漏信号时域错位影响时，表现如图 2.3(a) 中场景类似，依然较其它对比方法优异，只是GA_WED算法表现略优于LA_SD算法（见图 2.3(a)）。IA算法表现较图 2.3(a) 场景中较好，优于GA_DTW算法。值得注意的是，SW_DPA算法的表现并不稳定，甚至在1900多条能量迹时性能反而下降。这是因为SW_DPA算法攻击第十二个子密钥时引入了无用信息，导致攻击所得子密钥猜测总是落在错误的候选值上，进而影响了总体攻击成功率。而在噪声增大的场景下，噪声反而抵消掉了无用信息的负面影响，使得SW_DPA算法的表现反而比噪声较小时更好（见图 2.3(b)）。这种现象似乎说明噪声并不一定总是在侧信道攻击中起削弱攻击效率的副作用，可留待以后深入研究。而从图 2.3(b) 中可以看出，本章所提出的两种对齐方法在高噪声环境下性能仍旧稳健——此时LA_SD算法表现略优于GA_WED算法，但都显著优于对比算法。同图 2.2(b)中一样，GA_DTW算法抗噪声性相对较弱，其将能量迹对齐后攻击成功率为0。

类似的情形也发生在各个对齐算法消除FPGA变化工作时钟引发的能量泄漏信号失调影响的实验中。在噪声较小时，如图 2.4(a) 及 2.4(b) 所示，GA_DTW算法虽然表现不如GA_WED算法，但其效果较其在噪声较大情形下完全失效可观得多。相较之下，

本章提出的GA_WED算法无论在噪声较小还是在噪声较大情形下，总是能取得不错的攻击结果。而且，在图 2.2， 2.3 和 2.4 三种情形下，GA_DTW算法（其中DTW算法使用了快速DTW算法优化 [133]）在相同软硬件配置下运行速度始终不及GA_WED 算法，且前者所占内存显著大于后者。

总体看，以上各个对齐方法在三个不同场景下的差异表现的原因可分析如下：SA算法因为需要分析者观察并选择特征显著的匹配模式，所以不但对噪声极度敏感，而且可能会丢失部分与密钥相关的泄漏信息。而SW_DPA和IA算法因为使泄漏信号值累加而产生无用的累加噪声，掩盖了部分与密钥相关的泄漏信息，并不能使得原始能量泄漏信号经处理后完全对齐，相较完全对齐的泄漏信号，CPA求得的相关系数也会 [10]以一定比例系数下降，效率大打折扣。GA_DTW算法的核心是DTW算法，而DTW算法本质上是按尖峰点对尖峰点、波谷点对波谷点的对齐算法 [130]，而且仅有一个插入操作，导致有些样本点对齐过程中需求平均，继而会抹除一些原始泄漏信号的信息，并引入新的冗余信息，同时可能会使得重要的泄漏信息分散到不同的时刻。所以，GA_DTW算法有时甚至比不上对齐效率较低的IA算法。本章所提的LA_SD算法则充分利用了原始泄漏信号的完整信息，既不会损失信息，又因分段对齐时利用相应信号段的整体信息抑制了噪声带来的负面影响，使得该算法性能高效且在高噪声环境下表现稳健。而GA_WED算法包含三个编辑操作：删除、插入及替换操作，在保存必要的与秘密信息相关的泄漏信息的同时，也防止了对齐后冗余信息的引入，因而表现较GA_DTW算法良好。此外，因在对齐前对原始泄漏信号进行了非线性扩展增强了信号，削弱了噪声，提高了信噪比，故而GA_WED算法的抗噪声性能远优于GA_DTW算法。三个实验中，GA_WED算法使用A- 律或μ-律进行非线性扩展的效果类似。

简而言之，本章提出的两种对齐方法既保留了原始泄漏信号完整信息，又避免了冗余信息的引入，同时减弱了降低侧信道攻击效率的另一常见因素——噪声的影响。所以，这两种方法不仅对齐效率及优于对比方法，而且更较对比方法抗噪声干扰。

此外，本章节提出的两种泄漏信号对齐算法参数设置相当简捷。例如，LA_SD算法选择窗长时，只需要保证泄漏信号分段后有一个信号子序列包含敏感中间值的侧信息泄漏即可。对GA_WED算法而言，为了保存必要的与密钥相关的泄漏信息并防止冗余引入，删除操作的权重应比另外两个操作的权重大，而且这三个权重的选择与设备无关。另外一个参数——量化阶数的设置则只和密码芯片的泄漏模型有关。例如，上述试验中的密码芯片泄漏模型不是HW模型就是HD模型，共有9种可能的泄漏值，为了保证不损失泄漏信息，同时在一定程度上消除量化噪声及环境噪声的影响，只需将K设置得比9稍大即可，如本章节实验中设置其为10。

2.5 本章小结

综上所述，无论在智能卡（相当于加入了随机延迟的AES-128实现方案）、8-bit单

片机（加入了随机插入伪操作的AES-128实现方案），还是在FPGA（使用了变化时钟频率的AES-128实现方案）上，本章节提出的两种泄漏信号对齐算法都显著优于已有经典算法，甚至在高噪声环境下，依然保持良好性能。相对于使用未对齐的泄漏信号直接攻击，使用上述两种算法更是极大提高了密码芯片的侧信道分析效率。以上实验只是以密码芯片的能量泄漏信号为例，除此之外，本文算法同样也适用于别的泄漏类型，如电磁泄漏等。

另外，即使在采用了组合防御对策的情况下，本章节提出的两种方法性能依然稳定。如图 2.5 所示，尽管该AES-128掩码实现方案（Rotating S-boxes Masking Scheme，简写为RSM） [134]同时采用了随机插入伪操作来防御侧信道攻击，但本文方法依然有效。

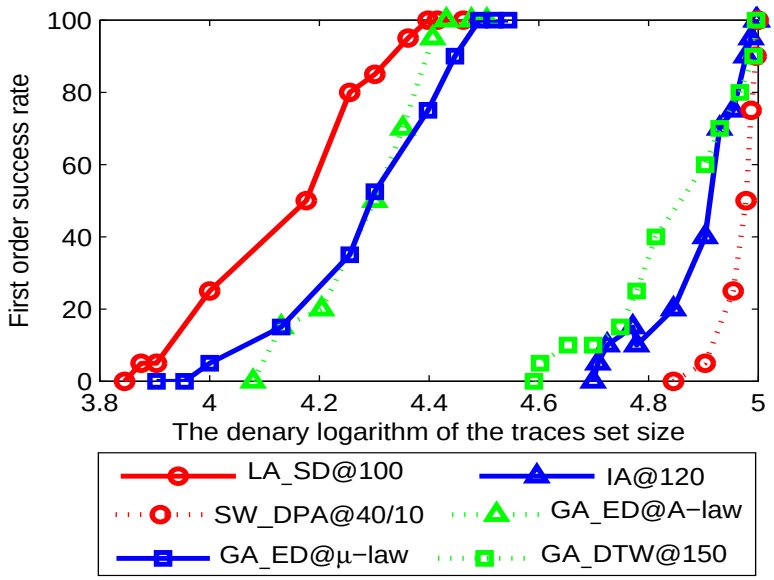


图 2.5　联合了RPIs的AES-128 RSM掩码实现的泄漏信号对齐后CPA攻击效果对比

本章节从信息利用方式的角度分类对齐技术，较系统地研究了泄漏信号对齐技术，提出了两种基于距离的密码芯片侧信道泄漏信号对齐算法，并在多种常见密码芯片类型上进行了较为全面地实验及分析。这两种方法能够在保持原有与密钥相关泄漏的同时，避免引入冗余信息，具有很高的信息利用率及对齐效率，并且抗噪声性能良好，参数调节简洁高效，对泄漏信号性质没有限制。通过本章的实验及分析可以看出，侧信道泄漏信号对齐技术是否高效的关键在于其能否保留依赖于密钥的泄漏信息，且避免引入与分析无关的冗余信息。该思路可以为以后研究高效的泄漏信号对齐技术提供借鉴。下一步，我们希望对采用了组合防御对策的密码芯片展开进一步分析，以期加强对目前学术界关注较少的面向组合防御对策的预处理技术的研究。

第三章　多信道融合攻击

如第 1.2.2 小节所述，本文建立了多信道融合攻击研究框架，将多信道融合攻击分为三类 [16]。鉴于目前多信道融合攻击研究中存在的问题，本章首先提出三种多信道融合攻击方法。这三种方法涵盖了多信道融合攻击的三种不同类型。其中，数据级融合攻击方案由多信道DPA [15]改进而来，并克服了后者的弱点。特征级融合攻击方法则是基于奇异值分解的融合攻击方法，属于非建模类攻击，在实际中可操作性强。而本章所提出的决策级融合攻击方法则充分利用了所有单信道攻击结果，可被视为Max_FA及Sum_FA [78]两个算法的推广。

进一步地，目前多信道融合攻击方法采取的融合方式或者是分别单独处理每个信道的侧信息泄漏信号，或者是单独提取每个信道的泄漏特征，又或者是单独进行单信道攻击，之后再联合得到的泄漏信号或特征或单信道攻击结果，获取最终融合攻击结果。但没有一种方法是利用所有侧信道泄漏信号联合信息或者所有侧信道泄漏信号的联合特征，又或者所有单信道攻击结果的联合信息，来进行分析的。为了研究不同融合方式对多信道融合攻击算法效率的影响，我们提出了另外三个均采用了第二类融合方式的融合攻击方案。这三种方法也分别涵盖了多信道融合攻击的三种不同类型。其中，数据级和决策级融合攻击方案皆基于非负矩阵分解，特征级融合攻击方案则以广义奇异值分解为基础。

本章还提出了基于偏相关分析的多信道泄漏融合判别标准 [16]，以用来判断两个侧信道的泄漏是否适于融合。与文献 [15]和 [78]中提出的类似判别标准相比，计算本文所提判别标准时，不必知道密码算法所用的密钥。

3.1　预备知识

下面首先介绍本章方法所涉及的相关知识，包括相关分析、基于贝叶斯推断的多信道融合攻击技术、奇异值分解、广义奇异值分解及非负矩阵分解。

3.1.1　相关分析

假设我们对实现在一个密码芯片上的某密码算法进行了一次加密或解密运算，并在其间获取到该密码算法实现中的某一个操作的单信道泄漏信号（如能量泄漏、电磁辐射等）。该操作对应的敏感中间值设为$Z(x,k)$，对应的泄漏设为$l(x,k)$。其中，x是一条已知明文或密文的一部分，k是该密码算法所使用密钥的相应部分（也即子密钥）。令f表示该侧信道的泄漏函数，α和β分别表示依赖于该侧信道的参数。若式子

$$l(x,k) = \alpha f(Z(x,k)) + \beta + \eta \tag{3-1}$$

成立，那么我们认为$l(x,k)$与$f(Z(x,k))$之间存在线性关系，并且该密码实现的侧信道泄漏属于线性泄漏 [135]。如果上式不成立，则认为$l(x,k)$与$f(Z(x,k))$之间不存在线性关系，并且该侧信道泄漏属于非线性泄漏。注意，式子 3-1 中的η表示与泄漏函数$f(Z(x,k))$无关的信道噪声，通常被视为零均值噪声。

如果对该密码算法随机输入明文或密文，使用同一密钥进行多次加密或解密操作，那么相应的单信道泄漏信号也会有多个，此时式子 3-1 可变化为

$$l(\boldsymbol{x},k) = \alpha f(Z(\boldsymbol{x},k)) + \beta + \boldsymbol{\eta}\ . \tag{3-2}$$

上式中，$\boldsymbol{x} = [x_1, x_2, \ldots, x_n]^T$，$Z(\boldsymbol{x},k) = [Z(x_1,k),\ Z(x_2,k), \ldots, Z(x_n,k)]^T$，$\boldsymbol{\eta} = [\eta_1, \eta_2, \ldots, \eta_n]^T$。注意斜体加粗的符号$\boldsymbol{bold}$表示一个列向量，斜体加粗的符号$\boldsymbol{bold'}$则表示一个行向量。

在确定密码芯片侧信道泄漏是线性泄漏的基础上，我们可以使用相关分析技术来进行侧信道分析。相关分析技术是一种经典的强大的侧信道分析方法，常见的诸如相关能量分析（CPA [88]）或相关电磁分析（Correlation Electromagnetic Analysis，简写为CEMA [3,136–138]）等等。相关分析将主密钥分成若干个子密钥，使子密钥的取值集合K远小于主密钥的取值集合，然后通过分治策略逐一恢复出所有子密钥，进而恢复主密钥。该类方法假设如果分析者猜测的子密钥正确，那么实际采集到的密码算法敏感中间值的侧信道泄漏与分析者根据泄漏函数得到的假设泄漏应高度线性相关。但若分析者猜测的子密钥错误，那么敏感中间值的真实泄漏与假设泄漏线性关系不存在，也即二者线性相关度极低。所以，分析者常常将经相关计算得到的具有最大相关系数值的子密钥猜测作为正确子密钥的猜测。定义k_{guess}为子密钥k的密钥猜测，那么有

$$k_{guess} = \underset{k_{can} \in K}{\operatorname{argmax}}\ |\rho(l(\boldsymbol{x},k), f(Z(\boldsymbol{x},k_{can})))|\ . \tag{3-3}$$

上式中k_{can}表示子密钥可能的候选值，$\rho(X,Y)$表示随机变量X和Y的相关系数。因为常见的侧信道泄漏属于线性泄漏或者可以使用线性泄漏近似，所以本章关于多信道融合攻击算法的研究都是建立在相关分析技术的基础上。

3.1.2 基于贝叶斯推断的多信道融合攻击

贝叶斯推断是一种以贝叶斯规则为基础的重要数据融合工具 [139–141]。贝叶斯推断同样可应用于多信道泄漏融合分析中。基于贝叶斯推断的多信道融合攻击方案最早提出于2003 年 [15]。不过文中方法基于建模类攻击，实际应用要求较高。其后基于贝叶斯推断的融合攻击方法被文献 [64]用于单信道泄漏多特征点组合攻击。该方法使用相关系数近似已知泄漏下子密钥的后验概率，实际可操作性更好。虽然文中只涉及组合攻击，但该方法同样也适用于多信道融合攻击。文献 [78]则利用贝叶斯推断来联合多个区分器或多个侧信道攻击结果，以期取得比单个区分器或单信道攻击更好的结果。

然而，这些研究没有被归结、统一到贝叶斯推断的融合框架下。下面我们在此框架下简要介绍基于贝叶斯推断的多信道融合攻击技术 [15]。

假设在一个密码算法实现运行中，分别从M个侧信道采集到M组不同的侧信息泄漏信号集合，并分别使用$\boldsymbol{l_1}, \boldsymbol{l_2}, \ldots, \boldsymbol{l_M}$表示这些泄漏信号集合。若令$L_M = \{\boldsymbol{l_1}, \boldsymbol{l_2}, \ldots, \boldsymbol{l_M}\}$，且将单个子密钥可能的候选值集合表示为$K = \{k_1, k_2, \ldots, k_N\}$，并使用符号$P(\cdot)$表示随机变量的概率分布函数，那么以下条件独立性

$$P(L_M|k_i) = P(\boldsymbol{l_1}, \boldsymbol{l_2}, \ldots, \boldsymbol{l_M}|k_i) = \prod_{j=1}^{M} P(\boldsymbol{l_j}|k_i) \tag{3-4}$$

满足时，子密钥第i个候选值在已知M个侧信道泄漏L_M条件下的后验概率可表示为

$$P(k_i|L_M) = \frac{P(\boldsymbol{l_1}, \boldsymbol{l_2}, \ldots, \boldsymbol{l_M}|k_i)P(k_i)}{P(\boldsymbol{l_1}, \boldsymbol{l_2}, \ldots, \boldsymbol{l_M})} = \frac{P(k_i)}{P(L_M)} \prod_{j=1}^{M} P(\boldsymbol{l_j}|k_i) \, . \tag{3-5}$$

又由贝叶斯公式

$$P(\boldsymbol{l_j}|k_i)P(k_i) = P(k_i|\boldsymbol{l_j})P(\boldsymbol{l_j}), \tag{3-6}$$

则公式 3-4 可变化为

$$\begin{aligned} P(k_i|L_M) &= \frac{P(k_i)}{P(L_M)} \prod_{j=1}^{M} \left[\frac{P(\boldsymbol{l_j})P(k_i|\boldsymbol{l_j})}{P(k_i)} \right] \\ &= \frac{\prod_{j=1}^{M} P(\boldsymbol{l_j})}{P(L_M)\left[P(k_i)\right]^{M-1}} \prod_{j=1}^{M} P(k_i|\boldsymbol{l_j}) \, . \end{aligned} \tag{3-7}$$

因为$P(L)$, $P(\boldsymbol{l_j})$与子密钥猜测值分布无关，且子密钥猜测值分布一般认为是均匀分布，所以最后的子密钥猜测为

$$k_{guess} = \underset{k_i \in K}{\operatorname{argmax}} \prod_{j=1}^{M} P(k_i|\boldsymbol{l_j}) \, . \tag{3-8}$$

简单来讲，基于贝叶斯推断的多信道融合攻击技术是联合了各个单信道攻击所得的子密钥的后验概率$P(k_i|\boldsymbol{l_j})$，进而得到优于单信道攻击的结果。在子密钥猜测值等概率分布，各侧信道泄漏信号分布相互独立的情况下，基于贝叶斯推断的多信道融合攻击的结果总会优于任意一个单信道的攻击结果。

当有新的单信道泄漏信息加入时，贝叶斯融合也可写成另一种“更新形式”，即

$$P(k_i|L_{M+1}) = CP(k_i|L_M)P(k_i|\boldsymbol{l_{M+1}}), \tag{3-9}$$

其中

$$C = \frac{P(\boldsymbol{l_{M+1}})}{P(k_i)P(\boldsymbol{l_{M+1}}|L_M)} \, .$$

这种表达形式有助于从可联合的侧信道不断增加的角度上理解基于贝叶斯推断的多信道融合攻击技术。式 3-9 的推导过程详见附录 A.2.1。

3.1.3 奇异值分解

奇异值分解（Singular value decomposition, 简写为SVD）是线性代数中一种重要的矩阵分解算法 [140]，在信号处理及统计等领域有重要应用。若给定一个矩阵L，其大小为$m \times n$，那么矩阵L存在一个分解，形式如下：

$$L = U \begin{bmatrix} \sigma_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \sigma_2 & & 0 & 0 & \dots & 0 \\ \vdots & & \ddots & & \vdots & & \vdots \\ 0 & \dots & & \sigma_r & 0 & \dots & 0 \\ 0 & \dots & \dots & 0 & 0 & \dots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \dots & \dots & 0 & 0 & \dots & 0 \end{bmatrix} V^H = U\Sigma V^H = \sum_{i=1}^{r} \sigma_i \boldsymbol{u_i} \boldsymbol{v_i^H} . \tag{3-10}$$

式 3-10称为矩阵L的奇异值分解。式 3-10中，$U = [\boldsymbol{u_1}, \boldsymbol{u_2}, \dots, \boldsymbol{u_m}]$表示一个$m \times m$的酉矩阵，$\Sigma$表示一个$m \times n$的对角矩阵，$r$表示矩阵$L$ 的秩，$V = [\boldsymbol{v_1}, \boldsymbol{v_2}, \dots, \boldsymbol{v_n}]$表示一个大小为$n \times n$的酉矩阵，$V^H$则表示$V$的复共轭矩阵，$\sigma_i$代表$L$第$i$个奇异值，而且满足

$$\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r > 0 . \tag{3-11}$$

另外，式 3-10中的向量$\boldsymbol{u_i}$表示L第i个左奇异向量，$\boldsymbol{v_i}$表示L第i个右奇异向量。一个矩阵的奇异值分解是唯一的。

假设一个密码算法实现的某个单通道泄漏信号集合为L，且L中包含了m条泄漏信号，每条泄漏信号有n个样本点。若L每个行向量代表一条泄漏信号，每个列向量代表密码算法运行中同一个中间值在同一时刻的泄漏样本点，那么从信号时频分析的角度出发，L的左奇异值向量包含了L的频域信息，也即L中所有泄漏信号在同一时刻的变化情况；奇异值包含了L的能量信息，也即泄漏信号的大小；右奇异值向量包含了L的时域信息，也即L中的单条泄漏信号在不同时刻的变化情况 [142–144]。因为绝大多数侧信道攻击使用统计手段揭示秘密信息时，所利用的正是所有泄漏信号中敏感中间值在同一时刻的变化信息，所以L的左奇异向量可以看作L的主要泄漏特征，可以用来刻画L。基于这一点，我们可以在奇异值分解的基础上构造多信道融合攻击方案。注意这里并不考虑奇异值的作用，因为它们仅仅包含了泄漏信号的能量信息，在左奇异值向量存在的情况下并不起作用。

3.1.4 广义奇异值分解

广义奇异值分解（Generalized Singular Salue Decomposition，简写为GSVD）是奇

异值分解的推广算法。若给定两个矩阵$L_1 \in \mathbb{C}^{m\times p}, L_2 \in \mathbb{C}^{n\times p}$，将它们串联起来，即

$$L = \begin{bmatrix} L_1 \\ L_2 \end{bmatrix} = \begin{bmatrix} L_1^T & L_2^T \end{bmatrix}^T , \tag{3-12}$$

那么存在两个酉矩阵$U \in \mathbb{C}^{m\times m}$和$V \in \mathbb{C}^{n\times n}$，一个大小为$p \times min(p, m+n)$的矩阵$Q$，及两个非负对角矩阵$S_1 \in \mathbb{C}^{m\times min(p,m+n)}$和$S_2 \in \mathbb{C}^{n\times min(p,m+n)}$，使得下面式子

$$L_1 = US_1Q^H, \quad L_2 = VS_2Q^H, \quad S_1^H S_1 + S_2^H S_2 = I \tag{3-13}$$

成立。上式被称作串联矩阵$(L_1^T, L_2^T)^T$的广义奇异值分解 [146]。可以看出，广义奇异值分解要求串接的两个矩阵L_1及L_2必须要有相同的列数。进一步地，如果矩阵L_2是一个单位阵，那么$(L_1^T, L_2^T)^T$的广义奇异值分解将会退化为矩阵L_1的奇异值分解。类似第 3.1.3 小节关于奇异值分解的分析，如果采集到一个密码算法实现的某两个不同的单通道泄漏信号集合为L_1和L_2，且两个集合中都包含了m条泄漏信号，每条泄漏信号有n个样本点，那么公式 3-13 中的U和V可被视为这两个侧信道侧信息泄漏的联合特征集合，并可据此实施多信道融合攻击。

3.1.5　非负矩阵分解

给定一个矩阵$L \in \mathbb{R}^{m\times n}$，若其组成元素都大于或等于0，则该矩阵称为非负矩阵，而且该矩阵存在以下分解形式：

$$L \approx WH . \tag{3-14}$$

该分解形式称为矩阵L的非负矩阵分解或非负矩阵近似（Non-negative Matrix Factorization or Non-negative Matrix Approximation，简写为NMF）。上式右边的两个矩阵$W \in \mathbb{R}^{m\times d}$及$H \in \mathbb{R}^{d\times n}$都是非负矩阵。参数$d$需在矩阵分解前预置，而且要满足$(m+n)d < mn$。根据式 3-14，矩阵$L$的第$i$个列向量（设为$\boldsymbol{L_i}$，$i = 1, 2 \ldots, n$）可以表示为

$$\boldsymbol{L_i} \approx W\boldsymbol{h_i} . \tag{3-15}$$

其中$\boldsymbol{h_i}$代表矩阵H第i个列向量。$\boldsymbol{L_i}$可以看成矩阵W所有列向量的加权和，且W的每个列向量的加权系数组成了$\boldsymbol{h_i}$。因此，W常被称作特征矩阵，H常被称为系数矩阵 [147]。

与奇异值分解具有唯一解不同，非负矩阵分解常常没有一个精确解。它的解常通过使用最优化方法来数值近似得到 [148]。若使用符号L表示一个密码芯片的多个侧信道的泄漏信号组成的集合，那么L中的元素在现实世界具有明确的物理含义，比如密码芯片的电压降或电磁辐射等等。显然，L的元素都是非负的。此时，特征矩阵W可以视为多个侧信道泄漏融合后的泄漏集合，求解出W即可进行多信道融合攻击。如此一来，我们通过非负矩阵分解得到的W的元素同样保持非负性，也同样具有类似L中元素（电

压降或电磁辐射等）的明确的物理含义，从而使融合攻击所用的融合数据具备了现实解释。

3.2 多信道融合攻击算法

本章节共提出六种多信道融合攻击算法，分别包括两个数据级融合攻击算法（简单融合攻击算法、基于非负矩阵分解的数据融合攻击算法）、两个特征级融合攻击算法（基于奇异值分解的融合攻击算法、基于广义奇异值分解的融合攻击算法）及两个决策级融合攻击算法（基于加权贝叶斯推断的融合攻击算法、基于非负矩阵分解的决策融合攻击算法）。这六种算法包含了两种不同融合方式，即简单融合攻击算法、基于奇异值分解的融合攻击算法及基于加权贝叶斯推断的融合攻击算法首先分别对每个单信道单独处理泄漏信号、提取特征或进行攻击，然后联合这些处理过的信号、特征或攻击结果再做最终攻击；而基于非负矩阵分解的数据融合攻击算法、基于广义奇异值分解的融合攻击算法及基于非负矩阵分解的决策融合攻击算法则分别提取所有侧信道的泄漏信号、所有侧信道泄漏信号的联合特征或所有侧信道攻击结果的联合信息，再进行攻击。下面分别来介绍这些算法。

不失一般性，这里我们以两种典型的侧信道泄漏（即密码芯片的能量泄漏及电磁辐射泄漏）的融合攻击为例，分别讨论以上六种融合攻击算法。假设一个密码芯片运行密码算法时，我们同时测量得到该芯片的一个能量泄漏信号集合L_{Pow}及一个电磁泄漏信号集合L_{EM}。注意，一般情况下，因为电磁泄漏信号变化频率远高于能量泄漏信号，所以电磁信道与能量信道中依赖于密钥的泄漏* 特征点在时域上未必是同一时刻发生的。为了方便表达，假设L_{Pow}及L_{EM}中每条行向量都分别代表一条泄漏信号，且都包含m条泄漏信号，每条信号包含n个采样点，那么有

$$\begin{aligned} L_{Pow} &= [(\boldsymbol{l}'_{\boldsymbol{p_1}})^T, (\boldsymbol{l}'_{\boldsymbol{p_2}})^T, \ldots, (\boldsymbol{l}'_{\boldsymbol{p_m}})^T]^T \\ &= [\boldsymbol{l}_{\boldsymbol{p_1}}, \boldsymbol{l}_{\boldsymbol{p_2}}, \ldots, \boldsymbol{l}_{\boldsymbol{p_n}}] \end{aligned} \tag{3-16}$$

和

$$\begin{aligned} L_{EM} &= [(\boldsymbol{l}'_{\boldsymbol{e_1}})^T, (\boldsymbol{l}'_{\boldsymbol{e_2}})^T, \ldots, (\boldsymbol{l}'_{\boldsymbol{e_m}})^T]^T \\ &= [\boldsymbol{l}_{\boldsymbol{e_1}}, \boldsymbol{l}_{\boldsymbol{e_2}}, \ldots, \boldsymbol{l}_{\boldsymbol{e_n}}], \end{aligned} \tag{3-17}$$

其中

$$\boldsymbol{l}'_{\boldsymbol{p_i}} = [l'_{p_{i,1}}, l'_{p_{i,2}}, \ldots, l'_{p_{i,n}}] \tag{3-18}$$

与

$$\boldsymbol{l}'_{\boldsymbol{e_i}} = [l'_{e_{i,1}}, l'_{e_{i,2}}, \ldots, l'_{e_{i,n}}] \tag{3-19}$$

* 除非特别声明，在本章“依赖于密钥的泄漏”表示一个和密钥相关的敏感中间值的侧信息泄漏。

分别是L_{Pow}和L_{EM}的第i个行向量，也即第i个泄漏信号，并且

$$\boldsymbol{l}_{\boldsymbol{p}_j} = [l_{p_{j,1}}, l_{p_{j,2}}, \ldots, l_{p_{j,m}}]^T \tag{3-20}$$

及

$$\boldsymbol{l}_{\boldsymbol{e}_j} = [l_{e_{j,1}}, l_{e_{j,2}}, \ldots, l_{e_{j,m}}]^T \tag{3-21}$$

分别表示L_{Pow}和L_{EM}的第j个列向量，$i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$。

3.2.1　简单融合攻击算法

简单融合攻击算法（Simple Fusion Attack, 简写为SFA）是多信道DPA攻击算法[15]的改进版本。因为多信道DPA攻击直接串联不同信道的泄漏信号集合得到新的泄漏信号集合，并实施单信道DPA攻击，所以这里记为串联融合攻击算法（Cascaded Fusion Attack, 简写为CFA）。CFA算法是基于单信道DPA攻击拓展而成，须假设不同信道的泄漏性质一致，亦即泄漏模型相同。但如果攻击时将DPA换成CPA，就能打破这个限制条件。不过，该算法适用的另一个前提条件——不同侧信道对应同一敏感中间值的侧信息泄漏必须在时域上对齐，依旧需要成立。相较之下，本章对CFA算法稍加处理，发展出了不需要上述前提假设的改进版本，即SFA 算法。下面介绍SFA算法内容。

为了描述方便，我们假设密码芯片关于某一个敏感敏感中间值的能量泄漏发生在时刻t_k，电磁泄漏发生在时刻q_k。通常，和假设能量泄漏与真实能量泄漏存在线性关系[88] 类似，假设电磁泄漏与真实电磁泄漏也近似存在线性关系 [76,78,136]。所以，根据式 3-1, 3-20 及 3-21 可得

$$\boldsymbol{l}_{\boldsymbol{p}_{t_k}} = \alpha_{pow} f_{pow}(Z(\boldsymbol{x}, k)) + \beta_{pow} + \boldsymbol{\eta}_{\boldsymbol{p}_{t_k}} \tag{3-22}$$

及

$$\boldsymbol{l}_{\boldsymbol{e}_{q_k}} = \alpha_{em} f_{em}(Z(\boldsymbol{x}, k)) + \beta_{em} + \boldsymbol{\eta}_{\boldsymbol{e}_{q_k}} . \tag{3-23}$$

上面两个式子中，$\alpha_{pow}, \beta_{pow}, f_{pow}$分别表示密码芯片能量信道的信道参数及泄漏函数，$\boldsymbol{\eta}_{\boldsymbol{p}_{t_k}}$表示能量泄漏在时刻$t_k$的零均值噪声项，$\alpha_{em}, \beta_{em}, f_{em}$分别表示密码芯片电磁信道的信道参数及泄漏函数，$\boldsymbol{\eta}_{\boldsymbol{e}_{q_k}}$表示电磁泄漏在时刻$q_k$ 的零均值噪声项。

直接将能量泄漏L_{Pow}和电磁泄漏L_{EM}串联起来，得到的融合泄漏信号数目相比单信道的泄漏信号数目会增加一倍。直觉上，在此基础上攻击应该能提高侧信息泄漏利用率，从而增加侧信道分析效率。该思想是CFA算法的主要立足点，也是SFA算法的核心。不过因两个信道的信道参数$\alpha_{pow}, \beta_{pow}$和$\alpha_{em}, \beta_{em}$的不同，直接串联$L_{Pow}$和$L_{EM}$并实施攻击的话，新的融合泄漏与敏感中间值的假设泄漏线性相关关系将被削弱，相关分析时相关系数的值也会降低，甚至某些情境下攻击效果比单信道攻击还差。相比CFA串联不同信道泄漏前对泄漏信号不做任何处理而言，SFA算法做了一些改进，旨在消除信

道参数α_{pow},β_{pow}和α_{em},β_{em}对相关分析的负面影响，并使SFA算法能够在不同侧信道对应同一敏感中间值的侧信息泄漏产生于不同时刻的情况下，仍然有效。算法 3 详细描述了简单融合攻击算法。

Algorithm 3 简单融合攻击算法

输入： 能量泄漏集L_{Pow}，电磁泄漏集L_{EM}，密码算法输入$\boldsymbol{x}$，子密钥候选取值集合K

输出： 密钥猜测k_{guess}

for $i = 1, 2, \ldots, m$ **do**

  $\boldsymbol{l'_{p_i}} \leftarrow \boldsymbol{l'_{p_i}} - 1/n \sum_{j=1}^{n} l'_{p_{i,j}}$ //去均值

  $\boldsymbol{l'_{e_i}} \leftarrow \boldsymbol{l'_{e_i}} - 1/n \sum_{j=1}^{n} l'_{e_{i,j}}$

end for

for $j = 1, 2, \ldots, n$ **do**

  $\boldsymbol{l_{p_j}} \leftarrow (\boldsymbol{l_{p_j}} - 1/m \sum_{i=1}^{m} l_{p_{j,i}}) / \sqrt{\sum_{i=1}^{m} (\boldsymbol{l_{p_j}} - 1/m \sum_{i=1}^{m} l_{p_{j,i}})^2}$ //向量标准化

  $\boldsymbol{l_{e_j}} \leftarrow (\boldsymbol{l_{e_j}} - 1/m \sum_{i=1}^{m} l_{e_{j,i}}) / \sqrt{\sum_{i=1}^{m} (\boldsymbol{l_{e_j}} - 1/m \sum_{i=1}^{m} l_{e_{j,i}})^2}$

end for

$L_{fusion} \leftarrow [L_{Pow}^T \; L_{EM}^T]^T$

$\boldsymbol{f}_{fusion} \leftarrow [f_{pow}(Z(\boldsymbol{x}, k_{can}))^T \; f_{em}(Z(\boldsymbol{x}, k_{can}))^T]^T$

$k_{guess} \leftarrow \underset{k_{can} \in K}{\operatorname{argmax}} \max_{j=1}^{n} |\rho(\boldsymbol{l}_{f_j}, \boldsymbol{f}_{fusion})|$ //定义 $\boldsymbol{l}_{f_j}$为L_{fusion}第j个列向量

返回： k_{guess}

从算法 3 可以看出，SFA算法第一步通过减去每条泄漏信号的均值来消除不同信道泄漏信号在幅度上的差别。这些差别来自信号采集过程中夹杂的诸如基底电压之类的无用信号。第二步，SFA算法对能量泄漏集合L_{Pow}和电磁泄漏集合L_{EM}中的每条列向量进行向量标准化操作。以上两个步骤可以保证L_{Pow}和L_{EM}量纲一致，在该算法中具有举足轻重的地位。通过这两个步骤，SFA算法可以消除CFA算法的第二个限制条件的影响。原因分析如下：

首先考虑第一种情况。若$t_k = q_k$，即不同侧信道对应同一敏感中间值的侧信息泄漏同时发生，则通过算法 3 第二步之后，串联L_{Pow}和L_{EM}得到的融合泄漏集合L_{fusion}的第t_k个（或第q_k 个）列向量可以表示为

$$[(U(\boldsymbol{l}_{\boldsymbol{p}_{t_k}}))^T \; (U(\boldsymbol{l}_{\boldsymbol{e}_{q_k}}))^T]^T \; . \tag{3-24}$$

上式中，$U(\boldsymbol{x})$表示对向量$\boldsymbol{x}$进行向量标准化操作，即对向量$\boldsymbol{x}$去均值后再除以它的模。此时，信道参数$\alpha_{pow},\beta_{pow},\alpha_{em},\beta_{em}$被向量标准化操作消除，继而CFA算法中这些参数带来的负面影响被消除，使得新的融合泄漏与敏感中间值的假设泄漏线性相关关系依然保持，而且由于泄漏数目的翻倍，相关分析时相关系数的值将会增加，攻击效率较单信道攻击提高。

再考虑第二种情况。若$t_k \neq q_k$，即不同侧信道对应同一敏感中间值的侧信息泄漏不是同时发生，则通过算法 3 第二步之后，L_{fusion} 的第t_k个及第q_k个列向量分别为

$$[(U(\boldsymbol{l}_{\boldsymbol{p}_{t_k}}))^T \quad U((\beta_{em} + \boldsymbol{\eta}_{\boldsymbol{e}_{t_k}}))^T]^T, \tag{3-25}$$

和

$$[U((\beta_{pow} + \boldsymbol{\eta}_{\boldsymbol{p}_{q_k}}))^T \quad (U(\boldsymbol{l}_{\boldsymbol{e}_{q_k}}))^T]^T \ . \tag{3-26}$$

由于两个噪声项$\boldsymbol{\eta}_{\boldsymbol{e}_{t_k}}$和$\boldsymbol{\eta}_{\boldsymbol{p}_{q_k}}$都是零均值噪声，式 3-25 及 3-26 可简化为

$$[(U(\boldsymbol{l}_{\boldsymbol{p}_{t_k}}))^T \quad (\boldsymbol{\eta}_{\boldsymbol{e}_{t_k}}/\sigma_{e_{t_k}})^T]^T, \tag{3-27}$$

和

$$[(\boldsymbol{\eta}_{\boldsymbol{p}_{q_k}}/\sigma_{p_{q_k}})^T \quad (U(\boldsymbol{l}_{\boldsymbol{e}_{q_k}}))^T]^T \ . \tag{3-28}$$

上式中，$\sigma_{e_{t_k}}, \sigma_{p_{q_k}}$分别表示$\boldsymbol{\eta}_{\boldsymbol{e}_{t_k}}$和$\boldsymbol{\eta}_{\boldsymbol{p}_{q_k}}$的方差。此时，如果$t_k \neq q_k$，因式 3-27 中的第二项及 3-28 中的第一项皆为被归一化后的噪声项，既不包含敏感中间值的泄漏信息，又远小于两式中的敏感中间值泄漏项，所以SFA算法相当于分别在两个时刻t_k和q_k实施两个单信道攻击，有些类似于Max_FA算法 [78]，即在两个单信道攻击中选一个更好的结果来作为最终结果。此时SFA算法得到的泄漏信号信噪比会明显高于CFA算法。因此，SFA算法表现总是优于CFA算法，且不需要不同侧信道对应同一敏感中间值的侧信息泄漏必须同时发生的前提假设。显然，SFA算法和CFA算法同属于采用第一种融合方式的数据级融合攻击算法。

3.2.2　基于加权贝叶斯推断的融合攻击算法

式 3-8 描述了基于贝叶斯推断乘法律的融合方式。在子密钥任意候选值的先验概率都相等，即$P(k_i) = P(k_j), \forall i \neq j, i, j = 1, 2, \ldots, N$时，该融合方式近似等价于基于贝叶斯推断加法律的融合方式，即

$$k_{guess} = \underset{k_i \in K}{\operatorname{argmax}} \sum_{j=1}^{M} P(k_i|\boldsymbol{l}_j) \ . \tag{3-29}$$

两种融合方式的等价性证明如附录 A.2.2 所示。不过无论是采用加法律还是乘法律融合，都需要准确刻画$P(k_i|\boldsymbol{l}_j)$。这需要分析者对密码芯片泄漏特征完全了解，或者需要使用大量泄漏信号建模，实际中往往不可行。于是文献 [64]使用相关系数来替代概率分布。该做法是合理的，因为子密钥候选值k_i的相关系数与k_i是正确密钥的可能性呈正相关。从这个角度讲，文献 [78]提出的Sum_FA算法同属于基于贝叶斯推断的融合攻击方法，因为其利用加法律来融合各个单信道攻击的结果。因此，文献 [64]和 [78]提出的融合攻击算法是等价的。

然而，实际中不同信道的采集设备、信道参数及信号组成等往往不同，采集到的各个信道的泄漏信息质量也千差万别。例如，使用较大直径的电磁探针探测到的密码芯片泄漏往往充斥着时钟信号，相较芯片的能量泄漏包含更多的噪声；但若能使用小直径的电磁探针，对密码芯片涉及敏感中间值运算的内存位置精确定位，往往能获得远比能量泄漏纯净的泄漏信号。这就导致不同侧信道攻击的效果是有区别的，也即不同侧信道的侧信息泄漏对整个融合攻击的贡献是不同的。

式 3-8 和 3-29 无法体现不同侧信道对融合攻击的不同贡献，从而无法在融合攻击中充分利用每个侧信道的泄漏信息。着眼于此，我们将贝叶斯加法融合律扩展，通过给每个侧信道攻击结果$P(k_i|\boldsymbol{l_j})$分配一个权重系数ω_j，来区别不同侧信道的侧信息泄漏对整个融合攻击的贡献，如下式所示：

$$k_{guess} = \underset{k_i \in K}{\operatorname{argmax}} \sum_{j=1}^{M} \omega_j P(k_i|\boldsymbol{l_j}) \ . \tag{3-30}$$

式 3-30中，ω_j代表了第j个侧信道的侧信息泄漏信号质量及该信道在整个融合攻击中的贡献。第j个侧信道的侧信息泄漏中包含的与秘密信息相关的泄漏越多，信号质量越好，分配的权重系数ω_j值越大。这样一来，式 3-30 将目前所有的基于贝叶斯推断的融合攻击技术统一在了一个大框架下。例如，Sum_FA算法 [78]相当于认为$\omega_j = 1, \forall j$，即侧信道的侧信息泄漏对整个融合攻击的贡献完全一样。而Max_FA算法 [78]则在所有侧信道攻击结果中选取最好的作为最终结果，相当于只一个权重系数取1，其余皆取0，即只有一个侧信道有贡献，只不过这个侧信道编号并不固定。

对L_{Pow}及L_{EM}来讲（即$M = 2$），基于加权贝叶斯推断的融合攻击算法(Fusion Attack Based on Weighted Bayesian Inference, 简写为WBI_FA)的描述如算法 4 所示。其中，ω_{pow}和ω_{em}分别表示分配给L_{Pow}及L_{EM}的权重。综上所述，可以看出WBI_FA算法属于采用第一种融合方式的决策级融合攻击算法。

Algorithm 4 基于加权贝叶斯推断的融合攻击算法

输入： 能量泄漏集L_{Pow}及权重ω_{pow}，电磁泄漏集L_{EM}及权重ω_{em}，密码算法输入$\boldsymbol{x}$，子密钥候选取值集合K

输出： 密钥猜测k_{guess}

1: $P(k_i|\boldsymbol{l_{p_j}}) \leftarrow \max\limits_{j=1}^{n} |\rho(\boldsymbol{l_{p_j}}, f_{pow}(\boldsymbol{x}, k_i))|$

2: $P(k_i|\boldsymbol{l_{p_j}}) \leftarrow P(k_i|\boldsymbol{l_{p_j}}) / \sum_{i=1}^{N} P(k_i|\boldsymbol{l_{p_j}})$ //归一化

3: $P(k_i|\boldsymbol{l_{e_j}}) \leftarrow \max\limits_{j=1}^{n} |\rho(\boldsymbol{l_{e_j}}, f_{em}(\boldsymbol{x}, k_i))|$

4: $P(k_i|\boldsymbol{l_{e_j}}) \leftarrow P(k_i|\boldsymbol{l_{e_j}}) / \sum_{i=1}^{N} P(k_i|\boldsymbol{l_{e_j}})$

5: $k_{guess} \leftarrow \underset{k_i \in K}{\operatorname{argmax}} \ (\omega_{pow} P(k_i|\boldsymbol{l_{p_j}}) + \omega_{em} P(k_i|\boldsymbol{l_{e_j}}))$

6: **返回：** k_{guess}

3.2.3　基于奇异值分解的多信道融合攻击算法

在3.1.3小节我们提到，利用奇异值分解可以提取侧信道泄漏信号中与秘密信息相关的泄漏特征（即泄漏信号矩阵的左奇异向量），然后据此可以构建一种多信道融合攻击方案。下面首先介绍如何寻找侧信道泄漏信号中与秘密信息相关的泄漏特征集合。

首先对L_{Pow}进行奇异值分解。在公式3-10的基础上，L_{Pow}可以被分解成如下形式：

$$\begin{aligned} L_{Pow} &= \sum_{i=1}^{r} \sigma_i \boldsymbol{u_i} \boldsymbol{v_i^H} \\ &= \sum_{i=1}^{r1} \sigma_i \boldsymbol{u_i} \boldsymbol{v_i^H} + \sum_{i=r1+1}^{r2} \sigma_i \boldsymbol{u_i} \boldsymbol{v_i^H} + \sum_{i=r2+1}^{r} \sigma_i \boldsymbol{u_i} \boldsymbol{v_i^H}, \\ &= L_{Pow1} + L_{Pow2} + L_{Pow3} \ . \end{aligned} \tag{3-31}$$

式3-31中$r = rank(L_{Pow})$, $r1 = rank(L_{Pow1})$, $r2 = rank(L_{Pow2})$, $r3 = rank(L_{Pow3})$, $1 \le r1 \le r2 \le r$. 如果矩阵L_{Pow2}包含了秘密信息的主要或全部泄漏信息，那么左奇异向量（Left Single Vector，简写为LSV）集合$U_{pow} = [\boldsymbol{u_{r1+1}} \ldots, \boldsymbol{u_{r2}}]^T$称为密码芯片能量泄漏$L_{Pow}$的密钥泄漏特征集（Key Leakage Feature Set，简写为KLFS）。

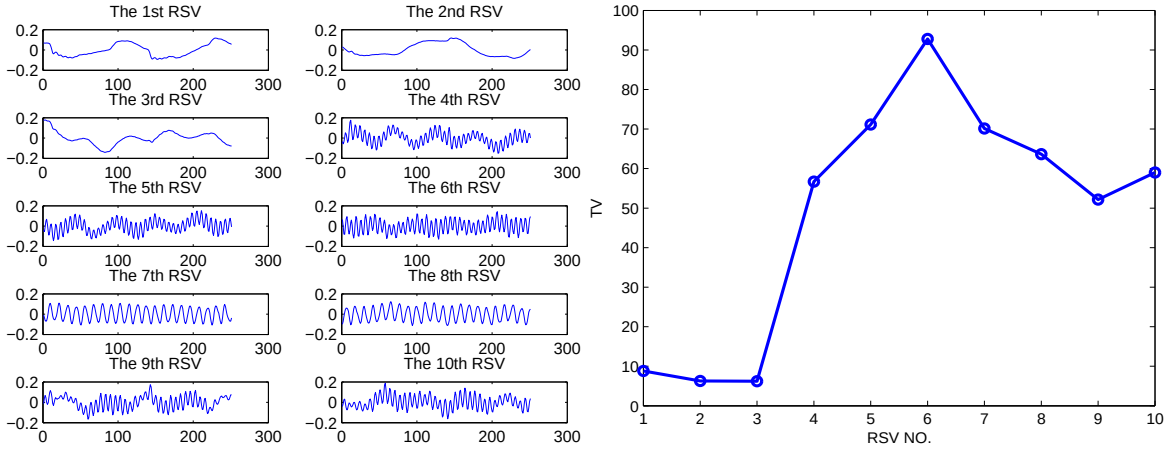
KLFS可以通过组成KLFS的左奇异值向量所对应的右奇异向量（Right Single Vector，简写为RSV）来寻找。相比其它在L_{Pow}内但不在KLFS中的LSVs，KLFS中的LSVs携带更多秘密信息泄漏，反映在时域上应该变化较大、几何曲线很不平坦。如前所述，泄漏信号集合L_{Pow}的左右奇异向量分别代表L_{Pow}的频率信息和时间信息，同时在时频分析领域，我们知道一个信号的时间信息和频率信息存在正交性[143]，所以KLFS中的LSVs所对应的RSVs应该比L_{Pow}内另外的RSVs在时域上变化小得多，也即前者的几何曲线比后者的几何曲线在外观上平坦得多。

综上所述，我们可以构造一个描述几何曲线平坦性的度量标准，例如离散总变分（Discrete Total Variation，简写为TV）[145]，来选择KLFS。L_{Pow}第i个右奇异向量v_i的离散总变分可表示如下：

$$TV = \sum_{j=0}^{n-1} | \ v_i^{j+1} - v_i^j \ |, \tag{3-32}$$

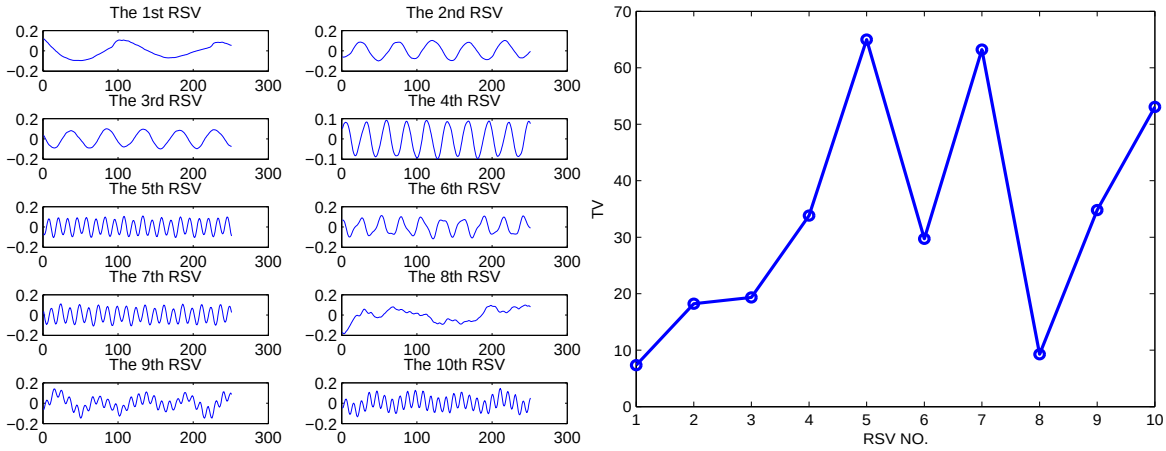
其中v_i^j是v_i第j个元素。图3.1(a)给出了一个实现在FPGA上的无保护AES-128加密算法最后一轮能量泄漏集合的前10个RSVs对应的几何曲线。该泄漏集合的第2和3个LSVs组成了KLFS，它们对应的RSVs的离散总变分的值也最小，如图3.1(b)所示。

同样地，电磁泄漏集合L_{EM}的KLFS（记为U_{em}）也可以相同的方法找到。图3.2(a)给出了与图3.1(a)中相同的AES-128算法实现的最后一轮电磁泄漏集合的前10个RSVs对应的几何曲线。该泄漏集合的第1个LSV组成了KLFS，它所对应的RSV的离散总变分的值也最小，如图3.2(b)所示。



(a) 能量泄漏的前10个RSVs　　(b) 能量泄漏的前10个RSVs的TVs值

图 3.1　无保护AES-128 FPGA实现的能量泄漏的前10个RSVs及其TVs



(a) 电磁泄漏的前10个RSVs　　(b) 电磁泄漏的前10个RSVs的TVs

图 3.2　无保护AES-128 FPGA实现的电磁泄漏的前10个RSVs及其TVs

Algorithm 5 基于奇异值分解的融合攻击算法

输入： 能量泄漏集L_{Pow}，电磁泄漏集L_{EM}，密码算法输入$\boldsymbol{x}$，子密钥候选取值集合K

输出： 密钥猜测k_{guess}

1: 分别对L_{Pow} 和 L_{EM}进行奇异值分解

2: 分别找到L_{Pow}的 KLFS U_{pow} 及 L_{EM}的KLFS U_{em}

3: $U_{pow} \leftarrow Std(U_{pow})$, $U_{em} \leftarrow Std(U_{em})$　//标准化

4: $L_{fusion} \leftarrow [U_{pow}^T \ U_{em}^T]^T$

5: $\boldsymbol{f}_{fusion} \leftarrow [f_{pow}(Z(\boldsymbol{x}, k_{can}))^T \ f_{em}(Z(\boldsymbol{x}, k_{can}))^T]^T$

6: $k_{guess} \leftarrow \underset{k_{can} \in K}{\operatorname{argmax}} \ \max\limits_{j=1}^{n} |\rho(\boldsymbol{l}_{f_j}, \ \boldsymbol{f}_{fusion})|$　//令$\boldsymbol{l}_{f_j}$表示L_{fusion} 的第j个列向量

7: **返回：** k_{guess}

在得到两个侧信道泄漏信号集合的KLFS U_{em}和U_{pow}之后，我们将二者结合起来组成新的融合泄漏特征集，然后在其上实施单信道攻击。算法 5 详细描述了基于奇异值

分解的融合攻击算法（SVD-Based Fusion Attack，简写为SVD_FA）。注意算法 5 中第三步使用了一个标准化函数Std来使U_{pow}和U_{em}量纲保持一致，以免影响矩阵分解效果。

SVD_FA算法要求每个侧信道中依赖于秘密信息的泄漏必须集中在少数特征上（即要求式 3-31 中$(r2-r1) \ll r$）。如果能满足这个要求，该融合攻击算法相对单信道攻击而言，能充分利用各个侧信道的泄漏信息，极大地提高侧信道攻击效率。否则，如果单信道依赖于秘密信息的泄漏特征过于分散，以致找不到单信道泄漏的密钥泄漏特征集，该融合攻击算法有可能无法实施。综上可知，SVD_FA算法属于使用第一类融合方式的特征级融合攻击算法。

3.2.4　基于广义奇异值分解的融合攻击算法

基于广义奇异值分解的融合攻击算法（GSVD-Based Fusion Attack，简写为GSVD_FA）类似于SVD_FA算法，不过如前面第 3.1.4 小节所述，GSVD_FA算法利用的是通过GSVD得到的两个不同侧信道泄漏的联合特征。该融合攻击算法首先将两个泄漏集合(L_{Pow}和L_{EM})按不同次序分别串联起来得到两个矩阵(L_{Pow}, L_{EM})和(L_{EM}, L_{Pow})，之后对这两个矩阵分别进行广义奇异值分解，得到公式 3-13 中的U和V。而U和V即可被视为L_{Pow}和L_{EM}中依赖于密钥的侧信息泄漏的联合特征集。最后，对得到的新的联合特征集进行单信道相关分析恢复密钥。算法 6 给出了GSVD_FA算法的详细步骤。

Algorithm 6 基于广义奇异值分解的融合攻击算法

输入： 能量泄漏集L_{Pow}，电磁泄漏集L_{EM}，密码算法输入$\boldsymbol{x}$，子密钥候选取值集合K

输出： 密钥猜测k_{guess}

1: 分别计算矩阵$[L_{Pow}^T \ L_{EM}^T]^T$和$[L_{EM}^T \ L_{Pow}^T]^T$的广义奇异值分解得到联合特征集U和V

2: $L_{fusion} \leftarrow [U^T \ V^T]^T$

3: $\boldsymbol{f}_{fusion} \leftarrow [f_{pow}(Z(\boldsymbol{x}, k_{can}))^T \ f_{em}(Z(\boldsymbol{x}, k_{can}))^T]^T$

4: $k_{guess} \leftarrow \underset{k_{can} \in K}{\operatorname{argmax}} \ \max\limits_{j=1}^{n} |\rho(\boldsymbol{l}_{f_j}, \boldsymbol{f}_{fusion})|$ //令$\boldsymbol{l}_{f_j}$表示L_{fusion}的第j个列向量

5: **返回：** k_{guess}

GSVD_FA算法适用的前提条件与SVD_FA算法一致，即每个侧信道中依赖于秘密信息的泄漏必须集中在少数特征上。显然，GSVD_FA算法属于使用第二类融合方式的特征级融合攻击算法。

3.2.5　基于非负矩阵分解的数据融合攻击算法

如小节所述，式 3-14 中L可视为采自多个侧信道的泄漏的集合，特征矩阵W可视为多个侧信道泄漏信号集合融合后得到的泄漏集合，因此求解出W就可以进行多信道融合攻击。下面介绍其原理。

一个密码芯片的能量泄漏集合L_{Pow}和电磁泄漏集合L_{EM}可以看作是以不同传感器（如电流探针和电磁探针等）测量得到的密码芯片真实泄漏的不同形式的记录。显然，

密码芯片的真实泄漏包含的信息更丰富，而以不同传感器采集得到的不同侧信息泄漏总会有不同程度的“失真”。而我们融合多个侧信道泄漏信息的过程，就是试图获得更多更全面的密码芯片的真实泄漏信息，甚至完全获取密码芯片全部的真实泄漏信息的过程。所以从这个角度出发，我们可将密码芯片的真实泄漏视为将多个侧信道信息融合得到的泄漏，并且该真实泄漏恰好可以通过NMF来获取。如果将式 3-14 中L视为侧信道泄漏L_{Pow}和L_{EM}的集合，那么特征矩阵W可视为密码芯片的真实泄漏，亦即融合泄漏，而系数矩阵H则刻画了不同传感器的失真程度。下面介绍基于非负矩阵分解的数据融合攻击算法（NMF-based Fusion Attack on Raw Leakages，简写为NMFRL_FA）。

将矩阵L_{Pow}和L_{EM}分别按列或按行展开，得到大小为$mn \times 1$的两个列向量。之后将这两个列向量作为矩阵L的列向量而构造出L。由于我们希望得到的融合数据集逼近密码芯片的真实泄漏，其大小应该和单信道泄漏集合大小一致，即设置$d = 1$。若考虑泄漏集合存在噪声（设为E），则式 3-14 可改写为

$$L \approx WH + E,\ s.t.\ W \geq 0,\ H \geq 0\ . \tag{3-33}$$

故而，使用优化算法来收敛噪声项E趋于稳定的过程也就是泄漏数据融合的过程，亦即

$$(W, H) = \underset{W,H}{\operatorname{argmin}} \parallel E \parallel_F^2 = \underset{W,H}{\operatorname{argmin}} \parallel L - WH \parallel_F^2\ . \tag{3-34}$$

上述最优化问题可以使用交互最小平方算法（Alternating Least Squares，简写为ALS）来求解 [147,148]。在得到特征矩阵W之后，将向量$W \in \mathbb{R}^{mn\times 1}$变形，每次从中按序取$m$个元素，依次作为新的矩阵的列，得到融合泄漏集合对应的矩阵$W \in \mathbb{R}^{m\times n}$。最后，我们使用融合泄漏集合$W$实施单信道攻击。算法 7 列出了NMFRL_FA算法的详细流程。可以看出，NMFRL_FA算法属于使用第二类融合方式的数据级融合攻击算法。

Algorithm 7 基于非负矩阵分解的数据融合攻击算法

输入： 能量泄漏集L_{Pow}，电磁泄漏集L_{EM}，密码算法输入$\boldsymbol{x}$，子密钥候选取值集合K，预置参数d

输出： 密钥猜测k_{guess}

1: 分别按列展开L_{Pow} 和 L_{EM}，并作为L的列向量得到L

2: $d \leftarrow 1$，使用ALS算法计算$W \in \mathbb{R}^{mn\times d}$

3: 变形向量W，每次按序取m元素依次作为新矩阵的列，使之变为$W \in \mathbb{R}^{m\times n}$

4: $L_{fusion} \leftarrow [W^T\ W^T]^T$

5: $\boldsymbol{f}_{fusion} \leftarrow [f_{pow}(Z(\boldsymbol{x}, k_{can}))^T\ f_{em}(Z(\boldsymbol{x}, k_{can}))^T]^T$

6: $k_{guess} \leftarrow \underset{k_{can}\in K}{\operatorname{argmax}} \max\limits_{j=1}^{n} |\rho(\boldsymbol{l}_{f_j}, \boldsymbol{f}_{fusion})|$ //令$\boldsymbol{l}_{f_j}$表示L_{fusion} 的第j个列向量

7: **返回：** k_{guess}

3.2.6　基于非负矩阵分解的决策融合攻击算法

NMFRL_FA算法将一个密码芯片的能量泄漏集合L_{Pow}和电磁泄漏集合L_{EM}看作以不同传感器（如电流探针和电磁探针等）测量得到的密码芯片真实泄漏（融合后的泄漏）的不同形式的记录。类似地，如果将单信道攻击结果看作“真实”攻击结果（联合多个侧信道攻击后的结果）的不同记录，我们还可以在NMF的基础上发展出一种决策级融合攻击方法。下面详细介绍该方法。

第一步，使用L_{Pow}实施CPA攻击，计算出所有子密钥候选值在所有时刻的相关系数值，并将这些相关系数值组成的矩阵（行向量表示某一子密钥候选值在不同时刻的相关系数值，列向量表示不同子密钥候选值在同一时刻的相关系数值）记为Δ_{Pow}；然后使用L_{EM}实施CEMA攻击，计算出所有子密钥候选值在所有时刻的相关系数值，并将这些相关系数值组成的矩阵记为Δ_{EM}。接着，对矩阵Δ_{Pow} 和Δ_{EM}取绝对值以保证$\Delta_{Pow} \geq 0$, $\Delta_{EM} \geq 0$。最后，类似算法 7 将矩阵Δ_{Pow} 和Δ_{EM}按列展开组成新矩阵后，进行非负矩阵分解得到特征矩阵W，并选择对应最大值的密钥候选值作为密钥猜测。

因为该算法是在单信道攻击得到的相关系数绝对值上实施的，而相关系数绝对值的取值范围是$[0,1]$，所以想要得到的特征矩阵W也应该与相关系数具有相同的物理含义，即限定W的取值范围也是$[0,1]$。进一步地，一个成功的攻击中，对应于正确密钥的最大相关系数值应该远远大于其它密钥候选值所对应的最大相关系数值。也就是说，所有密钥候选值对应的最大相关系数值应呈现出稀疏性，即非负矩阵分解求出的解应是稀疏的。于是，式 3-33 可修正为

$$L \approx WH + E,\ s.t.\ 0 \leq W \leq 1,\ H \geq 0\ . \tag{3-35}$$

式 3-34 也应调整为

$$\begin{aligned}(W,H) &= \underset{W,H}{\operatorname{argmin}} \parallel E \parallel_F^2 + \lambda \parallel W \parallel_F^2 \\ &= \underset{W,H}{\operatorname{argmin}} \parallel L - WH \parallel_F^2 + \lambda \parallel W \parallel_F^2\ .\end{aligned} \tag{3-36}$$

上式中λ是可调节参数，用来保证解的稀疏性 [147]。注意这里的E不再是噪声项，而是误差项。上式的求解可使用交互受限最小平方算法（Alternating Constrained Least Squares，简写为ACLS） [147,148]。可以看出，该算法与NMFRL_FA算法的不同之处在于标函数及限制条件。基于非负矩阵分解的决策融合攻击算法（NMF-based Fusion Attack on Correlation Coefficient Matrices，简写为NMFCCM_FA）流程见于算法 8。从算法融合的方式可知，NMFCCM_FA算法属于使用第二类融合方式的决策级融合攻击算法。

3.3　算法性能评估

为了分析、验证我们所提出的六种多信道融合攻击算法的效率，以及它们所采取

Algorithm 8 基于非负矩阵分解的决策融合攻击算法

输入： 能量泄漏集L_{Pow}，电磁泄漏集L_{EM}，密码算法输入$\boldsymbol{x}$，子密钥候选取值集合K，预置参数λ

输出： 密钥猜测k_{guess}

使用CPA和CEMA分别获取所有子密钥候选值的相关系数矩阵Δ_{Pow} 和 Δ_{EM}

$\Delta_{Pow} \leftarrow |\Delta_{Pow}|, \Delta_{EM} \leftarrow |\Delta_{EM}|$

按列展开Δ_{Pow} 和 Δ_{EM}，并作为L的列向量得到L

$d \leftarrow 1$，并使用ACLS算法计算$W \in \mathbb{R}^{nN \times d}$ //N表示子密钥候选值集合K的势

r变形向量W，每次按序取m元素依次作为新矩阵的列，使之变为$W \in \mathbb{R}^{N \times n}$

$index \leftarrow \underset{i=1}{\overset{N}{\arg\max}} \ \underset{j=1}{\overset{n}{\max}} \ \boldsymbol{W}_j$ //定义$\boldsymbol{W}_j$为W第j个列向量

$k_{guess} \leftarrow K(index)$ //定义集合K的第$index$个元素为$K(index)$

返回： k_{guess}

的不同融合方式对攻击效率的影响，根据前面对多信道融合攻击的分类，我们将在一个统一的框架下，分别考察这些算法针对典型的AES-128加密算法的不同实现方案（包括无保护软件实现、硬件实现及有保护实现）的攻击效果，并对比各个单信道攻击及已有多信道融合攻击方案分析结果，以期为针对密码算法的不同实现如何选择和实施高效的多信道融合攻击方法提出建议。

3.3.1 实验设置及参数

本章节分别在一个软件平台和一个硬件平台上实施实验来验证所提六种方法的效率。不失一般性，我们这里利用两种典型的侧信息泄漏——能量泄漏和电磁泄漏来做融合攻击。因实验所使用的示波器（型号：Agilent DSO9104A）不能以不同的采样率同时从不同的通道采集侧信道泄漏信号，所以信号采集中我们在能量泄漏通道和电磁泄漏通道上使用了同一个采样率。虽然一般能量泄漏信号与电磁泄漏信号都可近似视为低通信号 [149]，但能量泄漏信号与电磁泄漏信号的组成及频率成分差别很大，常常后者的最大频率要远高于前者的最大频率。根据通信与信号处理理论中的奈奎斯特-香农抽样定理 [149]，只有采样率不低于被采样信号最大频率的2倍时，才能无损地恢复出原始信号，否则会发生信号混叠。显然电磁泄漏信号的采样率要远高于能量泄漏信号的采样率。如果我们设置的采样率过高，则能量泄漏信号会发生过采样，产生过多的采样点，使得所采集泄漏信号的存储需求大大增加，而且计算代价反而会因过多的采样点数而增加，但能量分析的结果却不会因此有明显改善；如果我们设置的采样率过低，则电磁泄漏信号会发生降采样，损失一部分依赖于密钥的泄漏信息，削弱电磁攻击的效率。但是，如果我们能够在过高和过低的采样率之间选择一个合适的采样率，那么就可以平衡两个侧信道泄漏信号的需求，将采样率带来的负面影响降到最低。不同采样率对侧信道攻击的影响将在本章节第 3.3.4 小节详细讨论。

实验所使用的软件平台为内嵌了一个工作时钟频率为11.0592MHz的8-bit 8051 MCU的集成电路板。我们在该芯片上实现了一个串行的无保护AES-128加密算法，并采集了算法运行过程中芯片的能量和电磁泄漏。两个通道使用同一个触发信号触发，同时采集，且共同的采样率设为1.25GSa/s。这里，我们测量了密码算法运行时连接在单片机GND (Ground) 路径上的一个50Ω电阻的电压降，并将之作为该8-bit单片机的能量泄漏信号。而该8-bit单片机的电磁泄漏信号则通过一个直径10mm的H场电磁探针来测量。该探针被垂直放置在单片机寄存器位置的表面上。该AES-128的8-bit MCU实现的能量泄漏和电磁泄漏函数皆可近似视为汉明重量泄漏。我们总共随机输入了500条随机信息，采集了密码算法运行中这些随机输入所对应的500条能量泄漏信号和500条电磁泄漏信号。而且每条泄漏信号对应于AES-128加密算法的第一轮泄漏，分别包含了500,000个采样点。

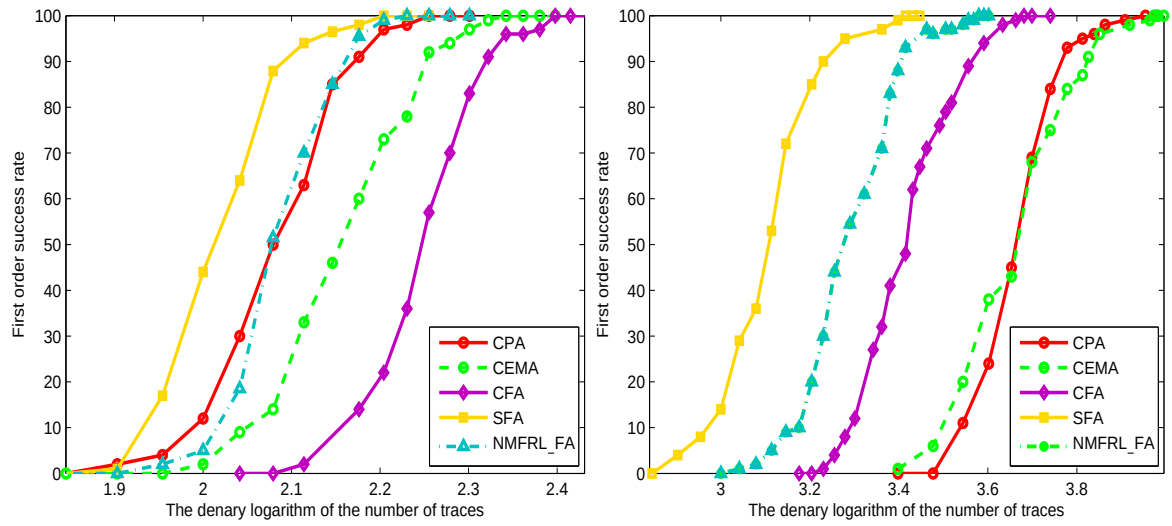
实验所使用的硬件平台为一个嵌入了FPGA (Xilinx Kintex-7)芯片的SAKURA-X开发板。我们在该芯片上实现了一个并行的无保护AES-128加密算法（工作频率为20MHz），并采集了算法运行过程中芯片的能量和电磁泄漏。两个通道使用同一个触发信号触发，同时采集，且共同的采样率设为5GSa/s。这里，我们测量了密码算法运行时连接在FPGA开发板VDD (Voltage Drain Drain) 路径上的一个49.9Ω电阻的电压降，并将之作为该FPGA的能量泄漏信号。而该FPGA的电磁泄漏信号则通过一个直径10mm的H场电磁探针来测量。该探针被垂直放置在FPGA周边位置的一个去耦电容器的表面上。该AES-128的FPGA实现的能量泄漏和电磁泄漏函数皆可近似视为汉明距离泄漏。我们总共随机输入了30,000条随机信息，采集了密码算法运算中这些随机输入所对应的30,000条能量泄漏信号和30,000条电磁泄漏信号。而且每条泄漏信号对应于AES-128加密算法的最后一轮泄漏，分别包含了250个采样点。

在实验中，针对实现在8-bit单片机上的AES的攻击目标是第一轮S盒的输出，而针对实现在FPGA上的AES的攻击目标是最后一轮S盒输入与输出的异或。我们同时对比了两类单信道攻击方法——CPA、CEMA，以及三类具有代表性的多信道融合攻击算法——CFA [15]、Sum_FA和Max_FA [78] 的攻击效果。而文献 [64]所提出的用于组合分析的基于贝叶斯推断乘法律融合的攻击方法（Production Fusion Attack，简写为Pro_FA）也被用来作对比。注意，因矩阵分解对矩阵元素数目变化比较敏感，凡文中多信道融合攻击方法中涉及矩阵分解的，都是在每条侧信息泄漏信号所有样本点上操作。

3.3.2 实验结果与分析

图 3.3, 3.4 及 3.5 分别给出了能量攻击、电磁攻击及各个多信道融合攻击方案攻击无保护AES-128算法的8-bit MCU实现及FPGA实现的一阶成功率曲线。注意，这里所有多信道融合攻击算法同时使用相同数目的能量泄漏信号和电磁泄漏信号进行攻击，并将所使用的某一单信道的侧信息泄漏信号数目作为其攻击所需的泄漏信号数目。这样

做是合理的，因为多个单信道泄漏可以同时获得，且多信道融合攻击算法通过联合多个信道而不是靠增加单个信道的泄漏量来提高侧信息利用率。从三个图中可以看出，几乎所有的多信道融合攻击算法都显著提升了单信道攻击（即CPA和CEMA）效率。另外可以发现，单信道攻击中CPA之所以比CEMA好，是因为我们采集电磁泄漏时所使用的H场电磁探针相对其测量的组件来讲直径较大，以致采集到的电磁泄漏包含比能量泄漏更多的冗余噪声（如时钟信号）[150]。接下来我们将分别对三组不同类型的多信道融合攻击算法的攻击结果进行介绍、分析。



(a) 针对AES 8-bit MCU实现的CPA, CEMA及数据级MCFAs攻击结果

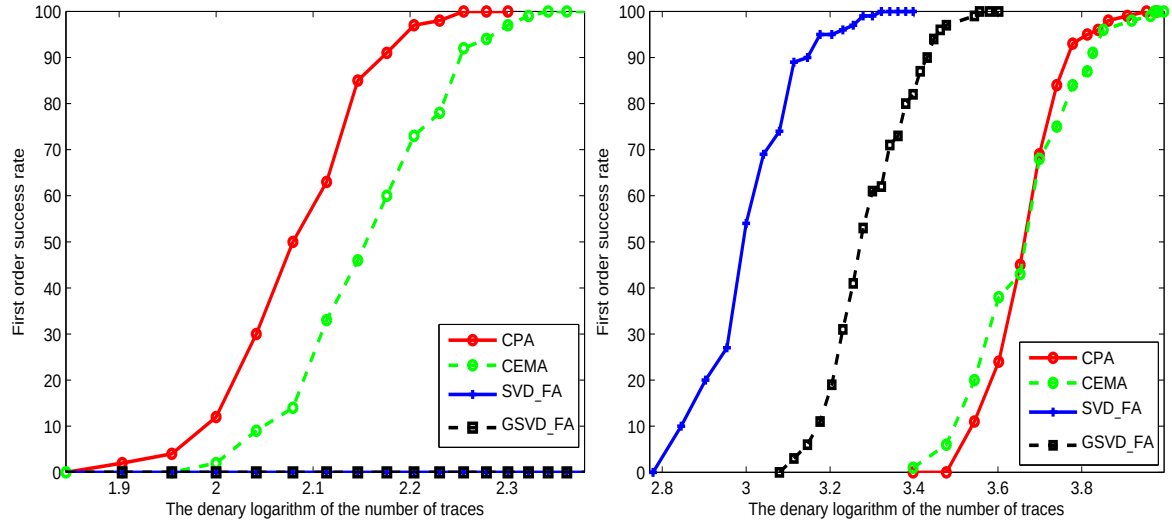
(b) 针对AES FPGA实现的CPA, CEMA及数据级MCFAs攻击结果

图 3.3 针对无保护AES-128算法的8-bit MCU实现及FPGA实现的CPA、CEMA及数据级MCFAs攻击结果

3.3.2.1 数据级多信道融合攻击

从图 3.3 中可以看出，在针对无保护AES-128的8-bit MCU实现的攻击中，串联融合攻击算法CFA性能甚至劣于两个单信道攻击CPA和CEMA。相反地，CFA在攻击无保护AES-128的FPGA实现时却较大幅度优于CPA和CEMA。这是因为无保护AES-128的8-bit MCU实现是串行实现，与敏感中间值相关的泄漏特征点数目较少，而且同一个敏感中间值的能量泄漏与电磁泄漏产生于不同时刻。这恰恰属于CFA适用的前提假设——不同侧信道对应同一敏感中间值的侧信息泄漏必须同时发生——无法满足的情形。相比之下，无保护AES-128的FPGA实现是并行实现，与敏感中间值相关的泄漏特征点数目要较MCU实现多上很多，而且同一个敏感中间值的能量泄漏与电磁泄漏发生在同一时刻的情况极多。相比CFA算法，我们提出的简单融合攻击算法SFA在针对无保护AES-128的8-bit MCU实现攻击中，表现优于CFA、CPA及CEMA（图 3.3(a)），甚至在攻击无保护AES-128的FPGA实现时性能排在第二位（图 3.3(b)）。以上现象和结果验证了本章前面第 3.2.1 小节关于SFA优于CFA和单信道攻击，以及不需要不同侧信道

对应同一敏感中间值的侧信息泄漏必须时域对齐的假设的分析。基于非负矩阵分解的数据融合攻击算法NMFRL_FA将不同侧信道泄漏视为融合泄漏的不同记录，并试图借助这些“记录”恢复出融合泄漏。显然，单信道泄漏中包含的敏感中间值泄漏特征点越多，说明对原有“真实”泄漏的失真越小，就越有利于“真实”泄漏的恢复。所以NMFRL_FA算法攻击AES-128的FPGA实现的效率优于攻击8-bit MCU实现的效率。然而，NMFRL_FA算法是基于非负矩阵分解的，而后者的求解是一个优化问题，需要近似计算且解不唯一，因此相较其它多信道融合攻击算法，NMFRL_FA在攻击无保护AES-128的FPGA实现中的表现处于中间水平。



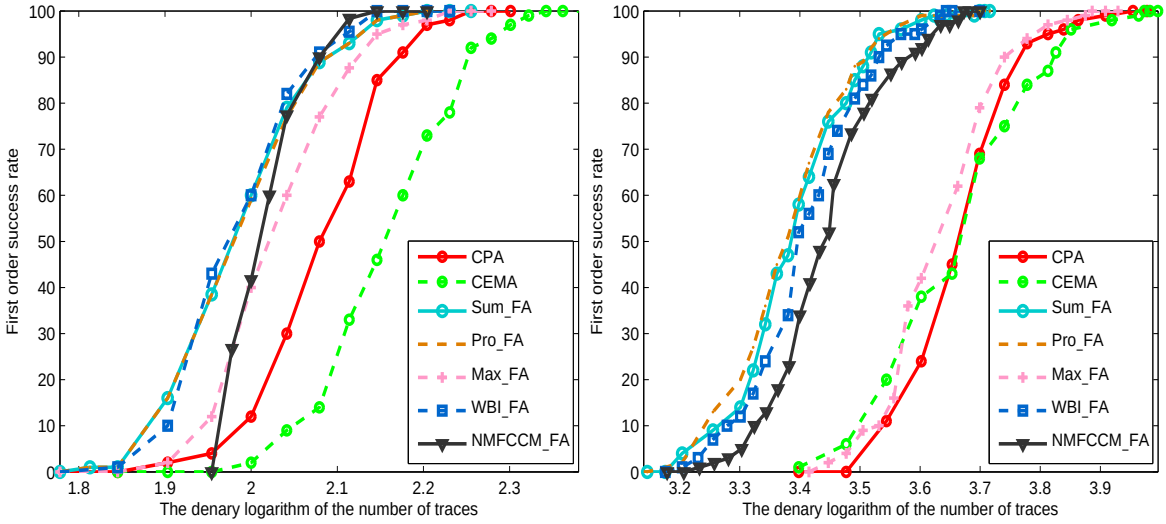
(a) 针对AES 8-bit MCU实现的CPA, CEMA及特征级MCFAs攻击结果　(b) 针对AES FPGA实现的CPA, CEMA及特征级MCFAs攻击结果

图 3.4　针对无保护AES-128算法的8-bit MCU实现及FPGA实现的CPA、CEMA及特征级MCFAs攻击结果

3.3.2.2　特征级多信道融合攻击

从图 3.4 中可以看出，在攻击无保护AES-128的FPGA实现中，基于奇异值分解的多信道融合攻击算法SVD_FA效率最高。然而在攻击无保护AES-128 的8-bit MCU实现中，SVD_FA算法却无法实施。其原因在于：无保护AES-128的FPGA实现中与敏感中间值相关的泄漏特征点数目较多，依赖于秘密信息的能量泄漏集中于其能量泄漏集合的第2个和第3个左奇异向量，而依赖于秘密信息的电磁泄漏集中于其电磁泄漏集合的第1个左奇异向量。也即，无保护AES-128的FPGA实现的每个单信道中依赖于秘密信息的泄漏都集中于少数特征上，所以很容易找到每个侧信道泄漏的密钥泄漏特征集KLFS。与之相反，AES-128的8-bit MCU实现中与敏感中间值相关的泄漏特征点数目较少，依赖于秘密信息的能量泄漏与电磁泄漏都分散在相应泄漏集合的前100个左奇异向量上，利用找到的每个侧信道泄漏的KLFS无法实施成功的攻击。这两组实验结果与前面第 3.2.3 小节的分析一致。基于广义奇异值分解的多信道融合攻击算法GSVD_FA在

攻击两种不同的实现时的表现类似于SVD_FA算法，不过由于相比SVD分别从能量泄漏和电磁泄漏中提取的密钥泄漏特征而言，GSVD从两个侧信道中提取的联合泄漏特征可能会损失一些单信道泄漏信息或引入一些冗余信息，导致GSVD_FA算法在图 3.4(b) 中的表现不如SVD_FA算法。



(a) 针对AES 8-bit MCU实现的CPA, CEMA及决策级MCFAs攻击结果

(b) 针对AES 8-bit MCU实现的CPA、CEMA及决策级MCFAs攻击结果

图 3.5 针对无保护AES-128算法的8-bit MCU实现及FPGA实现的CPA、CEMA及决策级MCFAs攻击结果

3.3.2.3 决策级多信道融合攻击

从图 3.5 中可以发现，因为充分考虑到了不同侧信道泄漏包含的对攻击有用的侧信息不同，并以此分配权重系数来充分体现每个单信道对融合攻击的贡献，基于加权贝叶斯推断的融合攻击算法WBI_FA性能较Sum_FA及Max_FA算法要好。如前面第 3.3.1 所述，两个平台上采集到的能量泄漏信号质量略优于相应的电磁泄漏信号，所以在两个实验中分配给能量通道的权重略大于分配给电磁通道的权重。图 3.5(a) 分配给能量通道和电磁通道的权重分别为0.535和0.465，图 3.5(b) 分配给能量通道和电磁通道的权重分别是0.5035及0.4965。统一来讲，Sum_FA算法是各个侧信道权重都为1的WBI_FA算法，而Max_FA算法可以看成只有一个侧信道权重为1、其它为0的WBI_FA算法，不过这个权重为1的信道并不固定，一直在变化。本质上，Max_FA算法仅仅是选择所有单信道攻击结果中最好的那个作为最终结果。这使得Max_FA算法的性能总会优于每个单信道攻击，却不会高出最优的单信道攻击很多。而Pro_FA算法是基于贝叶斯推断乘法律的融合攻击，本质上近似等价于基于贝叶斯推断加法律的融合攻击算法Sum_FA（如第 3.2.2 所述），所以Pro_FA算法在图中一阶攻击成功率曲线与Sum_FA算法十分接近。二者都没有充分体现不同侧信道对融合攻击的贡献。基于非负矩阵分解的决策融合攻击算法NMFCCM_FA在攻击AES-128的8-bit MCU实现中，即使与敏感中间值相关的泄

漏特征点极少，也表现优于其它所有多信道融合攻击算法（图 3.5(a), $\lambda = 0$）。但是，NMFCCM_FA算法攻击AES-128的FPGA实现时效率并不算突出（图 3.5(b), $\lambda = 0.5$）。这是因为NMFCCM_FA算法融合的是每个单信道攻击所得的所有子密钥候选值在所有时刻的相关系数矩阵，而AES-128的FPGA实现中过多的泄漏特征点可能无法满足解的强制稀疏性，反过来可能将求出的解引导向错误的子密钥猜测值。

此外，从图 3.3，3.4 及 3.5 上同样可以观察到不同融合方式对多信道融合攻击算法性能的影响。实验中用到的多信道融合算法，如CFA、SFA、Sum_FA、Pro_FA、Max_FA、WBI_FA及SVD_FA算法，在联合各个侧信道前，分别单独处理单信道泄漏信号、提取单信道泄漏特征或进行单信道攻击；而另外的几个算法，如NMFRL_FA、GSVD_FA及NMFCCM_FA算法则分别利用所有侧信道泄漏的联合信息、提取所有侧信道泄漏的联合泄漏特征或利用所有侧信道攻击结果的联合信息，来实施分析。总体看，无论攻击无保护AES-128的8-bit MCU实现或FPGA实现，采用第一种融合攻击方式的数据级融合攻击算法效率都高于采用第二种融合攻击方式的数据级融合攻击算法；采用两种融合攻击方式的特征级融合攻击算法攻击无保护AES-128的8-bit MCU实现时都失效，而攻击无保护AES-128的FPGA实现时，采用第一种融合攻击方式的特征级融合攻击算法性能优于采用第二种融合攻击方式的特征级融合攻击算法；采用第二种融合攻击方式的决策级融合攻击算法攻击无保护AES-128的8-bit MCU实现时，表现好于采用第一种融合攻击方式的决策级融合攻击算法，而攻击无保护AES-128的FPGA实现时，二者性能差不多。从实验结果来看，我们可以对无保护的密码算法的不同实现采取何种多信道融合攻击算法提供一些建议，例如：若一个无保护的密码算法实现对应于同一敏感中间值的不同侧信道的侧信息泄漏特征点较少，且在时域上不是同时发生的，那么我们依次推荐决策级、数据级融合攻击算法。这种情况下，优先推荐采用第二种融合方式的决策级融合攻击算法或采用第一种融合攻击方式的数据级融合攻击算法。若一个无保护的密码算法实现对应于同一敏感中间值的不同侧信道的泄漏特征点很多，且这些点在时域上多数是对齐的，那么我们依次推荐特征级、数据级及决策级融合攻击算法。这种情况下，优先推荐采用了第一种融合方式的多信道融合攻击算法。

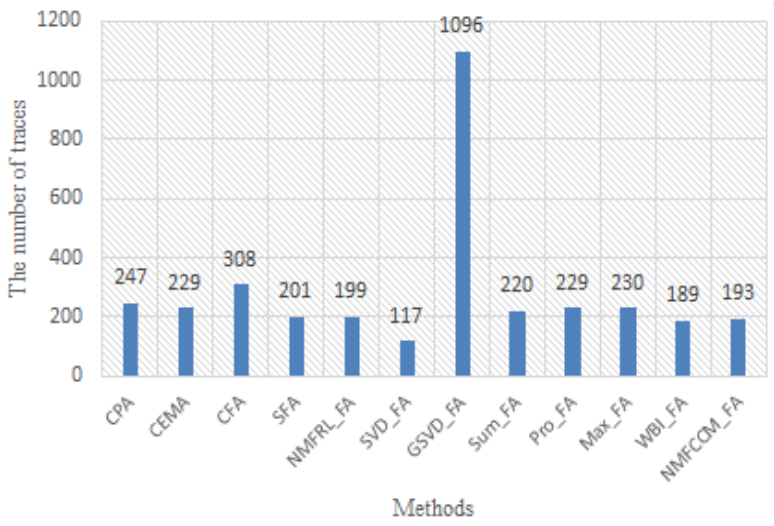
3.3.3　补充实验

为了进一步深入评估多信道融合攻击算法的性能，我们同样测量了一个实现在8-bit单片机上的有保护AES-128加密算法运行中的能量泄漏和电磁泄漏。该实现是串行实现，且受随机产生的布尔掩码保护 [10]。除了采集的侧信息泄漏数目是5,000条外，该实验采集泄漏信号时用到的设备及设置参数皆与第 3.3.1 节中采集无保护的AES-128的8-bit MCU实现泄漏时一样。我们这里对该受保护的AES-128掩码实现方案实施二阶侧信道攻击 [10]。攻击目标选择的是无保护AES-128加密算法第一轮的第一个S盒输出。我们使用有保护AES-128加密算法第一轮第一个掩码S盒输出的泄漏与第一轮第一

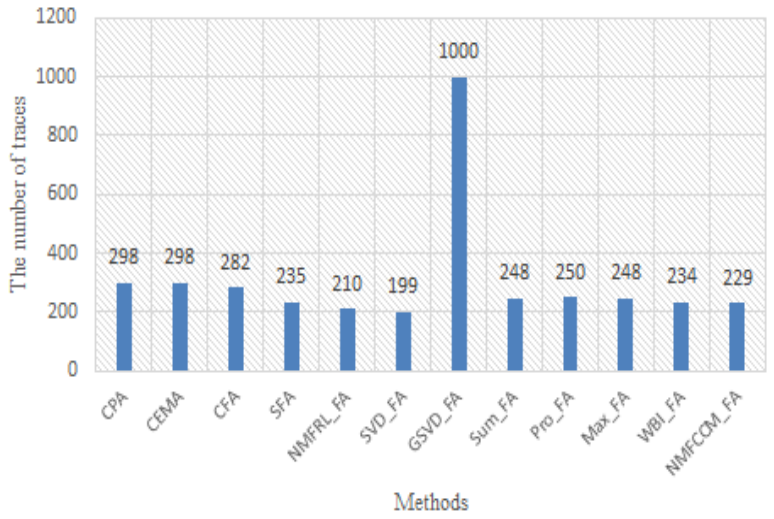
个输出掩码的泄漏的绝对值差，来近似代替该敏感中间值的实际泄漏 [10]。这需要在攻击前分别对所有侧信道泄漏信号进行预处理。以能量泄漏为例，在预处理阶段，我们大致确定有保护AES-128加密算法第一轮第一个掩码S盒输出对应的泄漏特征点的位置，在附近沿时间轴选取一个小邻域，然后大致确定第一轮第一个输出掩码的泄漏特征点位置并在附近沿时间轴选取一个小邻域，最后将这两个邻域内包含的元素两两组合求绝对值差，得到一个预处理后的泄漏集合，即是我们进行二阶攻击的所需要的能量泄漏集合。类似地，可以得到攻击所需的预处理后的电磁泄漏集合。经过预处理之后，得到的能量泄漏集合和电磁泄漏集合分别包含相同数目的泄漏信号，且每条信号有882个样本点，对应于敏感中间值的泄漏点不在同一个时间点上。图 3.6(a) 显示了所有多信道融合攻击算法及单信道攻击对有保护的AES-128实现成功实施二阶攻击所需的泄漏信号数目。为了对比，我们在上一步预处理后得到的两个侧信道的泄漏集合上，模拟产生了两个新的能量泄漏集合和电磁泄漏集合，其中每条泄漏信号内有990个样本点，且敏感中间值对应的能量和电磁泄漏多个泄漏点，时间轴上有所重合。图 3.6(b) 显示了所有多信道融合攻击算法及单信道攻击成功所需的泄漏信号数目。

从这两个实验可以看出，本章所提出的融合攻击方法性能优于对比方法。不过，从图 3.6 可以看出，SVD_FA算法和GSVD_FA算法的表现与图 3.3 中差别很大。寻其原因，在于尽管图 3.6(a) 中预处理后的两个侧信息泄漏集合只包含了一个与敏感中间值相关的泄漏特征点，但它们的长度较短，使得与秘密信息相关的泄漏信息能被少量的特征刻画，使用SVD找到的密钥泄漏特征集KLFS能被用来实施成功的攻击。但是，利用GSVD提取的联合特征却包含了大量冗余信息，且只包含少量的与敏感中间值相关的泄漏信息。图 3.6(a) 中SVD_FA 算法提取到的KLFS都是两个泄漏集合的第9个左奇异向量，而在图 3.6(b) 中提取到的KLFS则分别是能量泄漏集合的第7个左奇异向量和电磁泄漏集合的第8个左奇异向量。图 3.6(a) 上WBI_FA算法中分配给能量通道和电磁通道的权重分别是0.465及0.545，图 3.6(b) 中分配给能量通道和电磁通道的权重分别变成0.535和0.465。NMFCCM_FA算法中的参数λ总是置为0.05。

综上所述，当对一个被掩码保护的密码算法实现使用多信道融合攻击时，与单信道攻击一样，需先分别对该实现不同信道的侧信息泄漏进行预处理得到新的泄漏集合。如果预处理后不同信道的依赖于密钥的泄漏特征点不在同一时刻发生，我们依次推荐特征级、决策级和数据级融合攻击算法。如果预处理后不同信道的与敏感中间值相关的泄漏点在同一时刻发生，则优先推荐使用了第一种融合方式的特征级融合攻击算法，其次推荐数据级融合攻击算法，最后推荐决策级融合攻击算法。在后两种融合攻击算法中，我们更青睐使用利用了所有信道联合信息（即采用了第二种融合方式）的算法，如NMFRL_FA和NMFCCM_FA算法，并不推荐使用诸如GSVD_FA之类的采用了第二种融合方式的特征级融合攻击算法。因为这类融合攻击算法提取的各个信道的联合特征可能引入了过多冗余且仅包含极少的对攻击有用的泄漏信息。除此之外，并



(a) 单个泄漏点情形



(b) 多个泄漏点情形

图 3.6　CPA、CEMA及MCFAs对有保护的AES-128实现成功实施二阶攻击所需的泄漏信号数目

没有充足的证据反映出此场景下不同融合方式对数据级融合攻击算法和决策级融合攻击算法有重大影响。进一步地，如果攻击者对一个密码实现了解较少，并不确定该密码实现中的敏感中间值对应的不同侧信道泄漏是否同一时刻发生，此时建议使用决策级融合攻击算法。此类算法总能给出一个不错的结果。不过需要注意的是，所使用的决策级融合攻击算法应尽可能地利用不同参数来体现不同信道对融合攻击的贡献，如NMFCCM_FA和WBI_FA算法一样，而尽量不要像Sum_FA、Pro_FA或Max_FA算法一样，只是简单地对所有信道“一视同仁”或只选最好的侧信道分析结果。

另外，我们同样研究了只包含密码算法实现的一部分秘密信息的多个信道的融合攻击。我们针对第 3.3.1 节中的无保护AES-128 的FPGA实现，使用同样的示波器及配置参数，并同时将两个直径1mm H场探针分别垂直放置在FPGA芯片不同位置，测量了该无保护AES-128的FPGA实现运行中的部分秘密信息的电磁泄漏。表 3.1 则给出

表 3.1　CEMA1、CEMA2及MCFAs算法所恢复的S盒编号

#Traces	10,000	15,000	20,000	25,000	27,000	28,000
CEMA1	2,12,11,14	2,6,8, 11,12,14	2,8, 11,12,14	2,6, 11,12,14	2,6,11, 12,13,14	2,6,11, 12,13,14
CEMA2	12,14	11,12,14	2,8, 11,12,14	2,8, 11,12,14	2,8, 11,12,14	2,8, 11,12,14
CFA	no	11,12	6,11,12,14	6,11,12,14	6,8, 11,12,14	6,8, 11,12,14
SFA	11,12,15	2,11, 12,14,15	2,6,8, 11,12,14,15	2,6,11, 12,14,15	2,6,8, 11,12,14,15	2,6,8, 11,12,14,15
NMFRL_FA	8,11, 12,14,15	8,11, 12,14,15	2,8,11, 12,14,15	2,8,11, 12,14,15	2,8,11, 12,14,15	2,8,11, 12,14,15
SVD_FA	2,8,9,10, 11,12,14,15	2,6,8, 9,10,11, 12,14,15	2,6,8, 9,10,11, 12,14,15	1,2,6, 8,9,10 ,11,12,14,15	1,2,6, 8,9,10,11, 12,13,14,15	1,2,6, 8,9,10,11, 12,13,14,15
GSVD_FA	2,12,14	2,11,12,14	1,2,11, 12,13,14,15	1,2,11, 12,13,14,15	1,2,5,11, 12,13,14,15	1,2,5, 7,11,12, 13,14,15
Sum_FA	2,8,12,14	2,6,8, 11,12,14	2,6,8, 11,12,14	2,8, 11,12,14	2,8, 11,12,14	2,8, 11,12,14
Pro_FA	2,8,12,14	2,6,8, 11,12,14	2,6,8, 11,12,14	2,8, 11,12,14	2,8, 11,12,14	2,8, 11,12,14
Max_FA	2,11,12,14	2,6,8, 11,12,14	2,6,8, 11,12,14	2,11,12,14	2,6,8, 11,12,13,14	2,8,11, 12,13,14
WBI_FA	2,8, 11,12,14	2,6,8, 11,12,14	2,6,8, 11,12,14	2,6,11, 12,13,14	2,6,11, 12,13,14	2,6,8, 11,12,13,14
NMFCCM_FA	2,6, 11,12,14	6,8, 11,12,14	2,6,11, 12,14,15	2,6,11, 12,14,15	2,6,11, 12,14,15	2,6,8, 11,12,14,15

了随着泄漏信号数目增加，被两个单信道电磁攻击（分别记为CEMA1、CEMA2）及各MCFAs算法所恢复的S盒编号。图 3.7 展示了随着泄漏信号数目增加，被CEMA1、CEMA2及MCFAs算法所恢复的S盒数目的变化曲线。该实验表明多信道融合攻击在联合只包含一部分秘密信息的侧信道泄漏时的表现与联合包含全部秘密信息的侧信道泄漏时的表现类似，说明了高效的多信道融合攻击优于单信道攻击的原因在于前者在联合各个信道时提高了侧信息利用率，而这些侧信息却不能被单个侧信道攻击所利用。

3.3.4　讨论

为了更好地比较MCFAs与单信道攻击在实际资源利用效率上的差别，下面将分别考察MCFAs和使用双倍泄漏信号数目的单信道攻击的运行时间及所占用内存大小。此外，我们还将从经验攻击的角度，探讨不同采样率对侧信道攻击效率的影响。

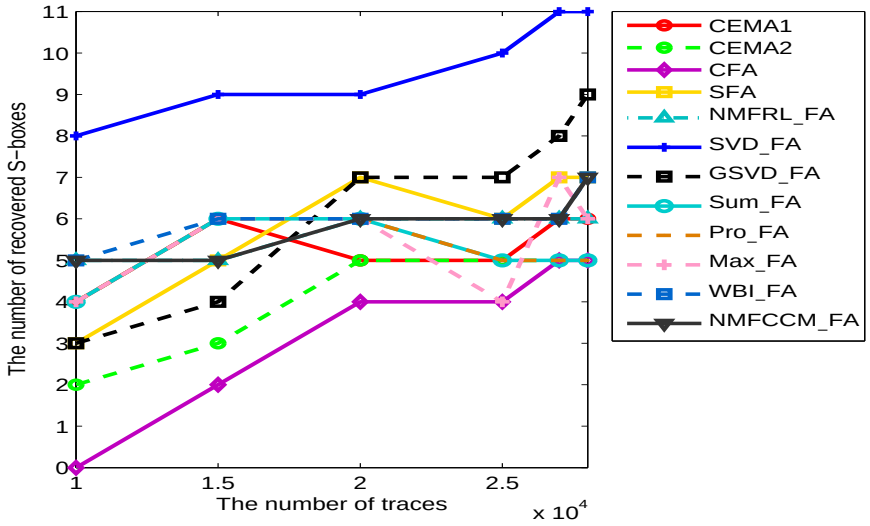


图 3.7　CEMA1、CEMA2及MCFAs算法所恢复的S盒数目对比

3.3.4.1　多信道融合攻击方法和单信道攻击的运行时间及所占内存对比

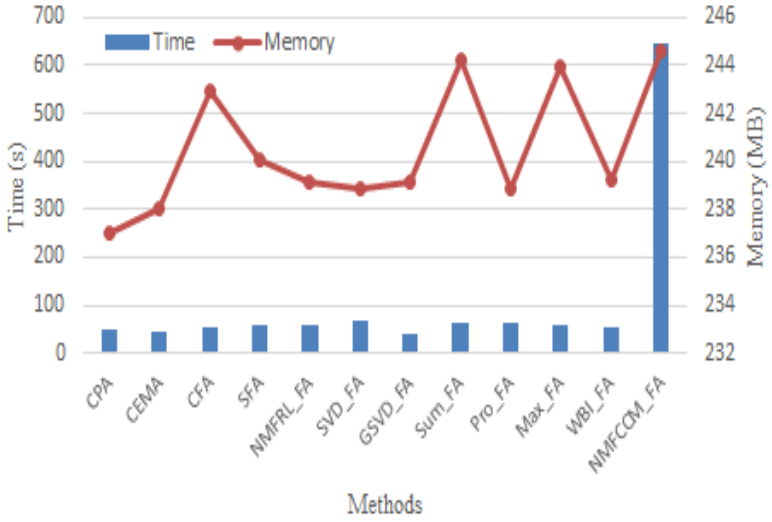
图 3.8 提供了多信道融合攻击方法和使用双倍泄漏信号数目的单信道攻击的运行时间，以及所占用内存大小对比曲线。攻击所用的泄漏信号取自第 3.3.1 小节中采集的无保护AES-128软件实现（即8-bit MCU实现）和硬件实现（即FPGA实现）的泄漏数据。

从图 3.8 上可以看出，整体上多信道融合攻击方法和使用双倍泄漏信号数目的单信道攻击的运行时间及所占用内存差别很小。不过图 3.8(a) 中NMFCCM_FA算法和图 3.8(b) 中GSVD_FA算法的运行时间都超出别的算法很多。这是因为无保护AES-128的软件实现的泄漏信号包含的采样点数较多，所组成的数据矩阵较大，且NMFCCM_FA算法中用到的NMF算法需要遍历所有子密钥候选值的相关系数矩阵，使得该融合攻击算法整体运行时间大大增加。而无保护AES-128的硬件实现的泄漏信号数目比软件实现超出更多，这严重削弱了依赖将能量泄漏和电磁泄漏信号串联后进行GSVD提取联合泄漏特征的GSVD_FA算法的效率。

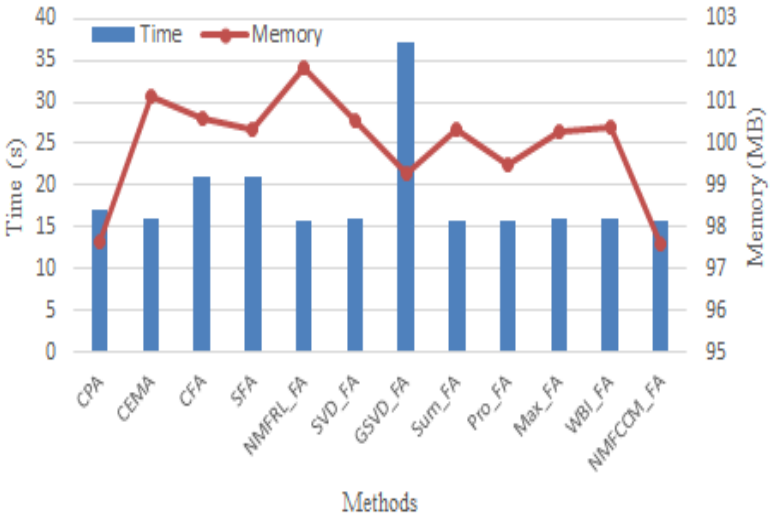
另外从表 3.2 中可以发现，本章所提方法攻击AES-128的硬件实现时需要泄漏信号数目少于简单地使用双倍泄漏信号数目的单信道攻击，亦即前者效率高于后者。相比之下，以前文献所提出的多信道融合攻击算法提升的效率要低于简单地使用双倍泄漏信号数目的单信道攻击。但是由于AES-128软件实现的泄漏信号中对攻击有用的泄漏特征点数远少于AES-128硬件实现泄漏信号包含的泄漏点数，在攻击AES-128 的软件实现时，所有多信道融合攻击算法提升的效率都低于简单地使用双倍泄漏信号数目的单信道攻击。然而在此情形下，如果实际中可获取的单信道侧信息泄漏量受限，多信道融合攻击算法依然有效，因为相对利用同等泄漏信号数目的单信道攻击而言，它们能通过同时联合多个单信道来提高侧信息利用率，从而提高侧信道分析效率。

3.3.4.2　采样率对攻击效率的影响

本小节将从经验攻击的角度出发探讨不同采样率对侧信道攻击效率的影响。由于



(a) CPA、CEMA及MCFAs攻击无保护AES-128的8-bit MCU实现运行时间及所占内存（200条能量迹，200电磁迹，或100条能量迹+100条电磁迹）



(b) CPA、CEMA及MCFAs攻击无保护AES-128的FPGA实现运行时间及所占内存（10,000条能量迹，10,000电磁迹，或5,000能量迹+5,000条电磁迹）

图 3.8　CPA、CEMA及MCFAs攻击无保护AES-128 MCU实现及FPGA实现运行时间及所占内存

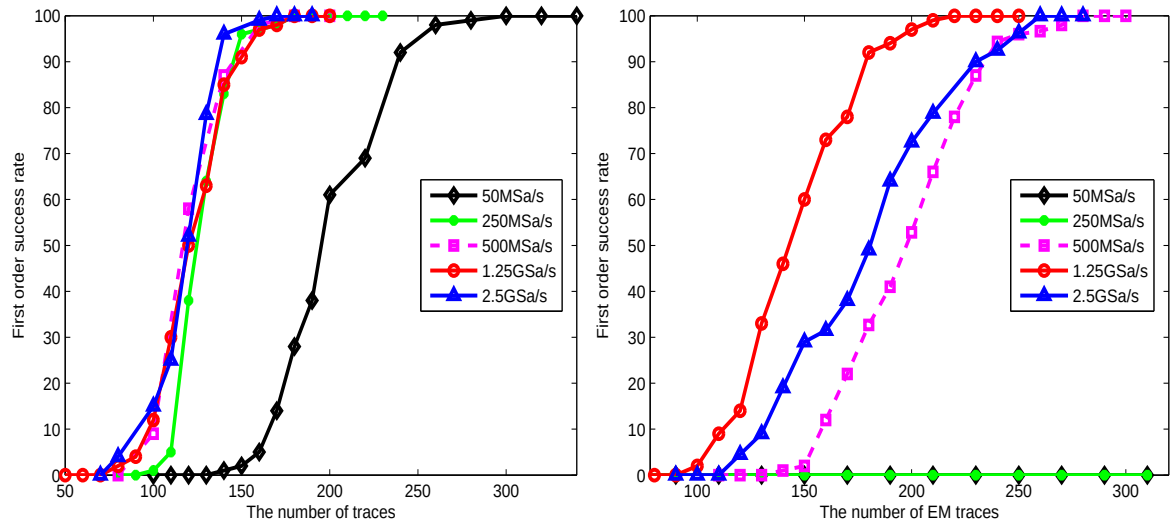
同时采集多个通道的泄漏信号时示波器一般只能使用同一个采样率，为了减少实验代价，本文使用同一台示波器同时采集密码芯片的能量泄漏和电磁泄漏。理论上，如果对一个信号以大于或等于奈奎斯特频率的采样率采样，该信号就能被其采样信号完美重构。从经验上看，密码芯片的能量泄漏和电磁泄漏的奈奎斯特频率往往是不同的，而且后者常常大于前者。如果示波器的采样率设置过高，则对密码芯片的能量泄漏信号而言，过采样并不会显著增加能量攻击的效率，反因样本点过多而增加计算时间和资源。与之相反，若示波器的采样率设置过低，则对密码芯片的电磁泄漏信号而言，欠采样会削弱电磁攻击的效率。但若示波器的采样率设置在密码芯片的能量泄漏信号

表 3.2　一阶成功率达到100%时CPA、CEMA及MCFAs攻击所需的泄漏信号数目

	#Traces	
Methods	MCU	FPGA
CPA	180	9,000
CEMA	220	9,400
CFA	250	4,800
SFA	160	2,600
NMFRL_FA	170	3,800
SVD_FA	\	2,100
GSVD_FA	\	3,600
Sum_FA	160	5,000
Pro_FA	160	5,000
Max_FA	170	7,700
WBI_FA	140	4,400
NMFCCM_FA	130	4,700

和电磁泄漏信号的奈奎斯特频率之间的一个合适位置，过采样对能量通道以及欠采样对电磁通道的影响将会处在一个可以容忍的范围内。

图 3.9 经验性地给出了不同采样率条件下，针对无保护AES-128的8-bit MCU实现的CPA攻击及CEMA攻击的一阶成功率的变化曲线。从图上可以发现不同采样率下CPA攻击的结果比较接近。最好的CPA结果由针对使用采样率2.5GSa/s采集到的泄漏信号攻击而获得，其所用能量迹数目为170时，一阶成功率便达到了100%。不过这也稍稍比其它三个采样率下的CPA攻击达到100%成功率所需要的能量迹数目180条好一些。图 3.9(a) 的攻击结果较契合上面的理论分析。



(a) 不同采样率条件下CPA攻击成功率　　(b) 不同采样率条件下CEMA攻击成功率

图 3.9　不同采样率条件下针对无保护AES-128的8-bit MCU实现的CPA攻击及CEMA攻击的一阶成功率

然而在图 3.9(b) 中，不同采样率下CEMA攻击的结果却变化较大。其中，在采样率达到2.5GSa/s之前，CEMA的成功率随着采样率增大而提高。但在采样率为2.5GSa/s的条件下，CEMA的结果甚至还不如在采样率为1.25GSa/s下的结果。这似乎与上述分析矛盾。寻其原因，在于所有采样率中，1.25GSa/s应该最接近电磁泄漏信号中可用于攻击的那部分信号的奈奎斯特频率，低于电磁泄漏信号奈奎斯特频率的采样率会削弱CEMA的攻击效率。此外，我们所采集到的密码芯片的电磁泄漏信号包含的不仅仅只有可用于攻击的泄漏信号，同时也夹杂了大量别的成分，尤其是时钟信号。时钟信号构成了密码芯片的电磁泄漏信号的主要部分，远远比可用于攻击的泄漏信号显著 [150]。时钟信号的存在对电磁攻击造成了负面影响，使得其效率低于能量攻击，且其影响在采样率从1.25GSa/s增加到2.5GSa/s时变得显著。所以本章实验中，使用1.25GSa/s的采样率同时采集密码芯片的能量泄漏和电磁泄漏。此外，另一个使用同一采样率的原因是，我们希望在同一泄漏集合下对比本章提出的两个数据级融合攻击算法，一个特征级融合攻击算法GSVD_FA，一个决策级融合攻击算法NMFCCM_FA以及其它多信道融合攻击算法的性能。

3.3.5 算法扩展

本章所提出的多信道融合攻击算法可以拓展到以下四种情形：

3.3.5.1 信道个数多于2的一阶多信道融合攻击

除GSVD_FA算法外，本章提出的所有MCFAs都能直接用于信道个数多于2的一阶多信道融合攻击。在这种情形下，GSVD_FA算法可以推广为基于高阶奇异值分解（如张量分解）的多信道融合攻击算法，但此时算法的计算复杂度可能会增长得很快。

3.3.5.2 高阶多信道融合攻击

在分别对各个信道的侧信息泄漏进行预处理，得到高阶攻击所需的预处理泄漏信号集合之后，本章提出的所有MCFAs都能直接用于高阶多信道融合攻击。不过，GSVD_FA算法可能会表现不佳，因为该算法通过GSVD提取的各信道侧信息泄漏联合特征可能会引入较多冗余信息，且包含较少可用于攻击的泄漏信息。

3.3.5.3 单信道具有非线性泄漏

当待联合的单信道泄漏是非线性泄漏，即式子 3-1 中$l(x,k)$与$f(Z(x,k))$之间的关系不是线性的，相关分析的攻击效率可能会降低，但可用其它的可度量两个随机变量间非线性关系的统计工具（如互信息分析 [84,96,151–155]）来代替。

3.3.5.4 各个信道泄漏信号采集参数配置不同

此时，待联合的各个侧信道泄漏信号采集参数配置（如采样率）各不相同。每条泄漏信号所包含样本点不同，使得本章提出的两个数据级融合攻击算法，一个特征级融合攻击算法GSVD_FA及一个决策级融合攻击算法NMFCCM_FA不能使用。但是，这

个问题可以通过对采样点较少的单通道泄漏信号插值 [32,149,156,157]，或对采样点较多的单通道泄漏信号压缩 [10,90,91,158]来解决。而本章所提出的另一种特征级融合攻击算法SVD_FA及另一种决策级融合攻击算法WBI_FA算法依然有效。

3.4　多信道融合度量标准

以上章节讲述的都是关于多信道融合攻击算法的内容，但在实施多信道融合攻击前，首先需要分析者判断不同侧信道是否适宜联合发动攻击。在现有研究中，文献[15]提出了一个判断两个侧信道是否可以联合的度量标准——OSNR（Output Signal to Noise Ratio）。文献 [78]则提出了另一个度量标准——PC (Possibility of Combination)。这两个度量标准的计算都需要分析者事先知道密钥，实际可操作性较差。本小节我们构造了一个无需知道密钥信息的基于偏相关分析的度量标准。下面将讲述其构造原理。

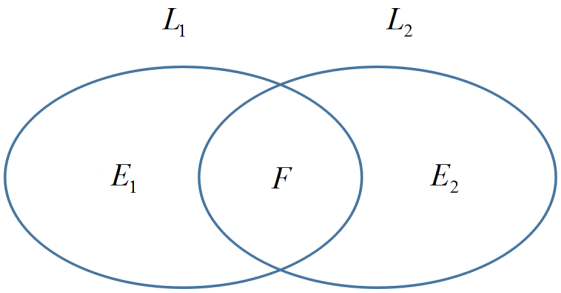
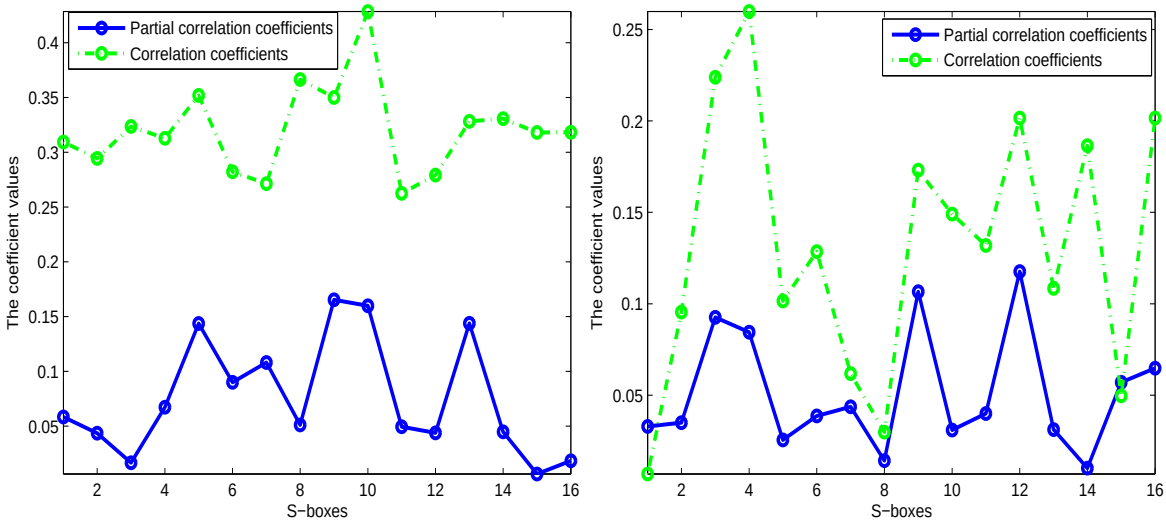


图 3.10　同一敏感中间值的两个不同侧信道泄漏关系的文氏图表达

假设从两个侧信道采集到的某个密码芯片的包含秘密信息的泄漏信号集合分别为L_1和L_2。显然L_1和L_2之间应该有一个依赖于密钥的交集部分F，如图 3.10 所示。这两个侧信道越适宜联合，交集F就应该越大，L_1与L_2之间的相关性就越大。这时，L_1与L_2分别除去共有部分F得到的E_1和E_2，应该是不相关的信号，诸如不同侧信道的电子噪声等等。相反地，如果这两个侧信道越不适宜联合，交集F就应该越小，L_1 与L_2之间的相关性就越小，E_1和E_2依然不相关。综合以上两种情形，L_1与L_2之间的关系可以使用净相关，即一阶偏相关 [159]来刻画。L_1与L_2的一阶偏相关刻画了去掉它们的共有部分F的影响后二者的相关显著程度。在此基础上，我们可以构造一个判断两个侧信道是否适宜联合的度量标准。如前所述，如果这两个侧信道越适宜联合，L_1与L_2之间的相关性就越大，去掉F后二者的相关性就越小，即L_1与L_2 的一阶偏相关系数值越大；如果这两个单信道越不适宜联合，L_1与L_2 之间的相关性就越小，去掉F后二者的相关性依然小，即L_1与L_2的一阶偏相关系数值越小。

为了验证以上观点，我们分别从第 3.3.1 小节采集到的无保护AES-128的8-bit MCU实现的泄漏信号集合中选择300条能量迹和相应的300条电磁迹，并分别使用L_1和L_2表示这两个泄漏信号集合。第 3.3.2 小节的攻击结果表明这两个通道泄漏信号是可以融合的。图 3.11(a) 画出了两个侧信道的泄漏集合L_1及L_2的16个S盒泄漏之间



(a) 适合联合的两个信道的泄漏集合L_1及L_2的相关系数及偏相关系数值（300条能量迹+300条电磁迹）

(b) 不适合联合的两个信道的泄漏集合L_1及L_3的相关系数及偏相关系数值（300条能量迹+300条电磁迹）

图 3.11　侧信道泄漏集合L_1与L_2及L_1与L_3的16个S盒泄漏之间的相关系数及偏相关系数值对比

的相关系数及偏相关系数值。而图 3.11(b) 则显示了能量迹集合L_1及另一个新的不包含秘密信息泄漏的电磁迹集合（标记为L_3）的16个S盒泄漏之间的相关系数及偏相关系数值。可以观察到，L_1及L_2的16个S盒泄漏之间的相关系数及偏相关系数值的差别要显著大于L_1与L_3的16个S盒泄漏之间的相关系数及偏相关系数值的差别。该结果有力地支持了我们的观点。

根据以上认识，我们可以将两个侧信道的泄漏集合L_1及L_2之间的相关系数及偏相关系数值的差值定义为一个度量标准，来确定这两个信道是否适宜联合以发动融合攻击。定义如下：

$$FM = |\rho(L_1, L_2) - \rho(L_1 L_2|F)|, \tag{3-37}$$

其中

$$\rho(L_1 L_2|F) = \frac{\rho(L_1, L_2) - \rho(L_1, F)\rho(L_2, F)}{\sqrt{1-\rho(L_1, F)^2}\sqrt{1-\rho(L_2, F)^2}},$$

并且$\rho(L_1, L_2)$表示对L_1中泄漏点与L_2中泄漏点求相关系数。注意，这里的泄漏点指的是对应于所有密钥候选值中最大相关系数所在时刻的采样点。FM刻画了L_1及L_2之间的相关系数及偏相关系数值的差别程度。如果FM总是取值很大，则泄漏L_1及L_2对应的两个信道适宜联合。否则，不推荐联合这两个信道实施融合攻击。

该融合标准不需要知道能量迹或电磁迹中依赖于密钥的泄漏特征点发生的时刻，也不需要使用密钥来刻画。若两个侧信道适于联合实施攻击，当泄漏信号的数目小的不足以实施一个成功的攻击时，所有密钥候选值的最大相关系数区分度不大且随机性

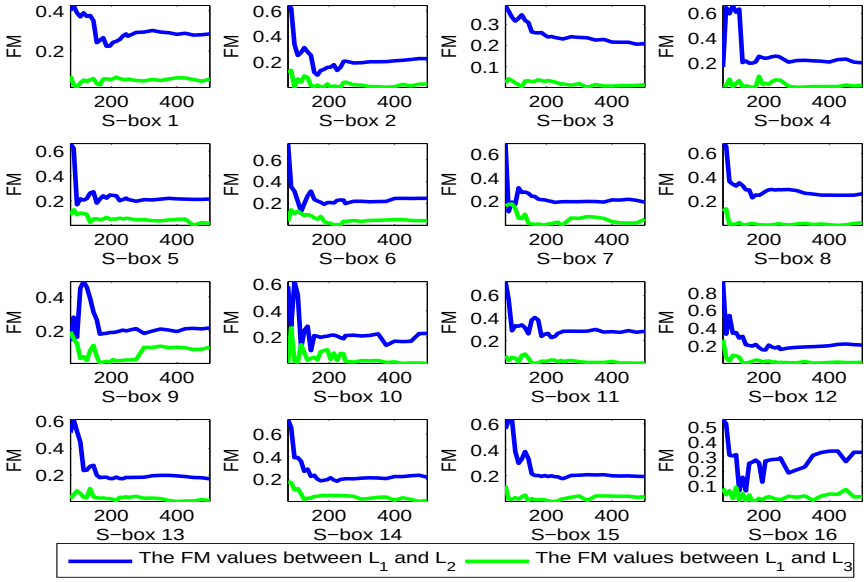


图 3.12　侧信道泄漏集合L_1与L_2及L_1与L_3的16个S盒泄漏之间的FM值对比

很强，对应于所有密钥候选值中最大相关系数所在时刻的泄漏点往往不包含密钥信息，所以L_1及L_2之间泄漏点的相关性及偏相关性都很小，FM的值相对较大。随着泄漏信号的数目的增加，依赖于密钥的泄漏特征点逐渐凸显，然后L_1及L_2之间泄漏点的相关系数及偏相关系数值的差别程度越来越明显，FM值也随之变大。若两个侧信道不适于联合实施攻击，则在上述两种情形下，FM的值总是很小。

图 3.12 分别显示了采集自不同侧信道的泄漏集合L_1及L_2的16个S盒泄漏之间的FM值（蓝线），以及采集自不同侧信道的泄漏集合L_1及L_3的16个S盒泄漏之间的FM值（绿线），随泄漏信号数目（图形横轴）增长的曲线图。可以看出L_1适合与L_2融合，而不适合与L_3 融合。这与前面的实验一致。当然，我们需要选择一个FM的经验阈值来进行判断两个信道是否适合联合。因为图 3.11 中的相关系数及偏相关系数值都较小，所以我们认为FM超过0.1就说明相关系数与偏相关系数之间差异显著，故在图 3.12 中，FM的判别阈值设为0.15。如果图 3.12 上一个子图中超过90%的FM值都大于0.15，就说明相关系数与偏相关系数之间差异显著，两个对应的S盒泄漏适合融合。否则，不推荐融合它们。不过这样选择FM的阈值需要较多经验，我们还可以取FM值的四分位点或八分位点进行判别。

进一步地，如果判断数目多于两个的侧信道是否适宜实施联合攻击，既可以对侧信道两两之间分别计算FM值判断后，再以一个侧信道为标准判断其它侧信道是否可以与此参考信道联合，也可以直接将FM计算公式中的一阶偏相关分析拓展至高阶偏相关分析上来计算并判断 [159]。

3.5　本章小结

本章系统研究了多信道融合攻击，将多信道融合攻击分为三类，统一了多信道融

合攻击研究框架，并提出了六种多信道融合攻击方法。这六种方法包括两种数据级、两种特征级及两种决策级融合攻击方法，涵盖了两类融合方式，效率总体优于现有多信道融合攻击方法及单信道攻击。通过本章的研究，我们能够针对不同密码实现，为多信道融合攻击提供建议。例如，如果在一个密码实现的不同侧信道的侧信息泄漏中，对应于同一敏感中间值的泄漏点较少且在时域上不同时发生，则适合使用数据级及决策级融合攻击方法；如果对应于该敏感中间值的不同侧信道的泄漏点较多且在时域上多有重合，则推荐特征级融合攻击方法；而决策级融合攻击方法在任何情况下都可以取得不错的表现。此外，本章提出了基于偏相关分析的多信道泄漏融合判别标准，以在实施融合攻击前判断不同侧信道是否适宜联合。本章的研究说明，一个恰当实施的多信道融合攻击通过提高密码芯片信息泄漏利用率来获得高于单信道攻击的效率，从而可为密码芯片侧信道安全性提供了更加全面、深刻地分析。本章工作推进了多信道融合攻击及侧信道分析技术的研究。在以后的研究中，我们将重点考虑如何联合采样率不同及泄漏函数未知的多个侧信道来进行融合攻击。这将有利于进一步推动密码芯片侧信道分析技术的发展。

第四章　泄漏评估与泄漏检测

本章将从通信信道理论的角度出发，开展有关泄漏评估与泄漏检测技术的研究。

为了结合参数类估计方法和非参数类估计方法的优点，本章将侧信道视为一个通信信道，并将通信信道的平均互信息作为密码芯片的侧信息泄漏量 [160]，然后从估计泄漏信号噪声分布入手，绕过对密码芯片侧信息泄漏分布的直接估计，完成针对密码芯片的泄漏评估。此外，该通信信道的信道容量提供了密码芯片泄漏量的一个上界，可粗略估计最坏场景下密码芯片可能的侧信息泄漏量。

另外，本章在侧信道通信信道模型的基础上，结合统计中的一致性检验知识，发展出了一种侧信道泄漏检测技术 [160]。侧信道泄漏检测的目标是找到密码芯片侧信道泄漏信号中可能的依赖于秘密信息的泄漏样本点。如果被检测出的泄漏样本点确实包含与秘密信息有关的泄漏，则可被用于侧信道攻击。此时这些泄漏样本点被称为POIs [17]。一个好的泄漏检测方法应尽可能多地检测出POIs，且尽可能少地检测出对攻击无用的泄漏样本点 [17]。本章所提方法属于基于统计的检测技术，不但对泄漏信号的采集没有特殊要求，而且找到的泄漏特征点基本属于POIs，能直接用来发动CPA攻击。下面详细介绍本章内容。

4.1　预备知识

在介绍泄漏评估技术与泄漏检测技术之前，首先简要介绍一些相关知识。

4.1.1　符号记法

本章使用大写字母标记随机变量，使用对应的小写字母标记随机变量的样本。例如，假设存在一个离散随机变量X，则该随机变量所有可能的K个样本值可以写成$x = \{x_k\}$。如果使用符号$Pr(\cdot)$ 标记一个离散随机变量取某个样本值的概率，则X第k个样本值$\{x_k\}$发生的概率可用符号$\{p_k = Pr(x_k)\}$ 表示。相似地，我们使用符号$p(\cdot)$表示一个连续随机变量的概率密度分布函数。

4.1.2　有限混合模型、高斯混合模型及最大期望算法

假设一个L维的连续随机变量Y的样本为y，则K元有限混合模型（Finite Mixture Model，简写为FMM） [161]的定义为

$$\begin{aligned} p(y|\Theta) &= \sum_{k=1}^{K} \alpha_k p_k(x|\theta_k), \\ s.t.\ 0 \le \alpha_k \le 1,\ &\sum_{k=1}^{K} \alpha_k = 1\ . \end{aligned} \tag{4-1}$$

式 4-1 中，$\Theta = (\alpha_1, \alpha_2, \ldots, \alpha_K; \theta_1, \theta_2, \ldots, \theta_K)$表示该有限混合模型的参数集，$p_k(x|\theta_k)$表示该模型第$k$个成分的概率密度函数。

从式 4-1可以看出，一个有限混合模型是一些概率密度函数的凸组合。当式 4-1中的K个成分都服从高斯分布时，式中的FMM也被称为高斯混合模型（Gaussian Mixture Model, 简写为GMM）。GMM是最常用的FMM [162]。FMM（包含GMM）是一种强大且灵活的统计建模工具，能够通过调整组成成分的数目K，来以任意精度逼近任何分布，常用于处理分布形式复杂的数据 [162,163]。实际中应用FMM逼近一个分布，最需要考虑的是参数估计问题，也即式 4-1中参数集合Θ的估计问题 [163]。该参数估计问题已经有大量成熟的解法，如期望最大化算法 [164]。

期望最大化算法是一种广泛应用的参数估计算法，常用来估计含有不完整数据或包含未被观察到的隐藏变量的模型的参数。该算法通过寻找模型参数的最大似然估计或最大后验估计来求解模型参数 [164]。期望最大化算法是一种迭代算法，每次迭代都包含两个步骤，即求期望（The Expectation Step, 简写为E-step)和最大化期望（The Maximization Step, 简写为M-step）。该算法首先需要给出所求模型参数的一个初始估计，然后在E-step中，通过使用此时模型的参数估计和观测数据，求出含有隐藏变量的完整数据的对数似然函数的条件期望；再在M-step中，将上一E-step中计算得到的对数似然函数的条件期望最大化，随后更新模型参数的估计值，继续下一个E-step，如此循环，直至算法收敛或达到停止条件为止。因为期望最大化算法每次迭代都会使得似然函数值增加，所以该算法总是能够保证在有限次迭代中收敛。如果所估计模型有n个样本，则使用期望最大化算法估计GMM参数的计算复杂度为$O(Ln + Kn^2)$。

4.2 基于通信信道理论的侧信道泄漏评估算法

为了更好地研究密码芯片泄漏评估问题，这里借鉴通信信道理论来计算密码芯片侧信息泄漏量。使用发展已经很成熟的通信信道理论研究侧信道泄漏评估技术，能够给后者提供一个坚实的理论支撑，更有利于指导实践。

4.2.1 侧信道的通信信道模型

假设s^*为一个密码算法实现所使用密钥的一部分（即子密钥），T为明文或密文的一部分。若将密码运算过程中与s^*和T相关的一个敏感中间变量表示为$f(T, s^*)$（f 指算法运算中某一操作函数），且将该变量对应的某种类型的真实泄漏*记为X，实际测量泄漏记为Y，那么有

$$Y = X + E = \psi(f(T, s^*)) + E, \tag{4-2}$$

其中，ψ表示依赖于密码芯片的泄漏模型，E表示独立于X的零均值噪声项。一般说来，

* 本章“真实泄漏”指由准确的密码芯片泄漏模型计算出的中间变量泄漏，与实际测量泄漏相比，不包含噪声。

s^*和T是离散变量，故$f(T, s^*)$也是离散变量，对应的X同样是离散随机变量。不过因为噪声E常常是连续随机变量，所以X与E的和Y也是一个连续随机变量。

如果将变量X看作信源，变量Y看作信宿 [165]，那么该侧信道可以看作一个通信信道（图 4.1）。此时，该侧信道侧信息泄漏量$I(X, Y)$*就是上述通信信道的平均互信息。更进一步地，因为在通信信道中，信道平均互信息的最大值是信道容量 [165]，所以，上述通信信道的信道容量提供了该密码芯片在该侧信道的信息泄漏的一个上界。

假设图 4.1 中通信信道的输入X总共存在K个可能的值，且这K个样本值为$x = \{x_k\}$, $\{p_k = Pr(x_k)\}$, $k = 1, \ldots, K$。将样本x中的第k个值x_k输入通信信道后，会得到一个输出$y = \{x_k\} + e$。其中，y, e分别表示连续随机变量Y和E的样本。那么有

$$p(y) = \sum_{k=1}^{K} p(y, x_k), \tag{4-3}$$

其中，

$$p(y, x_k) = p(y|x_k)p_k \ . \tag{4-4}$$

概率密度函数$p(y|x)$表示该通信信道的信道转移概率，刻画了该信道的特性。综上可以发现，利用通信信道来计算密码芯片的侧信息泄漏量，只需计算该通信信道的平均互信息即可，不必了解密码算法实现的敏感中间变量的值及泄漏模型。

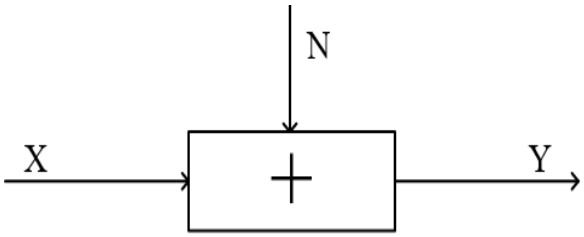


图 4.1　侧信道的通信信道模型

4.2.2　高斯加性信道

如果式子 4-2 中，噪声E服从均值为0、方差为σ^2的高斯分布，则式 4-3 中概率密度函数$p(y)$将会是一个一维GMM。此时图 4.1 中的通信信道是一个高斯加性信道。我们可以通过计算该高斯加性信道的平均互信息及信道容量，来分别得出密码芯片的侧信息泄漏量及泄漏量的上界。

4.2.2.1　高斯加性信道的平均互信息

由于噪声E方差为σ^2，式 4-3 可写成：

$$p(y|x_k) = p(n)|_{n=y-x_k} = \frac{1}{\sqrt{2\pi}\sigma} exp(-\frac{(y - x_k)^2}{2\sigma^2}) \ . \tag{4-5}$$

* 除非特别声明，本章中所讲的一个密码芯片在某一侧信道的侧信息泄漏量，总是表示实现在该芯片上的密码算法运算中的某一敏感中间变量对应的一个泄漏点所包含的信息泄漏量。

此时，$p(y)$是一个一维GMM，其表达式为：

$$p(y) = \sum_{k=1}^{K} p(y|x_k)p_k = \sum_{k=1}^{K} p_k \frac{1}{\sqrt{2\pi}\sigma} exp(-\frac{(y-x_k)^2}{2\sigma^2}) . \tag{4-6}$$

若我们已经得到通信信道输出的一系列观察值$\{y_1, \ldots, y_N\}$，则上述高斯混合模型的未知参数集合为

$$\{x_1, \ldots, x_k, p_1, \ldots, p_k; \sigma\} .$$

如前所述，这些未知参数可通过期望最大化算法 [164]估计出来。求解中需将似然函数$\prod_{n=1}^{N} p(y_n)$作为目标函数，并使目标函数最大化。由于似然函数$\prod_{n=1}^{N} p(y_n)$最大化等价于对数似然函数$\sum_{n=1}^{N} \log(p(y_n))$最大化，为了计算方便，我们使用后者作为目标函数。对数似然函数的完整表达形式如下：

$$\sum_{n=1}^{N} \log(p(y_n)) = \sum_{n=1}^{N} \log \left\{ \sum_{k=1}^{K} p_k \frac{exp(-\frac{(y_n-x_k)^2}{2\sigma^2})}{\sqrt{2\pi}\sigma} \right\} . \tag{4-7}$$

首先对式 4-7 中的每个参数分别求微分，然后令微分为0并求解方程，得到期望最大化算法的E-step，即

$$\hat{\gamma}_{nk}^{(t)} = \frac{p(y_n|x_k)p_k}{\sum_{k=1}^{K} p(y_n|x_k)p_k}, \tag{4-8}$$

然后求得期望最大化算法的M-step为

$$\begin{aligned} \hat{x}_k^{(t+1)} &= \frac{\sum_{n=1}^{N} \hat{\gamma}_{nk}^{(t)} y_n}{\sum_{n=1}^{N} \hat{\gamma}_{nk}^{(t)}}, \\ \hat{p}_k^{(t+1)} &= \frac{1}{N} \sum_{n=1}^{N} \hat{\gamma}_{nk}^{(t)}, \\ \hat{\sigma}^{(t+1)} &= \left\{ \frac{1}{N} \sum_{n=1}^{N} \sum_{k=1}^{K} \hat{\gamma}_{nk}^{(t)} (y_n - x_k)^2 \right\}^{1/2} . \end{aligned} \tag{4-9}$$

式 4-8 和式 4-9 中的$n = 1, \ldots, N, k = 1, \ldots, K$, $\hat{\cdot}$表示一个参数的估计值，t表示第t次迭代，γ_{nk}表示观察值y_n由该GMM中第k个成分产生的概率。当对数似然函数值收敛时，迭代终止。

在该GMM中所有未知参数被估计出来以后，即可计算高斯加性信道的平均互信息。高斯加性信道的平均互信息表达形式如下：

$$I(X,Y) = H(Y) - H(Y|X) = H(Y) - H(N) . \tag{4-10}$$

式 4-10 中符号$H(\cdot)$表示一个随机变量的香农熵。然而，即使估计出了所有未知参数，上式依然难以计算。原因在于$H(Y)$的表达式中含有指数函数的对数和及积分运算，一

般情况下无法得到$H(Y)$的闭式解 [166]。但我们可以使用一些别的措施求出$H(Y)$的近似解。例如，我们可以利用样本值$y_1,\ldots,y_N$来估计$H(Y)$，或者已知Y分布的情况下使用统计方法（如Monte Carlo采样）产生大量的样本点来近似计算$H(Y)$，等等。为了同时保证估计的精度及小的计算代价，我们这里使用泰勒展开的方法获取$\log(p(y))$的一个合适的近似值 [166]，继而求解得到$H(Y)$。该方法思路如下：

以x_k为中心，对$\log(p(y))$进行泰勒展开，得到$\log(p(y))$的R阶泰勒级数展开式

$$\log(p(y)) = \sum_{r=1}^{R}\left\{\frac{1}{r!}\frac{d^r}{dy}\{log(p(y))\}(y-x_k)^r|_{y=x_k}\right\} + O_R\ . \tag{4-11}$$

上式中O_R表示拉格朗日余项。于是，我们可以得到

$$H(Y) \approx -\int_{-\infty}^{+\infty} p(y)\left\{\sum_{r=1}^{R}\frac{1}{r!}\frac{d^r}{dy}\{\log(p(y))\}(y-x_k)^r|_{y=x_k}\right\}dy\ . \tag{4-12}$$

显然，$H(Y)$的精度及计算复杂度依赖于参数R。这里选择$\log(p(y))$二阶泰勒级数展开（即$R=2$）来近似$\log(p(y))$。此时变量Y的熵近似为

$$H(Y) \approx -\sum_{k=1}^{K} p_k\{[\log(p(y)) - \frac{1}{2}f(y)]|_{y=x_k}\}, \tag{4-13}$$

其中

$$\begin{aligned} f(y) =& \frac{1}{p(y)\sqrt{2\pi}\sigma}\sum_{i=1}^{K} p_i[\frac{1}{p(y)}(y-x_i)\frac{d}{dy}p(y)+ \\ & \frac{1}{\sigma^2}(y-x_i)^2 - 1]exp(-\frac{(y-x_i)^2}{2\sigma^2})\ . \end{aligned} \tag{4-14}$$

据此可以计算出高斯加性信道的平均互信息。

注意，在执行期望最大化算法前，首先需要选择GMM组成成分的数目K。组成成分的数目的选择是FMM应用中的另一个重要问题，直接决定了模型的近似精度。以前有一些关于如何选择最优的K的研究 [162,167,168]，本章则选择使得高斯加性信道的平均互信息达到最大的K。除此之外，期望最大化算法的初始值可能会影响算法的结果，很有必要多选几个初始值并多次运行期望最大化算法，直至计算得到的高斯加性信道的平均互信息值趋于稳定为止。

为了验证上述方法的性能，图 4.2 给出了一个关于无保护AES-128算法的侧信息泄漏量估计的模拟实验。该AES-128算法的真实泄漏模型是随机模型，然后加入高斯噪声得到模拟泄漏信号。实验又分别使用了汉明重量模型和ID (Identification) 模型及核密度估计方法 [169]来近似估计该密码算法的侧信息泄漏。可以发现，本小节方法估计的高斯加性信道的平均互信息和理论上的侧信息泄漏很接近，精度甚至和使用了高斯模板刻画泄漏模型的参数估计方法相当。这两种方法都优于使用了核密度估计的非参数估计方法。

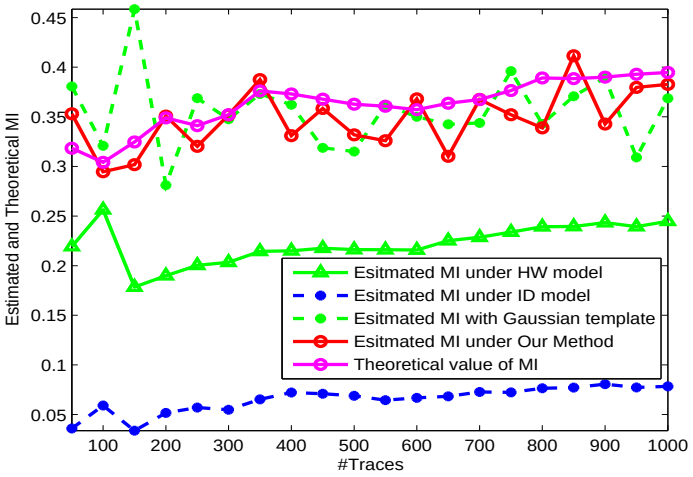


图 4.2　模拟高斯噪声场景下密码实现侧信息泄漏量估计值与理论值对比

4.2.2.2　高斯信道容量

通信信道的信道容量C是信道平均互信息所能达到的最大值，即

$$C = max[I(X,Y)] = max[H(Y) - H(N)] \ . \tag{4-15}$$

因信道是高斯加性信道，所以C是X的分布的凸函数，其值取决于$\{x_k\}$和$\{p_k\}$。而实际中密码芯片的侧信道泄漏（如能量泄漏）的能量总是有限的，即高斯信道的输出Y的能量是有限的。根据信息理论，此时若信源X服从高斯分布，信道的平均互信息会达到极值[170]。与前面类似，未知参数依然可通过期望最大化算法来求解。具体做法如下：

首先，分别将对应于同一个T的高斯加性信道输出Y的样本值归于一组。假设总共将信道输出的样本值分为m组，每组包含n_i个元素。这里$i = 1,\ldots,m$。令符号y_{ij}表示第i组第j个样本值。因为Y的每个样本值y_{ij}都是独立获取的，所以这些样本值之间彼此独立，并且满足$(y_{ij}|x_i,\sigma) \sim \phi(x_i,\sigma^2)$。其中，$\phi$表示均值为$x_i$、方差为$\sigma^2$的高斯分布，$j = 1,\ldots,n_i,\ i = 1,\ldots,m$。此时，信道的输入$X$也服从高斯分布。若设该分布均值为$\mu$、方差为$\tau^2$，则$X$的样本观察值$x_i \sim \phi(\mu,\tau^2)$。现在，信道模型中已知的参数是$y = \{y_{ij}, j = 1,\ldots,n_i;\ i = 1,\ldots,m\}$，待估计的未知参数分别是$z = (x_1,\ldots,x_m)$，$N = \sum_{i=1}^{m} n_i$和$\theta = (\mu, log\,\sigma, log\,\tau)$。

根据贝叶斯法则，我们得到

$$\begin{aligned} p(z,\theta|y) &= p(z,\theta,y)/p(y) = p(\theta|y,z)p(z|y), \\ p(z,\theta,y) &= p(\theta)p(z|\theta)p(y|z,\theta) \ . \end{aligned} \tag{4-16}$$

又因为$p(y)$和$p(z|y)$都独立于θ，故有

$$p(\theta|y,z) \propto p(z,\theta|y) \propto p(z,\theta,y), \tag{4-17}$$

也即有

$$\log(p(\theta|y,z)) \propto \log(p(z,\theta|y)) \propto \log(p(z,\theta,y)) \,. \tag{4-18}$$

又θ的共轭先验分布可以认为是与τ成比例 [171]，可得

$$\begin{aligned}\log(p(\theta|y,z)) \propto & -N\log\,\sigma-(m-1)\log\,\tau- \\ & \frac{1}{2\tau^2}\sum_{i=1}^{m}(x_i-\mu)^2-\frac{1}{2\sigma^2}\sum_{i=1}^{m}\sum_{j=1}^{n_i}(x_i-y_{ij})^2 \,.\end{aligned} \tag{4-19}$$

这里的z可视作隐藏变量，并可被期望最大化算法估计出来。首先在E-step中，计算出给定$\theta^{(t)}$和y时，式 4-19 的期望$E_z\{log(p(\theta|y,z))|\theta^{(t)},y\}$。又因为$x_i$的共轭先验分布依然是一个高斯分布 [171]，故有

$$(x_i|\theta^{(t)},y) \sim \phi(\upsilon_i^{(t)},\nu_i^{(t)}), \tag{4-20}$$

其中

$$\begin{aligned}\upsilon_i^{(t)} &= [\frac{\mu}{(\tau^{(t)})^2}+\frac{\sum_{j=1}^{n_i}y_{ij}}{(\sigma^{(t)})^2}]/[\frac{1}{(\tau^{(t)})^2}+\frac{n_i}{(\sigma^{(t)})^2}], \\ \nu_i^{(t)} &= [\frac{1}{(\tau^{(t)})^2}+\frac{n_i}{(\sigma^{(t)})^2}]^{-1},\end{aligned} \tag{4-21}$$

t表示第t次迭代。式 4-21 中的两个式子就是期望最大化算法的E-step的迭代公式。

随后，对$E_z\{log(p(\theta|y,z))|\theta^t,y\}$分别求关于参数$\mu,\sigma$和$\tau$的微分并令它们等于0，解方程后则可得到算法的M-step的迭代公式如下：

$$\begin{aligned}\hat{\mu}^{(t+1)} &= \frac{1}{m}\sum_{i=1}^{m}\upsilon_i^{(t)}, \\ \hat{\sigma}^{(t+1)} &= \left\{\frac{1}{n}\sum_{i=1}^{m}\sum_{j=1}^{n_i}[(y_{ij}-\upsilon_i^{(t)})^2+\nu_i^{(t)}]\right\}^{1/2}, \\ \hat{\tau}^{(t+1)} &= \left\{\frac{1}{m-1}\sum_{i=1}^{m}(\upsilon_i^{(t)}-\mu^{(t+1)})^2+\nu_i^{(t)}\right\}^{1/2} \,.\end{aligned} \tag{4-22}$$

因高斯加性信道的输入变量X及信道噪声N都服从高斯分布，且二者独立，故信道的输出变量Y也是一个高斯分布的变量，且其均值、方差分别等于输入变量X及信道噪声N均值和、方差和，亦即Y的均值为μ、方差为$\tau^2+\sigma^2$。此时，很容易得到高斯加性信道的信道容量

$$C = I(X,Y) = \frac{1}{2}log(1+\frac{\tau^2}{\sigma^2}) \,. \tag{4-23}$$

它只是描述了密码芯片侧信息泄漏量的一个上界，未必紧致。实际中平均互信息依赖于密码实现，可能等于C，也可能差别较大，C只能划定了一个密码芯片侧信息泄漏量

不可能越过的限。此外，上述过程中m就是GMM中的组成成分，不必再人为选择。

图 4.3 给出了一个真实高斯噪声场景下，本章方法和参数、非参数估计方法得到的密码芯片侧信息泄漏量估计值及信道容量估计值的对比曲线。实验测量的是一个无保护AES-128的8-bit MCU实现的能量泄漏。这个能量泄漏对应于AES-128算法第一轮的第九个S盒输出。根据经验，可将测量所得泄漏信号中的噪声近似认为是高斯噪声。

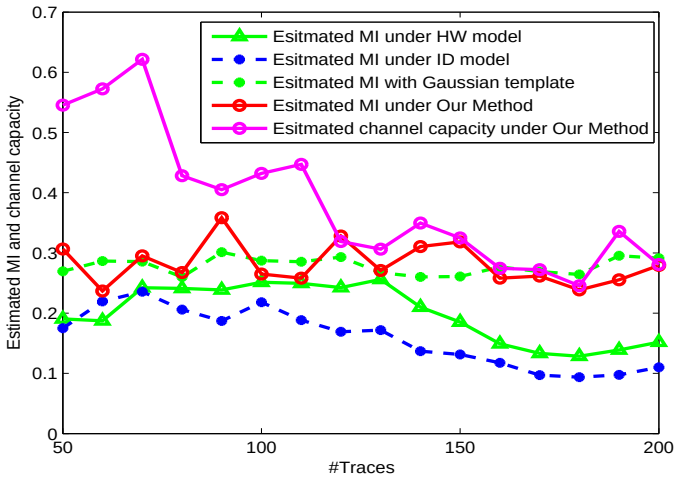


图 4.3　真实高斯噪声场景下密码芯片侧信息泄漏量估计值及信道容量估计值对比

从图 4.3 中可以观察到，基于HW模型的非参估计方法较基于ID模型的非参估计要好，说明HW模型比ID模型更准确，这也从图 4.4 上的攻击结果中得到了辅证。而本章方法计算得到的通信信道平均互信息要比前两种方法效果都高，和使用了高斯模板刻画泄漏模型的参数估计方法不相上下。

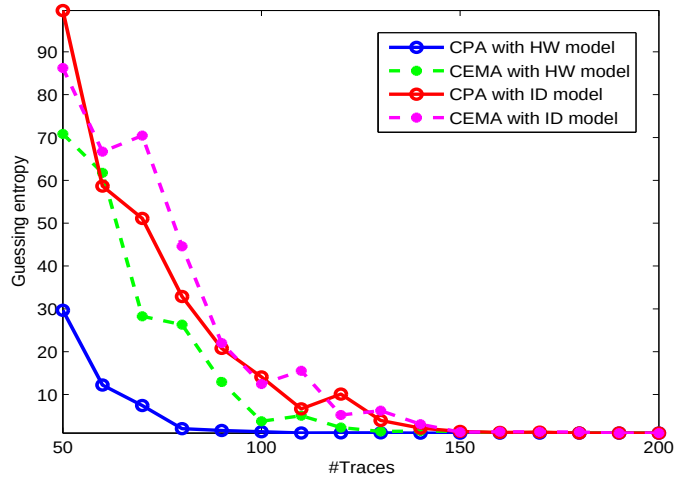


图 4.4　基于HW和ID模型的CPA及CEMA攻击所得的猜测熵

我们同时也估计了高斯加性信道的容量，提供了密码芯片侧信息泄漏量的一个粗糙上界。注意图 4.3 中随着能量迹数目的增大，我们估计的高斯加性信道的平均互信息

越来越接近于其信道容量。原因在于，该密码芯片的泄漏模型和噪声都近似服从高斯分布，近似满足高斯加性信道的平均互信息等于其信道容量的条件。这也辅证了我们经验性地将信道噪声看作高斯噪声是合理的。

4.2.3 非高斯加性信道

以上分析是在密码芯片的侧信息泄漏信号中的噪声属于高斯噪声的假设下进行的。然而，实际中泄漏信号内的噪声可能是非高斯的且没有闭式表达。这种情况下，图 4.1 中的通信信道是一个非高斯加性信道，对该信道进行参数估计将比较困难。幸运的是，如前所述，高斯混合模型可以以任意精度近似任意分布，因此我们可以先使用一个GMM来逼近非高斯噪声的分布，之后估计出非高斯信道参数，进而计算出非高斯加性信道的平均互信息及信道容量，从而获得密码芯片的侧信息泄漏量及其上界。

假设通信信道的非高斯噪声可以使用一个含有M个组成成分的一维GMM逼近，则非高斯噪声的概率密度函数$p(e)$可以写成

$$p(e) = \sum_{m=1}^{M} \alpha_m \frac{1}{\sqrt{2\pi}\delta_m} exp(-\frac{e^2}{2\delta_m^2}), \tag{4-24}$$

其中δ_m^2表示该GMM的第m个组成成分的方差。当$M = 1$时，非高斯噪声退化为高斯噪声。式 4-3 可调整为

$$p(y) = \sum_{k=1}^{K} p_k \sum_{m=1}^{M} \alpha_m \frac{1}{\sqrt{2\pi}\delta_m} exp(-\frac{(y - x_k)^2}{2\delta_m^2}) \, . \tag{4-25}$$

此时$p(y)$的对数似然函数为

$$\log\{\sum_{k=1}^{K} p_k[\sum_{m=1}^{M} \alpha_m \frac{1}{\sqrt{2\pi}\delta_m} exp(-\frac{(y - x_k)^2}{2\delta_m^2})]\}, \tag{4-26}$$

待估计的参数集为

$$\{x_1, \ldots, x_k, p_1, \ldots, p_k; \alpha_1, \ldots, \alpha_m, \delta_1, \ldots, \delta_m\},$$

其中$\sum_{k=1}^{K} p_k = 1, \sum_{m=1}^{M} \alpha_m = 1$，而且$\forall k, m, \, p_k \geq 0, \alpha_m \geq 0$。类似地，这些参数可以直接使用期望最大化算法来估计。

首先对$p(y)$的对数似然函数求微分，然后令微分为0并求解方程，可得期望最大化算法的E-step为

$$\begin{aligned} \hat{\gamma}_{nk}^{(t)} &= \frac{p(y_n|x_k)p_k}{\sum_{k=1}^{K} p(y_n|x_k)p_k}, \\ \hat{\beta}_{nm}^{(t)} &= \frac{\sum_{k=1}^{K} p_k \alpha_m \frac{1}{\sqrt{2\pi}\delta_m} exp(-\frac{(y-x_k)^2}{2\delta_m^2})}{\sum_{k=1}^{K} p(y_n|x_k)p_k}, \end{aligned} \tag{4-27}$$

之后可得期望最大化算法的M-step为

$$\begin{aligned}
\hat{x}_k^{(t+1)} &= \frac{\sum_{n=1}^{N} \hat{\gamma}_{nk}^{(t)} y_n}{\sum_{n=1}^{N} \hat{\gamma}_{nk}^{(t)}}, \\
\hat{\alpha}_m^{(t+1)} &= \frac{1}{N} \sum_{n=1}^{N} \hat{\beta}_{nm}^{(t)}, \\
\hat{p}_k^{(t+1)} &= \frac{1}{N} \sum_{n=1}^{N} \hat{\gamma}_{nk}^{(t)}, \\
\hat{\delta}_m^{(t+1)} &= \left\{ \frac{1}{\sum_{n=1}^{N} \hat{\beta}_{nm}^{(t)}} \sum_{n=1}^{N} \hat{\beta}_{nm}^{(t)} (y_n - x_k)^2 \right\}^{1/2},
\end{aligned} \tag{4-28}$$

其中$n = 1, \ldots, N, k = 1, \ldots, K, m = 1, \ldots, M$。

估计出所有参数后，$H(E)$可以使用第 4.2.2.1 小节中泰勒级数展开的方法近似计算，而$H(Y)$则利用Y的样本观察值近似计算，从而得出互信息$I(X, Y)$。使用期望最大化算法估计参数之前，需要预设参数K和M。这里依然采用多次试验的策略，来经验选择对应最大互信息的K和M值。

如前所述，非高斯噪声信道的信道容量C提供了密码芯片侧信息泄漏量的一个粗糙的上界。不过，非高斯噪声信道的信道容量并不像高斯噪声信道的信道容量那样有闭式解，它很难计算。此时，获取一个非高斯噪声信道的信道容量的上下界会比较容易。令符号σ^2表示非高斯信道噪声方差，如果输入变量的功率$E(x^2) \leq \sigma_x^2$，那么非高斯噪声信道的信道容量C满足下述不等式 [172]：

$$\frac{1}{2} log(1 + \frac{\sigma_x^2}{\sigma^2}) \leq C \leq \frac{1}{2} log(\frac{\sigma^2 + \sigma_x^2}{\sigma_e^2}) \,. \tag{4-29}$$

式 4-29 中σ_e^2表示非高斯噪声的熵功率，它满足等式$H(E) = \frac{1}{2} log(2\pi e \sigma_e^2)$。式 4-29 最右边的一项可以看作该非高斯噪声信道平均互信息的一个上界。

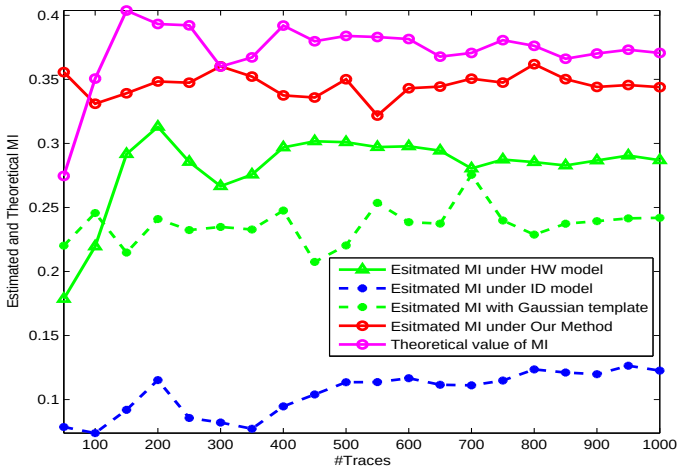
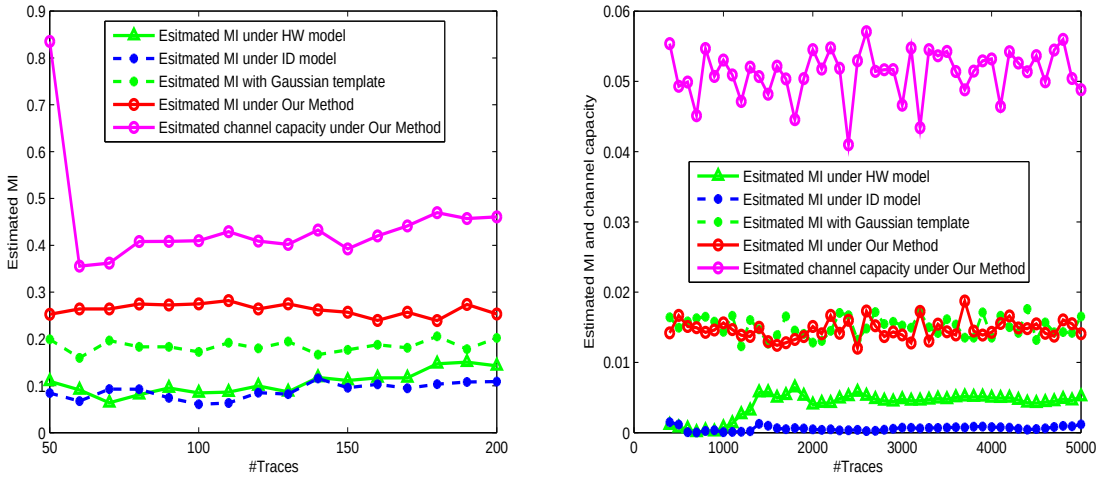


图 4.5　模拟非高斯噪声场景下密码实现侧信息泄漏量估计值与理论值对比

图 4.5 给出了一个模拟实验结果。该实验主要使用本文方法及基于高斯模板的参数、基于核密度估计的非参数估计方法，来分别估计一个具有HW泄漏的无保护AES-128实现的侧信息泄漏。泄漏信号中包含的噪声是非高斯加性噪声。该噪声的分布为一个包含三个成分的GMM。基于核密度估计的非参数估计方法分别使用HW模型和ID模型来估计该密码实现的侧信息泄漏量。可以观察到，本小节方法估计的高斯加性信道的平均互信息和理论上的侧信息泄漏很接近，精度超过了使用高斯模板刻画泄漏模型的参数估计方法，同时也优于使用核密度估计的非参数估计方法。有趣的是，基于HW模型的非参数估计方法表现好过基于高斯模板参数估计方法。究其原因，在于该实验中噪声的非高斯性及模拟泄漏信号的泄漏模型是HW模型。

图 4.6(a) 描述了一个真实非高斯噪声场景下，使用本文方法和参数、非参数估计方法得到的侧信息泄漏量估计值及信道容量估计值对比曲线。实验测量的是一个无保护的AES-128的8-bit MCU实现的电磁泄漏。这个电磁泄漏对应于AES-128算法第一轮加密运算的第九个S盒输出。据经验观察，测量的泄漏信号中的噪声属于非高斯噪声。从图 4.3 中可以观察到，基于HW模型的非参估计方法较基于ID模型的非参估计好，说明HW模型较ID模型更准确，这也从图 4.4 上的攻击结果中得到了辅证。基于高斯模板的参数估计方法计算得到的互信息值要比前两种方法得到的互信息值高。而我们的方法得到的互信息值高于这三种方法得到的值。我们同时也估计了非高斯加性信道的容量。由于噪声是非高斯的，我们的方法得到的互信息值高于基于高斯模板的参数估计方法计算得到的值，但随着电磁迹数目增加，其值一直小于信道容量。这也辅证了我们经验性地将该通信信道噪声视为非高斯噪声是合理的。



(a) 真实非高斯噪声场景下本节方法和基于高斯模板的参数、基于核密度估计的非参数估计方法所得侧信息泄漏量估计值及信道容量估计值对比（无保护AES-128实现）

(b) 真实非高斯噪声场景下本节方法和基于高斯模板的参数、基于核密度估计的非参数估计方法所得侧信息泄漏量估计值及信道容量估计值对比（有保护AES-128实现）

图 4.6　真实非高斯噪声场景下密码芯片侧信息泄漏量估计值及信道容量估计值对比

图 4.6(b) 给出了另一个实现在智能卡（Atmega163）上的受布尔掩码保护的AES-128加密算法第一轮第一个S盒输出的泄漏估计的例子。它的结论类似图 4.3。为了使得测量得到的能量迹中的一阶泄漏信息暴露出来，我们在估计智能卡侧信息泄漏量前对能量迹进行了预处理 [173]。然而由于预处理带来的不可避免地信息损失，图 4.6(a) 估计得到的智能卡侧信息泄漏量显著低于图 4.3 中无保护实现的侧信息泄漏量。这侧面说明了掩码减少了密码芯片侧信息泄漏量，即使经过预处理也无法恢复到无保护密码实现的泄漏水平，因此对前者的高阶攻击的效率总是低于对后者的一阶攻击 [173]。

综上可知，本节提出的基于通信信道理论的侧信道泄漏评估方法建立在期望最大化算法的基础上，计算有关密码芯片侧信息泄漏量时较为高效，且结合了目前非参数估计方法实际可操作性强及参数估计方法精度高的优点。

4.3 基于通信信道理论及一致性检验的侧信道泄漏检测算法

此外，我们基于侧信道所转化的通信信道的信道特性，发展出了一种基于统计的泄漏检测技术。其基本思想叙述如下：

因为侧信道泄漏信号中不依赖于秘密信息的泄漏特征点，对侧信道分析没有帮助，可以视为随机产生的噪声信号，所以直觉上，以这些泄漏点建立的通信信道模型的参数应该是随机变化的，即它们对应的通信信道模型应该是变参的通信信道模型。与之相反，建立在依赖于秘密信息的泄漏特征点上的通信信道模型应该是恒参的通信信道。故而，如果我们对使用期望最大化算法求解出的信道参数进行一致性检验，对应于第一种情形下的变参的通信信道模型，得到的信道参数的估计应该是非一致估计量；对应于第二种情形下的恒参的通信信道模型，得到的信道参数的估计应该是一致估计量。换言之，我们所估计出的恒参通信信道模型参数的一致性应该强于估计出的变参通信信道模型参数估计的一致性。

根据这个判断，第 4.2.2 小节中的关于估计通信信道的平均互信息及信道容量的分析，也适用于侧信道泄漏检测。我们这里要进行一致性检验的信道参数既可以是式 4-8 中的σ，也可以是式 4-22 中的σ, μ或τ。下面首先介绍下一致性或相合性检验的概念 [171]。

假设$\{Z_1, \ldots, Z_n\}$为一个样本总体Z的样本，$\theta \in \Theta$是Z中的参数，$\hat{\theta} = \hat{\theta}(Z_1, \ldots, Z_n)$表示$\theta$的一个估计量。如果$\forall\theta \in \Theta$，当$n \to \infty$时，$\hat{\theta}$能依照概率1收敛于$\theta$，也就是下式

$$\lim_{n\to\infty} Pr\{|\hat{\theta} - \theta| < \varepsilon\} = 1, \ \forall\varepsilon > 0 \tag{4-30}$$

成立，那么符号$\hat{\theta}$称为θ的一致估计量。

然而即使给出了参数一致性检验的概念，在实际中却往往因式 4-30 中概率难以计算，导致进行一致性检验并不容易。为了保证本节中参数一致性检验具有较强的实际可操作性，我们需要考虑别的替代方案。如果$\hat{\theta}$能依照概率1收敛于θ，那么所有迭代过

程中$\hat{\theta}$的曲线起伏应该比较小，从而可以据此进行参数一致性检验。因为建立在依赖于秘密信息的泄漏特征点上的通信信道模型应该是恒参通信信道，所以整个期望最大化算法所有迭代过程中$\hat{\theta}$的标准差的变化，应该远小于建立在与秘密信息无关的泄漏点上的变参通信信道模型参数估计中$\hat{\theta}$的标准差的变化。综上所述，该方案通过考察整个期望最大化算法所有迭代过程中$\hat{\theta}$的标准差的变化情况来替代参数一致性检验。

进一步地，为了获得一个更鲁棒的结果，我们推荐使用表现更稳定的平均绝对偏差代替标准差来度量$\hat{\theta}$的整体变化 [174]。样本总体Z的样本平均绝对偏差形式如下：

$$d_n = \frac{1}{n}\sum_{i=1}^{n}|Z_i - \bar{Z}|, \tag{4-31}$$

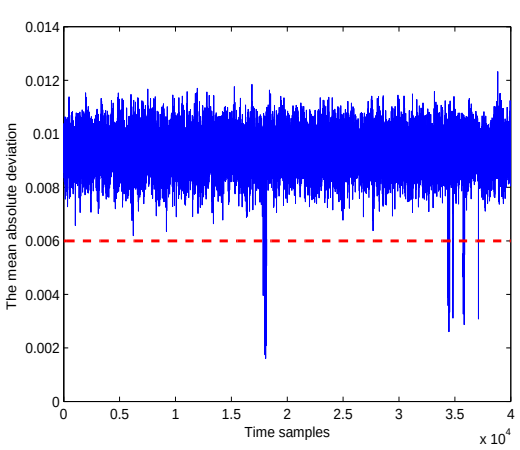
其中

$$\bar{Z} = \frac{1}{n}\sum_{i=1}^{n}Z_i$$

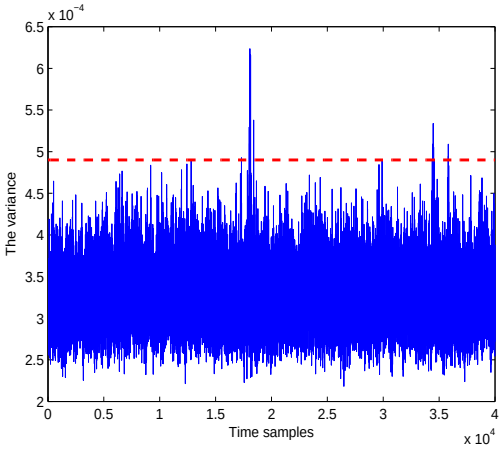
表示样本均值。当然，为了判断在一个时刻的样本点上是否存在泄漏，一个经验的阈值（诸如样本点的四分位点之类）需要预置。若在某一时刻的样本点的d_n高于阈值，则将该样本点视为一个秘密信息泄漏点。

我们使用了一些实际实验来验证所提出方法的有效性，结果如图 4.7 及图 4.8 所示。图中的对比方法是文献 [95]提出的另一种基于统计的泄漏检测技术，即基于方差的泄漏检测技术。该方法同样对密码芯片泄漏采集没有特殊要求。注意，二图中所有图形的水平轴都代表时刻，纵轴都代表对应于同一明文或密文输入的泄漏信号的均值差，或者式 4-22 中τ的所有迭代过程中的估计值的平均绝对偏差d_n，并且所有图形中的虚线划定了判断阈值。若某一时刻的泄漏点在纵轴上的值大于方差的阈值或d_n的阈值，则认为它包含依赖于秘密信息的泄漏。图 4.7 分别展示了本节提出的方法及基于方差的泄漏检测方法，针对一个无保护AES-128的8-bit MCU实现第一轮第一个S盒的能量泄漏的泄漏检测结果（根据明文第一个字节将测量泄漏样本分类）。图 4.8 分别展示了我们提出的方法及基于方差的泄漏检测方法，对一个无保护AES-128的FPGA实现的能量泄漏的泄漏检测结果（根据密文第一个字节将测量泄漏样本分类）。

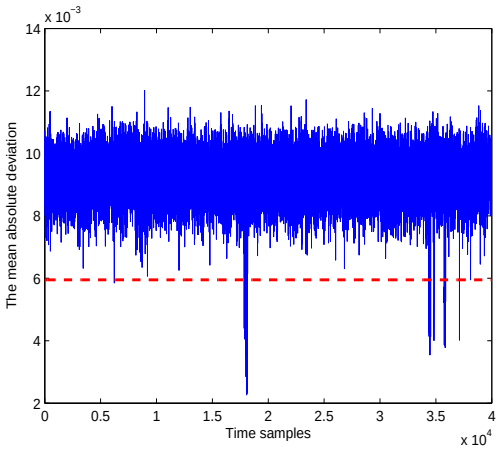
在图 4.7 和图 4.8 中，两种泄漏检测技术检测出的依赖于秘密信息的泄漏点几乎和使用CPA分析检测出的泄漏点一致（见图 4.9，针对MCU及FPGA实现所选的攻击目标分别是第一轮第一个S盒输出，以及最后一轮第一个S盒输入与输出的异或值）。图 4.7 中检测出的泄漏特征点对应于AES-128 MCU实现的第一轮第一个S盒输出的能量泄漏，而图 4.8 中检测出的泄漏特征点对应于无保护AES-128 FPGA实现最后一轮第一个S盒输出和输入异或值的能量泄漏。也就是说，这些被检测出的泄漏特征点是CPA的POIs，可以直接拿来实施侧信道攻击。相较之下，基于T-test的一类泄漏检测算法通常会检测出很多对攻击无用处的泄漏点 [17]。更进一步地，本节提出的方法找



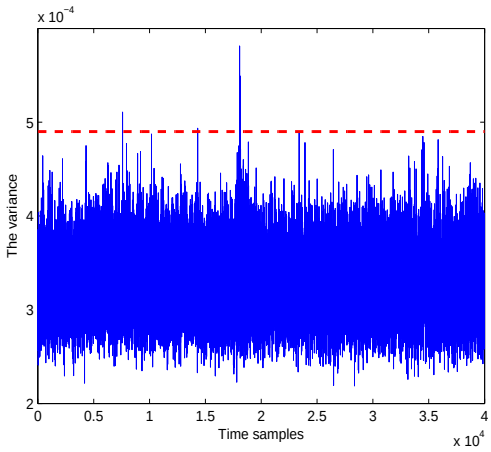
(a) 本节所提泄漏检测方法检测结果（1,000条能量迹）, SNR=+∞



(b) 基于方差的泄漏检测方法检测结果（1,000条能量迹）, SNR=+∞



(c) 本节所提泄漏检测方法检测结果（1,000条能量迹）, SNR=30dB



(d) 基于方差的泄漏检测方法检测结果（1,000条能量迹）, SNR=30dB

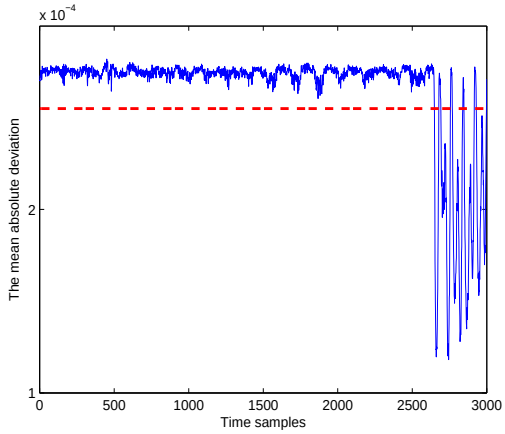
图 4.7　针对AES-128 MCU实现的第一轮第一个S盒输出的能量泄漏的检测结果

出了所有CPA的POIs，而基于方差的泄漏检测方法却未找完全，甚至检测出无用样本点。这种差别在图 4.7(a) 和图 4.8(a) 中比在图 4.7(b) 和图 4.8(b) 中表现更明显。

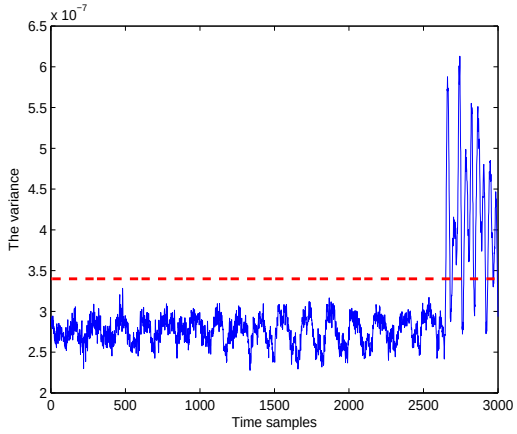
最后，为了考察本节提出的泄漏检测技术的抗噪声性能，我们在原始泄漏信号的基础上按一定“信噪比”*添加了高斯噪声，并进行泄漏检测。结果详见图 4.7(c), 4.7(d) 和图 4.8(c), 4.8(d)。从图中可以观察到，结果依然是本节提出的方法找出了所有CPA的POIs，而基于方差的泄漏检测方法检测出的POIs却更少，无用样本点更多。不过，随着噪声加大，两种方法的效率均有所下降。此时只需增加泄漏信号数目来抵消增长的噪声带来的负面影响即可。

图 4.10 分别给出了两种检测方法对同一密码算法的FPGA实现的第一轮第一个S盒输出的能量泄漏的检测结果（根据明文第一个字节将能量泄漏样本分类）。可以观察到

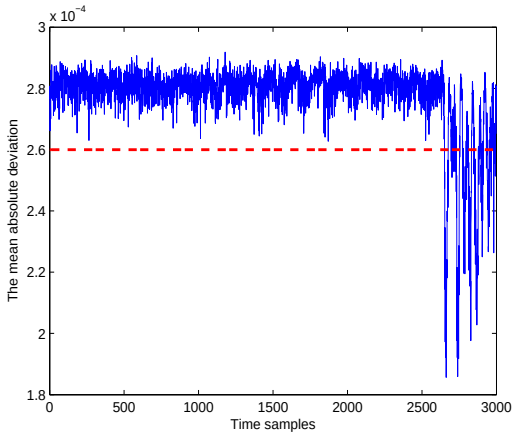
*　表示将原始信号视为“纯净”信号，然后添加噪声。



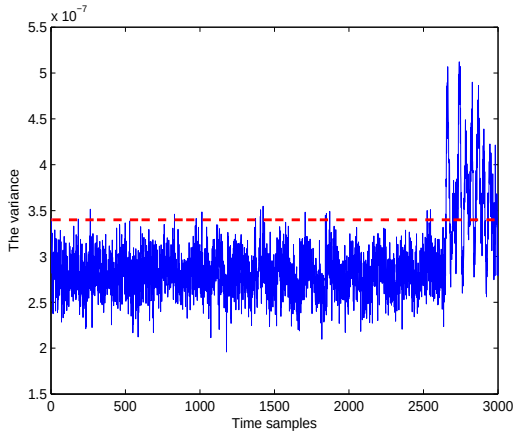
(a) 本节所提泄漏检测方法检测结果（30,000条能量迹），SNR=+∞



(b) 基于方差的泄漏检测方法检测结果（30,000条能量迹），SNR=+∞

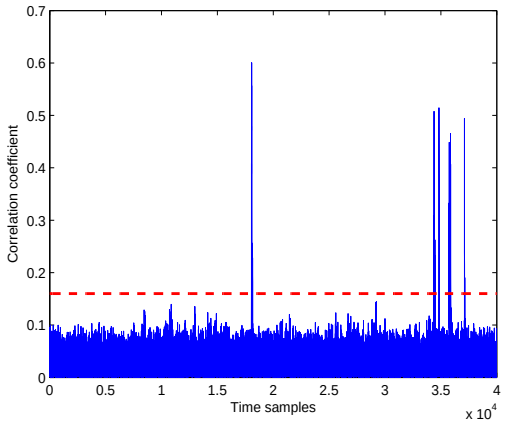


(c) 本节所提泄漏检测方法检测结果（30,000条能量迹），SNR=80dB

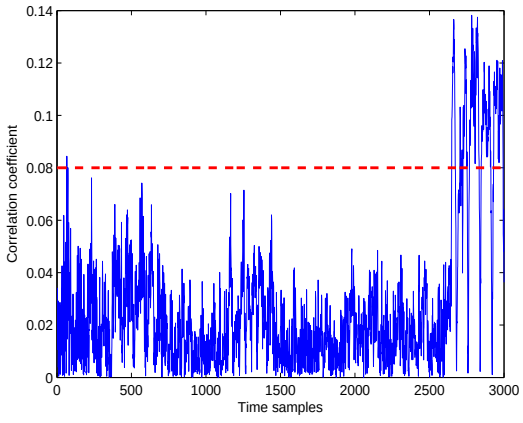


(d) 基于方差的泄漏检测方法检测结果（30,000条能量迹），SNR=80dB

图 4.8 针对AES-128 FPGA实现的最后一轮第一个S盒输入输出异或值的能量泄漏的检测结果



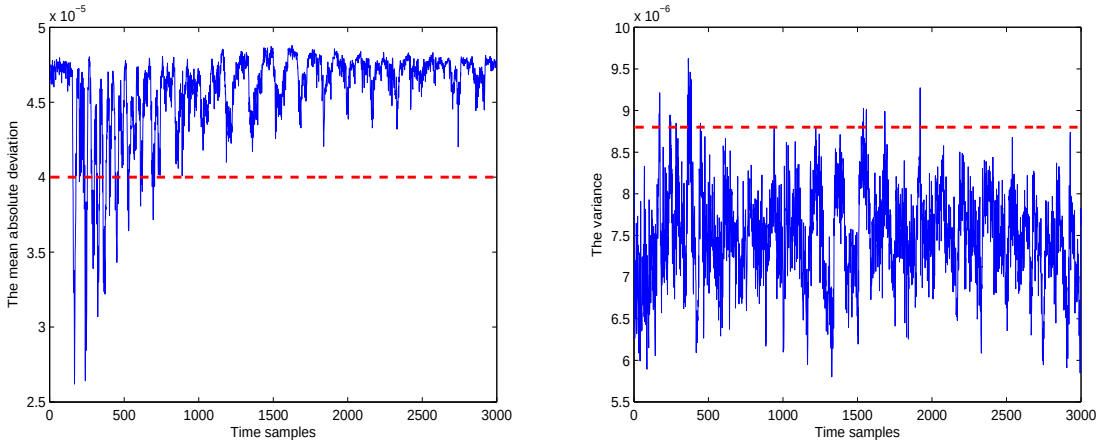
(a) 使用1,000条能量迹检测到的MCU实现的POIs



(b) 使用30,000条能量迹检测到的FPGA实现的POIs

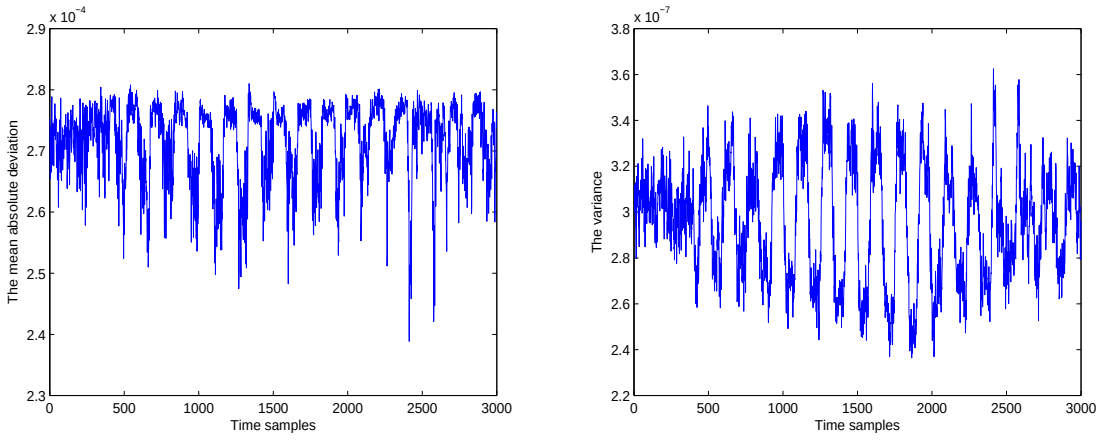
图 4.9 CPA分析找到的AES-128 MCU实现及FPGA实现的POIs

本节所提方法性能远远优于对比方法——后者甚至不能检测出有效的泄漏特征点。一个值得注意的现象是，因FPGA实现的泄漏模型是汉明距离模型，且由于行移位操作的作用，导致最后一轮中某些S盒输出的泄漏与输入的明文不对应，使检测到的泄漏点有时包含较多的非POIs点（图 4.11，根据密文第二个字节将测量泄漏样本分类）。另外，本节提出的泄漏检测技术同样能检测出其它类型的侧信息泄漏点。图 4.12 给出了一个针对密码芯片电磁泄漏的检测例子（根据密文第一个字节将电磁泄漏样本分类）。



(a) 本节所提泄漏检测方法检测结果（30,000条能量迹） (b) 基于方差的泄漏检测方法检测结果（30,000条能量迹）

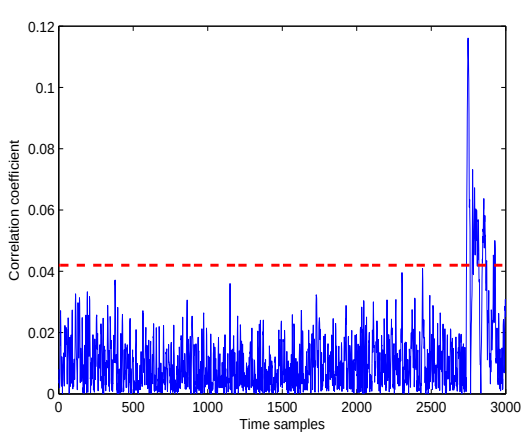
图 4.10　针对AES-128 FPGA实现的第一轮第一个S盒输出的能量泄漏的检测结果



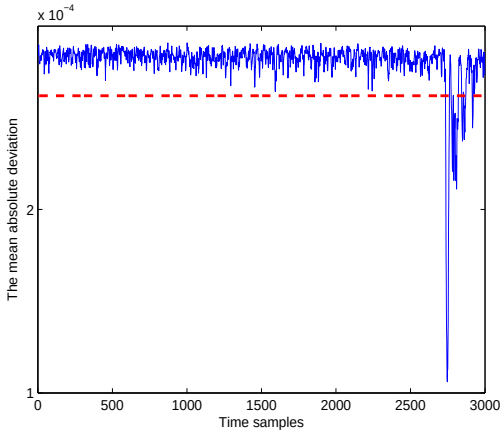
(a) 本节所提泄漏检测方法检测结果（30,000条能量迹） (b) 基于方差的泄漏检测方法检测结果（30,000条能量迹）

图 4.11　针对AES-128 FPGA实现的最后一轮第二个S盒输出的能量泄漏的检测结果

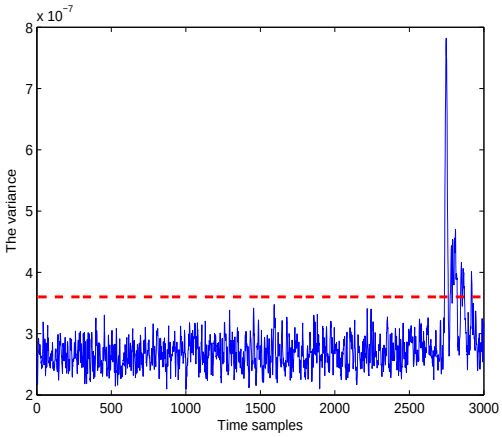
当将本文所提泄漏检测方法与基于方差的泄漏检测方法用于受保护密码算法实现的泄漏检测时，例如对一个AES-128算法的布尔掩码实现进行泄漏检测，若对泄漏信号不做预处理，则由于掩码隐藏了泄漏信息，同一消息对应的泄漏信号的均值的方差信



(a) CEMA分析得出的检测结果（30,000条电磁迹）



(b) 本节所提泄漏检测方法检测结果（30,000条电磁迹）



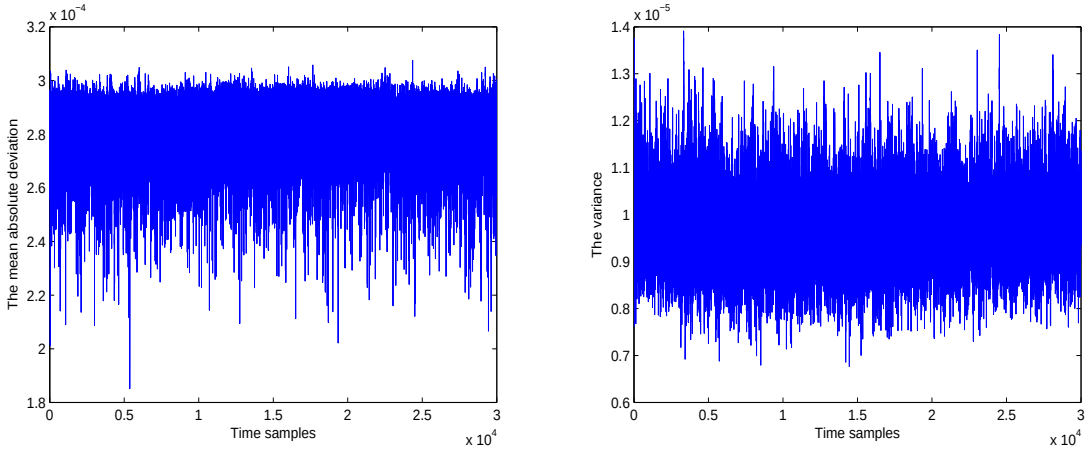
(c) 基于方差的泄漏检测方法检测结果（30,000条电磁迹）

图 4.12 针对AES-128 FPGA实现的最后一轮第一个S盒输入输出异或值的电磁泄漏的检测结果

息也被遮盖，而建立的侧信道的通信信道模型输入输出也会不准确（如图 4.13 所示，该实验根据明文第一个字节将测量泄漏样本分类），从而无法检测出该实现的POIs。

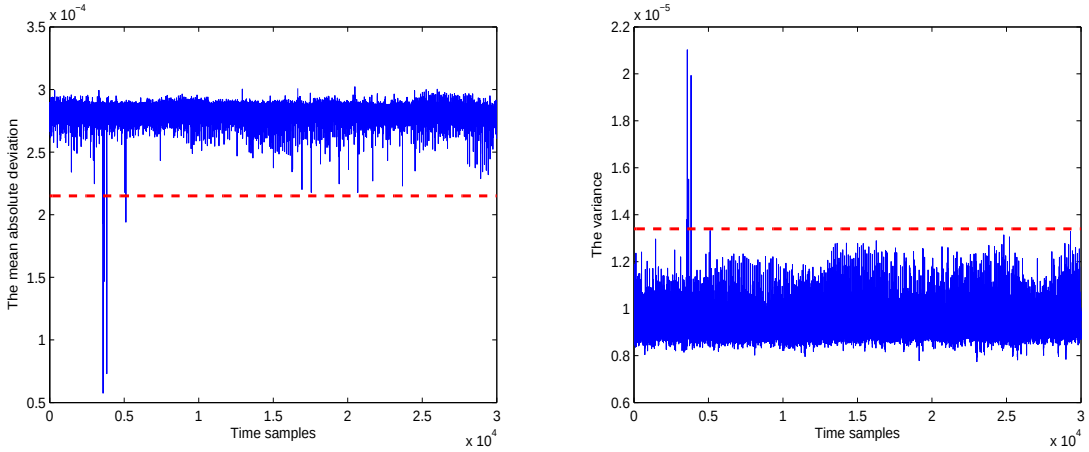
如果在对泄漏信号进行预处理而恢复一部分被掩码隐藏的泄漏信息后，再进行泄漏检测，则两种方法能很容易地检测出该实现的POIs（如图 4.14 所示，该实验根据明文第一个字节将测量泄漏样本分类）。此外，使用别的侧信道的通信信道模型参数（例如式 4-8 中的参数σ）进行一致性检验也能达到相似效果，这里不再赘述。

综合以上实验结果，本文提出的泄漏检测方法优于基于方差的泄漏检测技术 [95]。寻其原因，在于本文方法利用的是泄漏的分布信息，而基于方差的泄漏检测技术则仅仅利用了泄漏的均值和方差信息。除此之外，本节提出的泄漏检测方法是基于高斯噪声假设的，而高斯噪声使得一个通信信道在所有加性噪声信道中信道容量最小 [172]，这意味着，本节提出的泄漏检测方法可以在最坏情况下运行，即在可获取的密码芯片侧信息泄漏量最小的情况下依然能检测到泄漏。



(a) 本节所提泄漏检测方法检测结果（5,000条能量迹） (b) 基于方差的泄漏检测方法检测结果（5,000条能量迹）

图 4.13 针对一个实现在智能卡上的AES-128掩码方案第一轮第一个S盒输出的能量泄漏的检测结果



(a) 本节所提泄漏检测方法检测结果（5,000条能量迹） (b) 基于方差的泄漏检测方法检测结果（5,000条能量迹）

图 4.14 预处理后针对一个实现在智能卡上的AES-128掩码方案第一轮第一个S盒输出的能量泄漏的检测结果

4.4 扩展讨论

基于本章所提出的侧信道的通信信道模型，可以将我们的工作拓展到以下四个方面。

4.4.1 多泄漏特征点分析

当密码芯片的侧信道泄漏信号中存在多个与敏感变量相关的泄漏特征点时，文中通信信道模型的输入就会变成一个扩展信源 [165]。此时每个泄漏特征点对应一个通信信道，从而使计算得出的通信信道平均互信息增大。也就是说，密码芯片的侧信息泄漏相对于单点泄漏会多。这从信息论角度解释了为何多点侧信道攻击效率高于单点侧

信道攻击 [64]。

4.4.2　泄漏模型刻画

如果我们知道了密钥，那么使用文中方法刻画密码芯片的泄漏模型也是可行的。因为式 4-8 中的γ_{nk}的含义是样本观察值y_n由高斯混合模型中第k个成分生成的概率，故对应于式 4-2 中每个T的模型泄漏值可以利用一些匹配算法, 如匈牙利算法 [175]获得。所以当密钥知道时，中间值也可知道，中间值对应的模型泄漏也就得到了，从而刻画出密码芯片的泄漏模型。

4.4.3　碰撞攻击

在密钥未知的情况下，利用匹配算法得到式 4-2 中每个T的模型泄漏值后，可以进行碰撞攻击恢复密钥。以AES-128为例，我们可以将整个明文或密文分成16个字节，每个字节对应一个T。因每个T的模型泄漏值已知，故所有子密钥的关系也可以确定下来。只需枚举一个子密钥的所有可能值，主密钥就可以通过一组或多组明密文对验证恢复。

4.4.4　抑制噪声及估计信噪比

顺带地，在我们估计出 4-8，式 4-22 或式 4-28 中的噪声参数之后，就可以使用相应滤波器来减弱噪声，提高泄漏信号信噪比。进而原始泄漏信号的信噪比也能一道估计出来。

4.5　本章小结

本章在通信信道理论框架下，将侧信道看作一个通信信道，研究了侧信道泄漏评估与检测技术，并在不同信道模型下计算出通信信道的平均互信息，继而以通信信道的平均互信息作为密码芯片的侧信息泄漏量的估计。本章提出的方法结合了以往参数估计方法和非参数估计方法的优点。此外，我们根据通信信道理论，发现可将通信信道的信道容量看作密码芯片的侧信息泄漏量的一个粗糙的上界估计。文中所提出的通信信道的平均互信息及信道容量的计算都是建立在期望最大化算法的基础上，运算效率较高。有趣的是，我们依据侧信道通信信道模型的信道特性及参数一致性检验，提出了一种基于统计的侧信道泄漏检测技术，其基本思路是利用待估计参数的一致性或相合性来检测泄漏点。本章工作为侧信道泄漏评估与检测技术的研究提供了新的视角。未来的研究中我们将继续研究第 4.4 节提出的四个扩展问题，以及在未知掩码的情况下，掩码实现方案的泄漏评估与检测问题。

第五章　密钥枚举与密钥排序

如第一章所述，目前关于密钥枚举技术的研究，基本都是在最优密钥枚举算法[20]的基础上发展而来。不过，这些密钥枚举算法所做的仅是将主密钥候选值按概率大小枚举，并没有改变真实主密钥在所有主密钥候选值中的排序。而侧信道攻击所得真实主密钥在所有主密钥候选值中的排序位置才是决定密钥枚举算法最终枚举次数的根本因素。如果有算法能将真实主密钥在所有主密钥候选值中的排序位置提前，那么将会从根本上提高密钥枚举效率。本章即着眼于此，结合真实密钥排序位置随泄漏信号数目变化的曲线积分，提出了两种方法。它们通过改变侧信道攻击所得子密钥候选值的排序，将所有真实子密钥的排序位置提前，进而将真实主密钥的排序位置提前，从根本上减少密钥枚举次数。

另外，在对密钥排序技术的研究中，本章利用子密钥候选值的位置排序来估计真实主密钥的排序位置，并应用信号多抽样率抽取及插值技术来提高文献 [25]所提方法的精度，同时基于子密钥相关性，提出一种能评估最坏情况下密码芯片安全水平的密钥排序算法。

5.1　预备知识

下面介绍与本章内容有关的概念及知识，包括密钥枚举、密钥排序及信号的抽取与插值等内容。

5.1.1　密钥枚举概念介绍

如第 1.2.4 小节所述，若攻击者获得的侧信道泄漏量不足以完成一次成功的攻击，则会导致真实密钥在所有密钥候选值排序中排在某一中间位置。这种情形下，可结合密钥枚举技术来进行分析。密钥枚举的流程可简述为：通过将主密钥分成多个部分进行侧信道攻击后，得到各个子密钥所有候选值的排序（即key rank）及分数（如概率、相关系数等），然后据此枚举主密钥候选值，以期恢复完整的主密钥。现在的研究在对各个子密钥所有候选值进行枚举时，常常依据最大似然原则 [20]，即将各个子密钥候选值的后验概率分别相乘，得到相应主密钥候选值的后验概率，并依序枚举主密钥候选值。

总而言之，密钥枚举就是联合侧信道攻击恢复出的密钥的部分信息，通过枚举来恢复密钥的完整信息。示意图 5.1 在将一个主密钥分为两个子密钥的假设下，给出了由这两个子密钥概率分布联合得到的主密钥概率分布的几何表达。图中X轴及Y轴分别表示两个子密钥可能的取值，Z轴$P(k_1,k_2)$表示由两个子密钥后验概率相乘而得到的主密钥的后验概率，并用红色标记出概率最高的密钥候选值部分，黄色、青色部分的概率

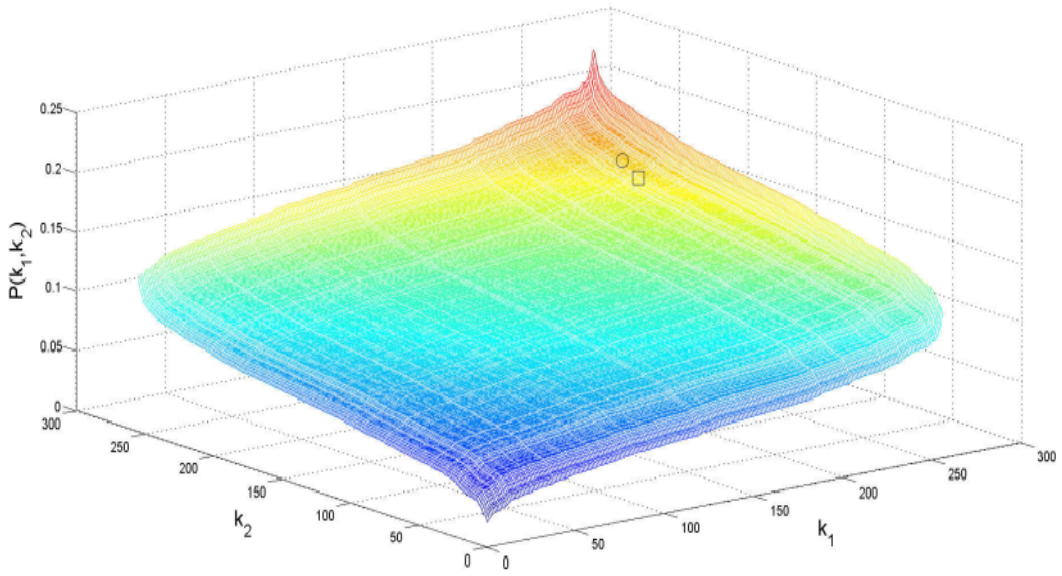


图 5.1　密钥空间的几何表达

值依次降低，蓝色部分的概率最低。进行密钥枚举时，按从红色到黄色、青色及蓝色部分依序进行。例如，图 5.1 中圆圈标示处所对应的主密钥候选值的后验概率较矩形标示处所对应的主密钥候选值的后验概率大，枚举时应优先枚举前者所对应的主密钥候选值。

密钥枚举属于侧信道分析技术范畴，其过程类似暴力穷搜破解，但一般要比暴力穷搜破解快得多。

5.1.2　密钥排序概念介绍

密钥排序属于侧信道检测技术范畴，与密钥枚举的概念非常接近。二者的区别在于，密钥枚举应用于分析者获取的密码芯片侧信息泄漏不足以完成一次成功侧信道攻击，但枚举次数不能超过分析者计算能力（以现在的计算能力而言，约为2^{40} ～ 2^{50} [115]）的场景下，属于侧信道分析范畴；密钥排序则用于分析者的计算能力受限的场景下，即真实密钥的排序位置较为靠后（例如在所有候选值中排在第2^{100}位）时。此时分析者并不能分辨出密码芯片的安全水平到底是2^{51}还是2^{120}，只能在预先知道真实密钥信息的前提下，使用密钥排序技术，才能检测出密码芯片安全水平 [21]。除了需要知道真实密钥之外，密钥排序不必枚举出在真实密钥排序前的所有密钥候选值，只需估计出真实密钥的排序位置即可。

5.1.3　信号的抽取与插值

在实际中采集到的信号常常包含大量冗余，需要对信号进行抽取，在无损信号的同时压缩信号，提高处理效率。与之相反，当信号包含的样本点过少，则需对信号进行插值处理。在信号处理领域，以一定抽样率对模拟信号采样得到数字信号的过程称

为信号的“抽样”，降低抽样率的过程称作信号的“抽取”，增加抽样率的过程称作信号的“插值”，也即“抽样率扩张” [156]。

下面简要介绍下对一个离散时间信号减小采样率进行整数倍抽取，以及提高采样率进行整数倍插值后，其相较原始信号发生的变化。

5.1.3.1 信号的整数倍抽取

假设一个密码芯片运行密码算法时产生的能量泄漏信号为$x_a(t)$。显然，$x_a(t)$是连续时间信号。当我们以一定采样率（记为f_s）对$x_a(t)$进行抽样得到能量迹时，此时得到的信号是离散时间信号，记为$x(n)$。此时，$x(n)$的频谱是$x_a(t)$的频谱以T（$T = 2\pi/f_s$）为周期的延拓 [156]。若连续时间信号的采样率f_s 大于或等于2 倍该信号最高频率（即奈奎斯特频率）分量时，根据奈奎斯特-香农抽样定理，$x(n)$能完美恢复信号$x_a(t)$。否则会产生频率混叠失真。但是如果我们对信号的奈奎斯特频率并不十分清楚，或者因为其它原因，设置的f_s远远大于奈奎斯特频率，那么信号的抽样数据量会变得过大，冗余过多。这种情况下，为了提高信号处理效率，我们可以减小采样率，只要保证信号不发生频率混叠失真即可。例如我们可以将抽样率减少至f_s的$1/D$，即在$x(n)$中每D个连续的值中抽取一个组成新的序列信号$x_d(n)$，以减少信号处理的数据量。这里要求D是整数，上述过程也被称为信号的整数倍抽取 [149,156]。序列信号$x_d(n)$的频谱是$x(n)$频谱先进行频率D倍的扩张，后按$2\pi/D$ 的整数倍移位叠加而成。

5.1.3.2 信号的整数倍插值

与信号的整数倍抽取相对的是信号的整数倍插值。假设采样率f_s过小，将其增大I倍，即是对序列信号$x(n)$的插值 [149,156]。这里要求I是整数。对信号的进行整数倍插值，也可以将$x(n)$转化为$x_a(t)$，再增加采样频率，但这会产生失真和采样误差。一般做法是：先在$x(n)$中每两个连续的值中插入$(I-1)$个零值，扩展原信号的频谱后，再使用一个低通滤波器进行平滑插值，获得新的扩展序列信号$x_I(n)$。此时所得新的序列信号$x_I(n)$的频谱是$x(n)$频谱频率I倍的压缩。

实际应用中通常将信号的整数倍抽取与插值混合使用，即先插值后抽取，既减少数据量，又避免失真 [156]。图 5.2*描述了离散时间信号$x(n)$经过整数倍抽取与插值后频谱的变化。图中(b)则表示$x(n)$ 经3倍抽取后得到的信号$x_d(n)$ $(D = 3)$的幅度谱，(c) 则表示将(b)中的$x_d(n\Psi$又经2倍插值后得到的信号$x_I(n)$ $(I = 2)$的幅度谱，而(d)则表示将$x(n)$经2倍插值后又经7倍抽取后得到的信号$x_Id(n)$ $(I = 2, d = 7)$的幅度谱。其中，$X(e^{j\omega T})$表示序列信号以数字频率ω为变量的傅里叶变换 [149,156]。可以看出，在对信号进行整数倍抽取与插值时，应保证抽取和插值后的频谱不会发生混叠，以免信号失真，同时也应尽可能地占满频谱，减少信号的数据量。

* 图片来源于文献 [156]。

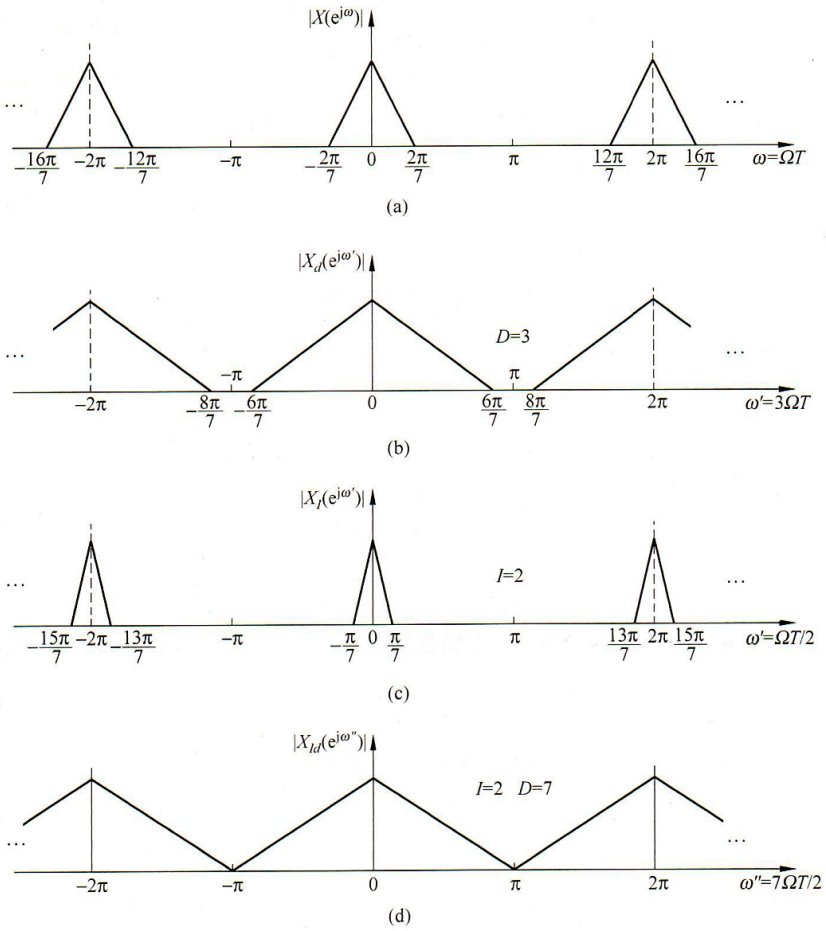


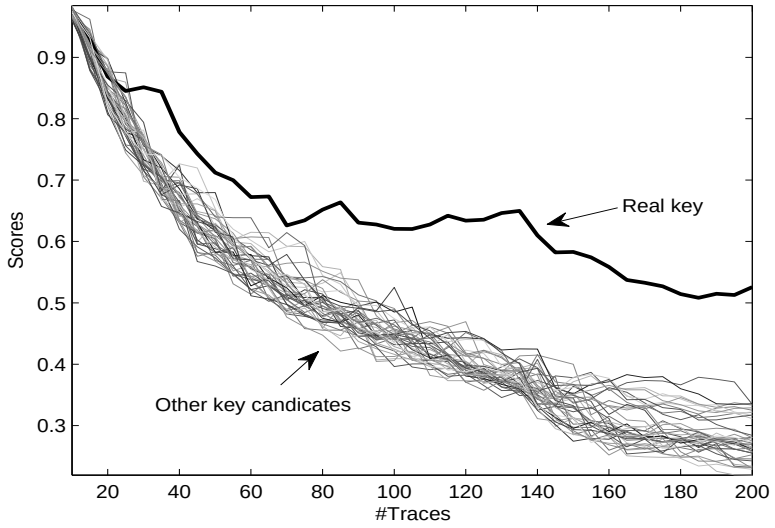
图 5.2　连续时间信号、序列信号、抽取序列信号及插值序列信号的频谱

5.2　密钥枚举技术研究

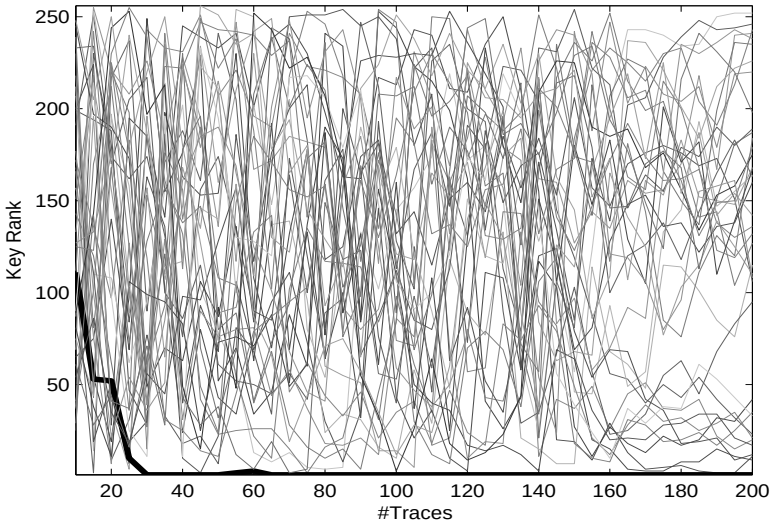
我们首先来看下随着泄漏信号数目增加，侧信道攻击所得真实密钥与其它密钥候选值的分数及排序变化曲线。

图 5.3(a) 给出了真实密钥（图中加粗黑线）与其它密钥候选值的分数大小变化曲线。从图 5.3(a) 中可以观察到，随着密码芯片侧信息泄漏量的增加，侧信道攻击使得真实密钥与其它密钥候选值的区分度越来越大。换言之，真实密钥在所有密钥候选值中的排序位置随着密码芯片侧信息泄漏量的增加，在稳步地上升。虽然实际中真实密钥的排序位置可能会略有波动，但其整体上依然保持快速上升的趋势。

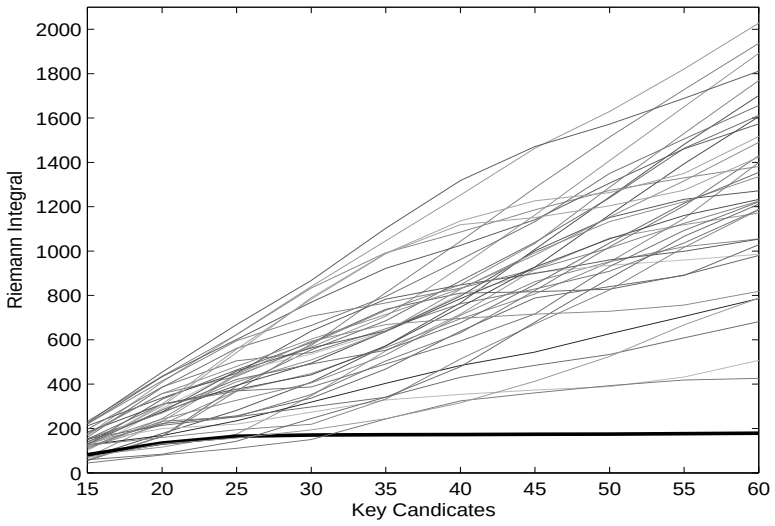
与之等价地，在图 5.3(b) 中我们给出了真实密钥（图中加粗黑线）与其它密钥候选值的排序位置随着侧信息泄漏量变化的曲线。图中真实密钥的排序位置整体趋于前列，且越到后来上升越快，而其它密钥候选值的排序变化则显得有些随机、杂乱。侧信道攻击显然是通过密钥排序位置这一度量指标来区分真实密钥与其他密钥候选值的。在此基础上，只要我们能找出另一个可合理刻画真实密钥排序的上升速度的度量指标，那么即使在可获取的侧信息泄漏量不充足的情形下，也能将真实密钥与多数密钥候选值提前区分开来，进而提升真实密钥在所有密钥候选值中的排序位置。



(a) 真实密钥与其它密钥候选值的分数变化曲线



(b) 真实密钥与其它密钥候选值的排序变化曲线



(c) 真实密钥与其它密钥候选值的排序变化曲线所围面积

图 5.3 侧信道攻击所得真实密钥与其它密钥候选值的分数及排序变化曲线，以及排序曲线所围面积

可以发现，图 5.3(b) 中密钥候选值排序越靠前，相应的曲线上点的值越小、下降得越快。当一条曲线中的点呈下降趋势，且越到后来下降速度越快时，可以发现曲线下面所围面积也会剧减。这时曲线与横轴所围部分面积，即曲线的黎曼积分，可视为一个度量指标，用来度量密钥候选值排序位置的上升速度信息。显而易见，曲线的黎曼积分越小，说明曲线下降得越快，相应的密钥候选值排序上升越快。假设曲线上有n个点，且各点坐标分别为$(1, y_1), (2, y_2), \cdots, (n, y_n)$，则曲线与横轴所围部分面积可通过计算曲线的黎曼积分得到，其表达式如下：

$$S = \sum_{i=1}^{n} y_i - \frac{(y_1 + y_n)}{2} . \tag{5-1}$$

图 5.3(c) 给出了图 5.3(b) 中所有曲线的黎曼积分。可以观察到，当分析者可利用的侧信息较充足时，使用式 5-1 中的指标来区分真实密钥和其它密钥候选值，效率未必比直接按密钥候选值分数或排序区分高。例如在图 5.3(c) 中当侧信息泄漏数目达到35条时真实密钥才排在第一位，而在图 5.3(a) 或图 5.3(b) 中25条就排在了第一位。但当分析者可利用的侧信息泄漏信号数目很少时，例如少于20条时，图 5.3(c) 中真实密钥始终排在前几位，而在图 5.3(a) 或图 5.3(b) 中则在十几位，甚至更远。

鉴于此，我们将密钥的排序位置信息与密钥排序位置变化所成曲线的积分结合起来构成新的指标，以期其能在多种情形下有效提升真实密钥在所有密钥候选值中的排序、改善区分效果。下面首先给出一种基于密钥排序及排序积分的加权算法。

5.2.1 基于密钥排序及排序积分的加权算法

在上述讨论的基础上，我们综合考虑真实密钥在所有密钥候选值中的排序位置信息及其排序位置变化所成曲线的积分这两种度量指标，来提升真实密钥在所有密钥候选值中的排序。比较简单地，可对上述两个指标加权得到一个新的指标来考察真实密钥的排序信息。据此，我们提出了一种基于密钥排序及排序积分的加权算法，即在侧信道攻击获得的所有密钥候选值的排序位置信息基础上，计算随着侧信道泄漏信号数目增加，每个密钥候选值的排位变化所成曲线的积分，然后按照这些积分值的大小对所有密钥候选值排序，随后对同一密钥候选值新得到的排序与侧信道攻击得到的排序进行加权（即密钥排序的权重随着泄漏信号的增多而变大，而密钥排序积分的权值则随泄漏信号数目减少而变大），最后获得所有密钥候选值的新的排序。算法 9 给出了基于密钥排序及排序积分的加权算法的具体步骤。

在得出新的各个子密钥所有候选值的排序后，可以使用最优密钥枚举算法或者其改进算法 [115]进行攻击，从而减少最优密钥枚举算法所需内存及运行时间。如果我们的算法对真实子密钥的排序提升很大，不仅会大大减少最优密钥枚举算法的性能限制，甚至直接进行暴力穷搜也未必不可行。本节所提方法需要选择合适的最小泄漏信号数目，因为过少的泄漏信号数目得到的排序结果一般不好，会拉低泄漏信号数目增大带

Algorithm 9 基于密钥排序及排序积分的加权算法

输入： 数目为N的侧信道泄漏信号集合Q，攻击所使用的最小泄漏信号数目N_1，步长N_2，主密钥所分成的子密钥数目m，子密钥候选值空间K，及权重系数ω_1, ω_2

输出： 各个子密钥所有候选值的排序R

$i \leftarrow N_1, t \leftarrow 1, R \leftarrow \emptyset, R = \bigcup_{j=1}^{m}\{R_j\}$
while $i \leq N$ **do**
    从Q中选择前i条泄漏信号
    for $j = 1, 2, \ldots, m$ **do**
        for $k = 1, 2, \ldots, |K|$ **do**
            进行侧信道攻击，得到第j个子密钥的第k个候选值的分数
        end for
        得到并保存第j个子密钥的每个候选值的第t次排序$R_{j,t}$
        $R_j \leftarrow R_j \cup R_{j,t}$
    end for
    $i \leftarrow i + N_2, t \leftarrow t + 1$
end while
for $j = 1, 2, \ldots, m$ **do**
    for $k = 1, 2, \ldots, |K|$ **do**
        计算第j个子密钥的第k个候选值的位置变化曲线的积分
    end for
    根据上一步计算所得每个候选值的位置变化曲线的积分，得到并保存第j个子密钥的每个候选值的积分排序RS_j
    $R_j \leftarrow \omega_1 R_j + \omega_2 RS_j$
end for
返回： 各个子密钥所有候选值的排序R

来的提升效果，从而削弱该方法的提升效率。但最小泄漏信号数目如何选择，目前只能依靠经验判断。为了进一步提高真实子密钥的排序，我们将可利用的密码芯片的侧信道泄漏数目固定在一个较大的值，提出了另一种方法。下面详细介绍该方法。

5.2.2 基于密钥排序积分的随机多次平均算法

假设我们使用相同数目的不同样本来估计同一分布总体的熵或信息量，那么结果应该很接近。换言之，服从同一分布的相同数目的不同样本包含的信息量理论上应该是一样的。因密码芯片的侧信息泄漏依赖于真实密钥，所以若我们假设真实密钥排序服从某一分布，那么在由已知相同数目的不同泄漏信号集合实施的多次攻击中，真实密钥排序的位置都应该很接近，相对其它的密钥候选值排序变化也应最小。基于此思

Algorithm 10 基于密钥排序积分的随机多次平均算法

输入： 数目为N的侧信道泄漏信号集合Q，随机选择的泄漏信号数目N_1，实验重复次数N_2，子密钥候选值空间K

输出： 各个子密钥所有候选值的排序R

$R \leftarrow \emptyset, R = \bigcup_{j=1}^{m}\{R_j\}$
for $t = 1, 2, \cdots, N_2$ **do**
    从Q中选择随机选择N_1条泄漏信号
    for $j = 1, 2, \ldots, m$ **do**
        for $k = 1, 2, \ldots, |K|$ **do**
            进行侧信道攻击，得到第j个子密钥的第k个候选值的分数
        end for
        得到并保存第j个子密钥的每个候选值的第t次排序$R_{j,t}$
        $R_j \leftarrow R_j \cup R_{j,t}$
    end for
end for
for $j = 1, 2, \ldots, m$ **do**
    for $k = 1, 2, \ldots, |K|$ **do**
        计算第j个子密钥的第k个候选值的位置变化曲线的积分
    end for
    根据上一步计算所得每个候选值的位置变化曲线的积分，得到并保存第j个子密钥的每个候选值的积分排序RS_j
    $R_j \leftarrow RS_j$
end for
返回： 各个子密钥所有候选值的排序R

想，我们提出了基于密钥排序积分的随机多次平均算法来提升各个真实子密钥在各自候选值集合中的排序。我们随机选择一定数量的侧信道泄漏信号，多次计算各个子密钥所有候选值的排序，观察并使用一个指标来度量各个子密钥候选值中排序位置变化，随后据其变化从小到大排列，得到新的各个子密钥候选值的排序。这里我们依然使用式 5-1 作为度量指标。算法 10 给出了上述方法的细节。

该方法需要多次随机选择一定数目的侧信道泄漏信号，而且重复实验的次数越多越好（如100次），少了则样本太少、近似总体分布的误差大，导致结果不稳定。图 5.4 经验性地给出了该方法所得结果随重复实验的次数变化的一个例子。注意，真实密钥的位置由最优枚举算法的改进版本 [115]计算得到。同时，为了更加清晰地考察我们所提方法的性能，图中超出目前计算能力2^{50}的部分则是在已知密钥的前提下使用密钥排

序技术 [115]求得。从图中可见只要平均次数足够，算法 10 就能收敛。实验所用的泄漏集合是一个实现在8-bit 单片机上的AES-128算法第一轮S盒输出的电磁泄漏。该泄漏信号集合共包含80条电磁迹，我们每次随机从中选择75条泄漏信号运行算法 10。该方法应尽可能多地选择泄漏信号数目，以便尽可能地利用泄漏信息来提升真实密钥的排序。但同时所选泄漏信号数目不应过于接近总的泄漏集合大小，以免每次所选泄漏信号相关太大，导致算法失效。例如，假设我们每次从上述AES-128实现的80条泄漏信号选75条来运行该算法，平均100次所得真实密钥的排序为$2^{13.0718}$，而若选择80条泄漏信号得到的结果$2^{111.8205}$，还不如使用10条泄漏信号重复100次得到的结果$2^{103.6327}$好。

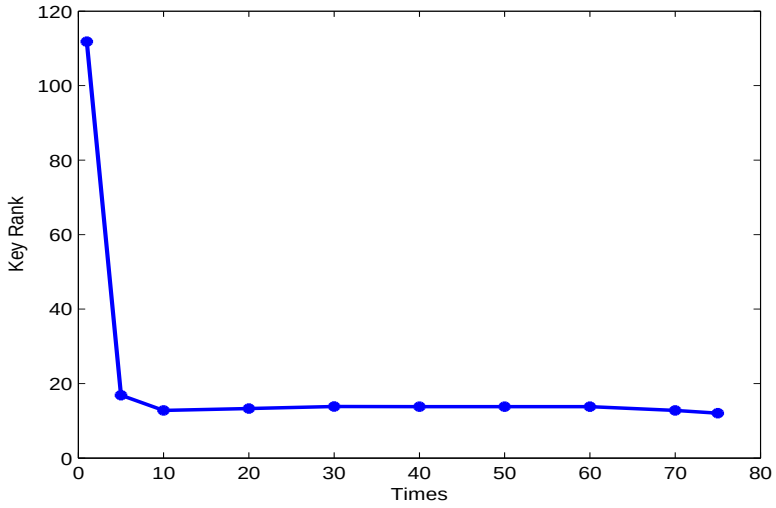
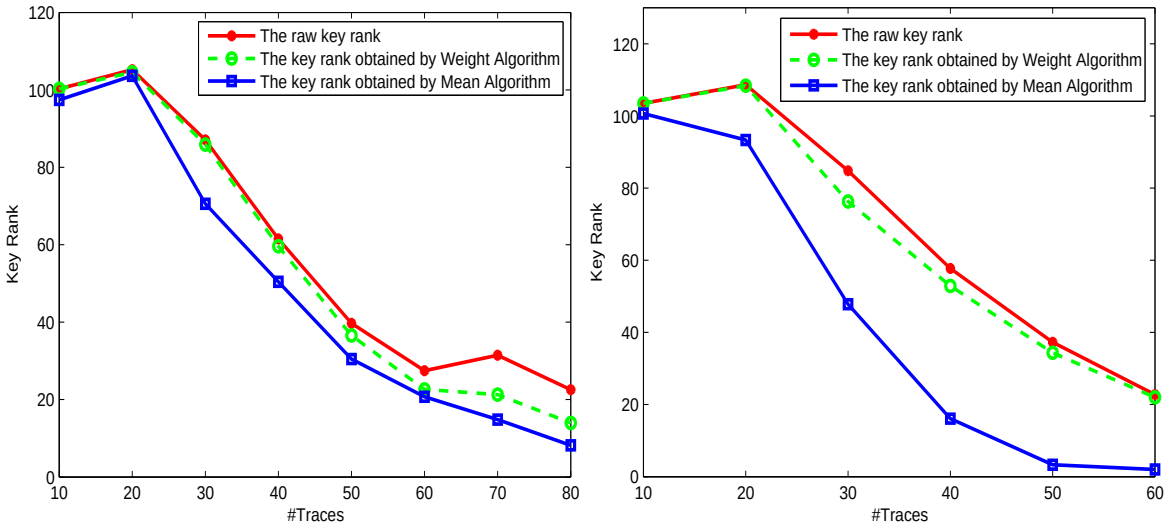


图 5.4 基于密钥排序积分的随机多次平均算法所得真实密钥排序位置随重复次数变化曲线

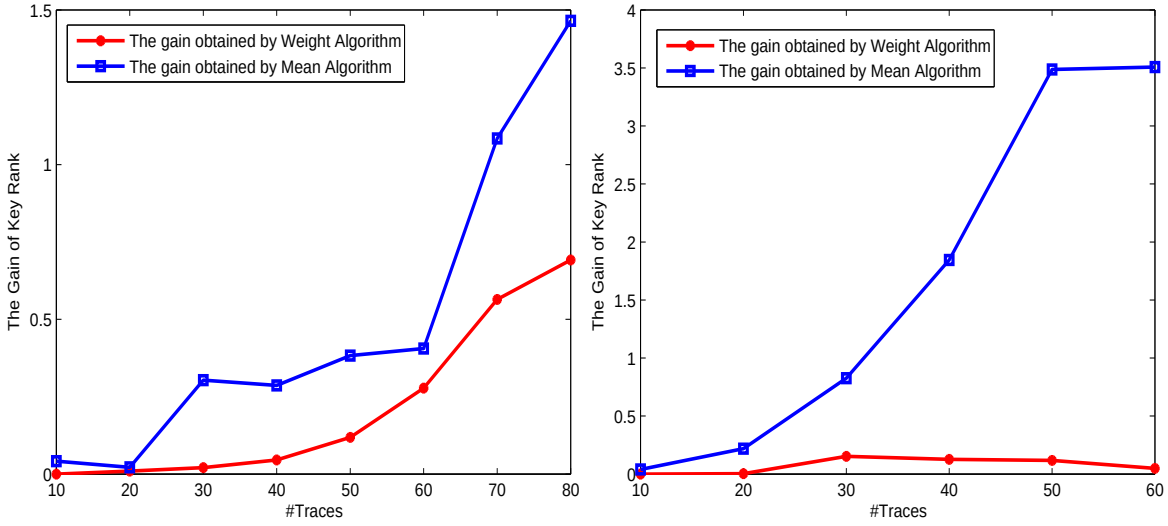
图 5.5(a) 和图 5.5(b) 分别给出了基于密钥排序及排序积分的加权算法（图中中文简写为加权算法，英文简写为Weight Algorithm）和基于密钥排序积分的随机多次平均算法（图中中文简写为平均算法，英文简写为Mean Algorithm）的性能对比。图 5.5(a) 和图 5.5(b) 实验所用的数据分别是一个实现在8-bit单片机上的AES-128算法（第一个S盒加布尔掩码）第一轮S盒输出的电磁泄漏（总条数80条）和能量泄漏（总条数60条）。在使用基于密钥排序及排序积分的加权算法时，密钥排序的权重随着泄漏信号数目的增多而变大，而密钥排序积分的权重则随泄漏信号数目减少而变小，以充分利用二者优势，提高算法性能。在两个实验中，这两个指标权重随着泄漏信号数目变化而轮流取为0.4或0.6，且算法起始值与泄漏信号总数总相差20条，步长都设置为10。而基于密钥排序积分的随机多次平均算法每次平均100次来获取一个稳定的结果。可以看出，两种方法都提高了真实密钥在所有密钥候选值中的排序位置。如果在此基础上再使用最优密钥枚举算法进行密钥枚举，将显著提高最优密钥枚举算法的效率。而且，相对基于密钥排序及排序积分的加权算法，基于密钥排序积分的随机多次平均算法对真实密钥排序位置的提升更为显著。在图 5.5(a) 中，当泄漏信号数目达到77条时，使用平均算法仅需枚举$2^{8.1699}$次，此时只有4个子密钥排序不在第一位。而在 5.5(b) 中，当泄漏信号

数目达到50条时，甚至仅需枚举$2^{3.3219}$次，此时仅2个子密钥排序不在第一位，即使暴力穷搜也仅需65536次枚举；当泄漏信号数目达到57条时，只需枚举2次，仅1个子密钥排序不在第一位，只暴力穷搜也仅需256次枚举。另外值得注意的是，当真实密钥在密钥候选值中的排序位置较为靠后时，基于密钥排序积分的随机多次平均算法甚至能将真实密钥的排序拉至攻击者所能承受的枚举能力范围内。



(a) 使用电磁信号泄漏条件下的结果　　(b) 使用能量泄漏信号条件下的结果

图 5.5　针对AES-128 MCU实现加权算法和平均算法使用前后真实密钥排序位置变化

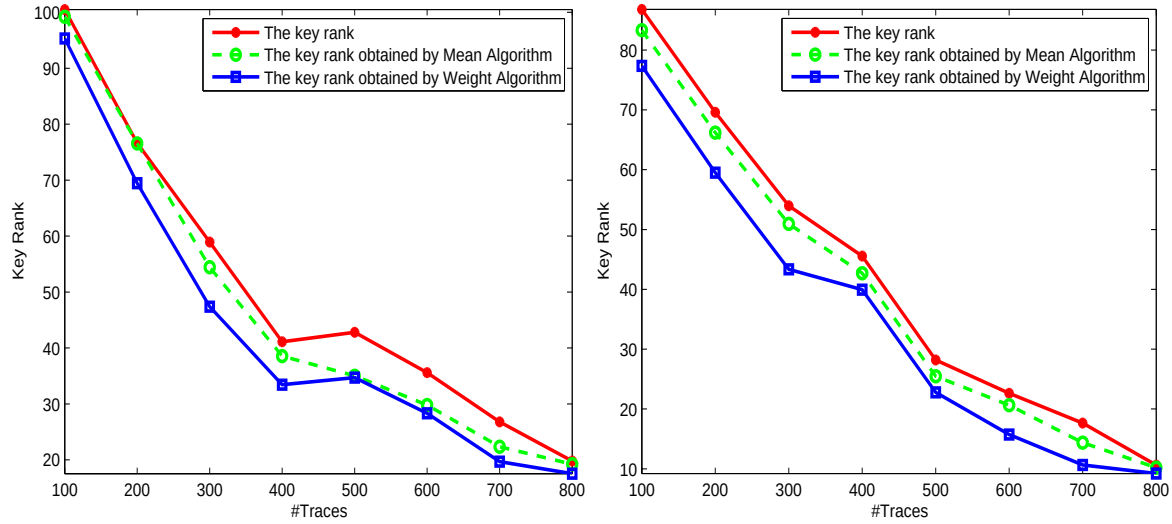


(a) 使用电磁信号泄漏条件下的结果　　(b) 使用能量泄漏信号条件下的结果

图 5.6　针对AES-128 MCU实现加权算法和平均算法对真实密钥排序位置的提升效果

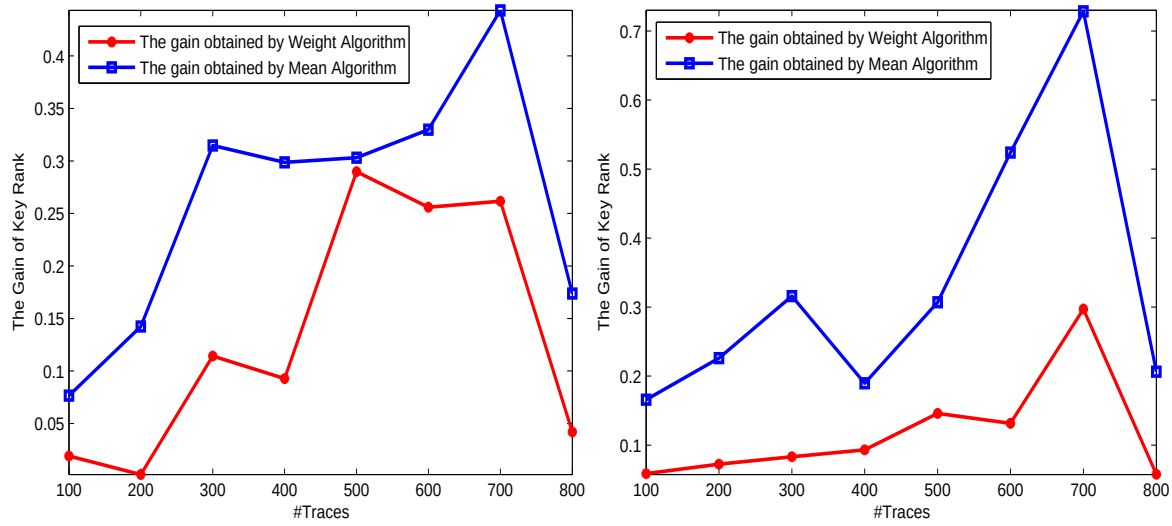
图 5.6(a) 和图 5.6(b) 分别给出了两种算法关于真实密钥排序位置的增益。该增益指标的形式化表达为$\log_2(I_0/I_1)$，其中I_0表示真实密钥在所有密钥候选值中的原始排序位置，I_1 表示运行两种算法后真实密钥在所有密钥候选值中的新的排序位置。可以发现，

基于密钥排序及排序积分的加权算法在侧信息严重不足导致真实密钥排序很靠后时，对真实密钥排序位置的提升效果微弱，而基于密钥排序积分的随机多次平均算法表现则相对要好。图 5.7 和图 5.8 给出了两种方法针对一个AES-128 FPGA实现的分析，结果与上述AES-128 8-bit 单片机实现类似，不再赘述。



(a) 使用电磁信号泄漏条件下的结果　　(b) 使用能量泄漏信号条件下的结果

图 5.7　针对AES-128 FPGA实现加权算法和平均算法使用前后真实密钥排序位置变化



(a) 使用电磁信号泄漏条件下的结果　　(b) 使用能量泄漏信号条件下的结果

图 5.8　针对AES-128 FPGA实现加权算法和平均算法对真实密钥排序位置的提升效果

5.3　密钥排序技术研究

当真实密钥在密钥候选值中的排序位置较为靠后，即使使用了我们提出的算法，依然不能将真实密钥的排序提升至分析者的计算能力之内时，要对密码芯片安全水平

进行评估，就只能在知道主密钥信息的前提下，使用密钥排序技术。如前所述，目前关于密钥排序技术的研究除了文献 [25,124]之外，都是基于文献 [14]的思想发展而来，也即它们首先基于最大似然准则对所有密钥候选值进行排序，然后估计真实密钥的排序位置。实际上，在已知密钥的前提下，利用子密钥候选值的位置排序来估计真实主密钥位置比利用子密钥候选值的后验概率排序来估计真实主密钥位置更高效 [21,25,124]。所以本章关注的是利用子密钥候选值的位置排序来估计真实主密钥位置的密钥排序技术。

已有的研究中，文献 [124] 从子密钥的枚举成功率出发，以使主密钥的恢复成功率达到或超过某个预设值为条件限制，以枚举次数最小化为目标，来评估一个密码实现的安全水平。而文献 [25]与文献 [124]中的算法相反，是以枚举次数最小化为条件限制，以最大化主密钥的恢复成功率为目标，相比后者更为合理。不过该算法为了提高效率，使用了基于均匀采样的降采样技术，要求子密钥的成功率与子密钥枚举次数之间的曲线平滑且单调递增，否则可能采样失真、影响评估精度。本节在文献 [25]的基础上，改进了其所使用的降采样技术，以期消除文献 [25]方法的限制，提高评估精度。本节所提出的算法描述如下。

5.3.1 基于信号整数倍抽取与插值的密钥排序算法

文献 [25]中的基本思路是：在可利用的密码芯片侧信道泄漏信号数目固定的情况下，得到各个子密钥枚举次数与子密钥恢复成功率的关系曲线，然后对得到的所有关系曲线均匀降采样，使每个子密钥对应曲线采集到相同的点数N_{max}，得到N_{max}个点对$(s_{i,1},c_{i,1}),\ldots,(s_{i,N_{max}},c_{i,N_{max}})$。其中$(s_{i,1},c_{i,1})$表示在一定泄漏信号数目下，第$i$个子密钥经过$c_{i,1}$次枚举后，子密钥被恢复的概率为$s_{i,1}$。随之从第一个子密钥开始，从第一个点对开始依次与第二个子密钥对应的所有点对结合，依次类推，直到遍历完所有点对。之后按照相同的枚举次数合并成功率，并重新进行降采样得到N_{max} 点，用来表示枚举次数与第一个及第二个子密钥恢复的联合成功率的曲线，并与下一个子密钥结合，如此往复，直至遍历完所有子密钥。最后，该算法会得到一条枚举次数与主密钥恢复成功率的曲线，来反映密码芯片的安全水平。可以看出，该算法是基于子密钥候选值的位置排序进行枚举，更符合实际，效率也较基于子密钥候选值的后验概率排序的方法高。该算法通过只取N_{max}个点对，排除了一些于枚举意义不大的点，提高了密钥排序的效率，但唯一影响算法性能的也是降采样环节。一方面若采样率过小，可能会造成信号失真，过大则有冗余；另一方面，如果子密钥的成功率与子密钥枚举次数之间的曲线并不满足平滑且单调递增的条件，该算法可能会丢失不少细节信息。本小节改进了上述算法的降采样环节，通过使用信号整数倍抽取与插值来防止或减少采样失真，并最大限度地降低采样点数。

如第 5.1.3.2 小节所述，为了防止信号失真，需对信号先插值、后抽取。假设一个

Algorithm 11 基于信号整数倍抽取与插值的密钥排序算法

输入： 各个子密钥枚举次数与及子密钥恢复成功率组成的$|K|$个点对，信号整数倍抽取倍数D及插值倍数I

输出： 主密钥枚举次数与主密钥恢复成功率关系曲线$SR_{1:m}$

for $i = 1, \ldots, m$ **do**
    对第i个子密钥枚举次数与成功率关系曲线进行I倍信号插值
    对第i个子密钥枚举次数与成功率关系曲线进行D倍信号抽取，得到N_{max}个点对
    $SR_i \leftarrow \{(s_{i,1}, c_{i,1}), \ldots, (s_{i,N_{max}}, c_{i,N_{max}})\}$
end for
for $i = 2, 3, \ldots, m$ **do**
    $SR_{1:i} \leftarrow \emptyset$
    for all $(s_j, c_j) \in SR_{1:i-1}$ **do**
        for all $(s_{i,k}, c_{i,k}) \in SR_i$ **do**
            $SR_{1:i} \leftarrow SR_{1:i} \cup (s_j s_{i,k}, c_j c_{i,k})$
        end for
    end for
    对$SR_{1:i}$排序，并进行I倍插值
    if $i < m$ **then**
        对$SR_{1:i}$再进行D倍信号抽取，得到N_{max}个点对
    end if
end for
返回： 主密钥枚举次数与主密钥恢复成功率关系曲线

密码实现中，主密钥可分为m个子密钥，各个子密钥的候选值有$|K|$个，那么每个子密钥枚举次数与子密钥恢复成功率组成的点对都有$|K|$个。令符号$SR_i = \{(s_i, c_i)\}$表示第i个子密钥枚举次数与子密钥恢复成功率的关系曲线，$SR_{i:j}$表示枚举次数与第i, j个子密钥恢复的联合成功率的关系曲线，则$SR_{1:m}$表示主密钥枚举次数与主密钥恢复成功率的关系曲线。本小节所提方法的细节如算法 11 所示。

5.3.2 基于子密钥相关的密钥排序算法

可以发现，以上所讲密钥排序算法都是建立在组成主密钥的各个子密钥相互独立的假设基础上，所以主密钥的枚举次数与成功率的关系分别由各个子密钥的枚举次数的乘积与成功率的乘积构成。这实际上是认为在求各个子密钥枚举次数与成功率的过程中，各个子密钥是独立操作，甚至可以使用相同数目的不同侧信道泄漏信号集合分别求得。而实际中，我们使用侧信道攻击对一个主密钥的所有子密钥时，一般会使用同一组泄漏信号集合进行攻击（当然利用的信息不同），而不会在恢复每个子密钥时再

分别使用不同的泄漏数据信号集合。换言之，实际求各个子密钥枚举次数与成功率的过程中，各个子密钥之间并不是完全独立的。

以上两种情形是有区别的。举个例子，以上第一种情形相当于在实际中投一个骰子，分别投多次，然后看投中某一值的事件发生了几次，再投第二个骰子，看投中某一值的事件发生了几次，最后计算第一次投中某一值且第二次投中某一值的概率——这个概率自然是两个事件发生概率的乘积；第二种情形则相当于同时投两个骰子，看每次第一个骰子投中某一值且第二个骰子投中某一值同时发生的概率——这个概率要看符合要求的事件在全体事件中所占的比例。具体地，假设第一种情形下，第一个骰子投了10次，其中投中1和2各1次，第二个骰子也投了10次，其中投中4、5和6各1次，那么第一个骰子投中值在1～2之间且第二个骰子投中值在4～6之间的概率是$0.2\times0.2 = 0.04$。同样地，假设第二种情形下，同时投两个骰子10次，其中第一个骰子出现1和2各1次，第二个骰子出现4、5和6各1 次，那么每次第一个骰子投中值在1 ～2 之间且第二个骰子投中值在4～6之间的概率是$2/10 = 0.2$。简而言之，第二种情形考虑了子密钥间的相关信息，可以用来从另一个角度来考察密钥排序并评估密码芯片的安全水平。据此，我们提出了基于子密钥相关的密钥排序技术。该算法思路如下：

我们首先随机从泄漏信号集合中抽取一定数目的泄漏信号，分别对各个子密钥进行恢复，得到各个子密钥在其所有候选值中的排序，之后将各个排序位置相乘即得到主密钥的最少枚举次数（也即密码芯片的最坏安全水平）。重复实验多次，得到真实主密钥所需枚举次数的记录，即可得到主密钥枚举次数与主密钥恢复成功率的关系曲线。需要注意的是，该密钥排序算法考察的是密码芯片的最坏安全水平，因为实际分析中若无法知道主密钥，是不可能知道主密钥枚举到多少次恰好是合适的。算法 12 给出了密钥排序算法的执行流程。为了使数据更平滑、丰富，我们对主密钥枚举次数与主密钥恢复成功率的关系曲线进行了信号整数倍插值处理。

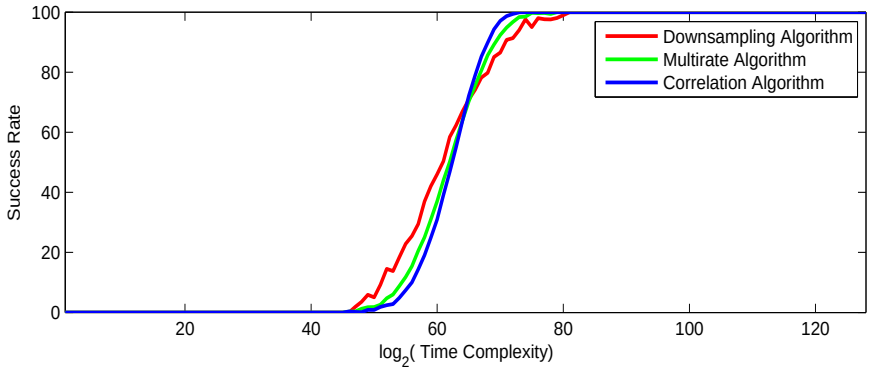
图 5.9 分别给出了文献 [25]中的基于降采样的密钥排序算法（图中中文简写为降采样算法，英文简写为Downsampling Algorithm）、基于信号整数倍抽取与插值的密钥排序算法（图中中文简写为多抽样率算法，英文简写为Multirate Algorithm）及基于子密钥相关的密钥排序算法（图中中文简写为相关算法，英文简写为Correlation Algorithm）的性能对比。其中，图 5.9(a) 实验所使用的数据是一个实现在FPGA上的无保护AES-128算法最后一轮S 盒输入输出异或值的电磁泄漏信号（总条数100 条），而图 5.9(b) 实验所使用的数据是另一个实现在FPGA上的有保护AES-128算法最后一轮S 盒输入输出异或值的能量泄漏信号（总条数100条）。该AES-128 掩码实现方案与第 2.5 小节所用掩码方案一样。实验中基于信号整数倍抽取与插值的密钥排序技术都是先对每个子密钥成功率曲线进行$I = 2$倍的插值，然后进行$D = 7$倍的抽取。而且我们对基于子密钥相关的密钥排序算法的最终结果进行了$I = 1$倍的插值，使其更光滑。从图中可以看出，相比文献 [25]所提算法所得的成功率曲线，基于信号整数倍抽取与插值的密钥排

Algorithm 12 基于子密钥相关的密钥排序算法

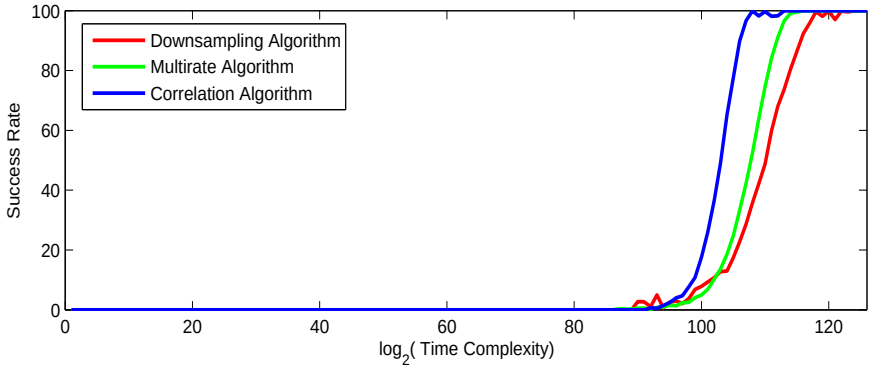
输入： 侧信道泄漏信号集合Q，随机选择的泄漏信号数目N_1，实验重复次数N_2，信号整数倍插值倍数I

输出： 主密钥枚举次数与主密钥恢复成功率关系曲线

$C_t \leftarrow 1, S_t \leftarrow 0, C \leftarrow \emptyset,$
for $t = 1, 2, \cdots, N_2$ **do**
    从Q中选择随机选择N_1条泄漏信号
    for $i = 1, \ldots, m$ **do**
        得到第i个子密钥在所有候选值中的排序位置c_i
        $C_t \leftarrow C_t c_i$
    end for
end for
$C \leftarrow C \cup C_t$
返回： 对C排序，并进行I倍插值，得到主密钥枚举次数与主密钥恢复成功率之间的关系曲线



(a) 使用无保护AES-128 FPGA实现电磁信号泄漏条件下的结果



(b) 使用有保护AES-128 FPGA实现能量信号泄漏条件下的结果

图 5.9 降采样算法、多抽样率算法与相关算法所得时间复杂度与主密钥恢复成功率关系曲线对比

序技术所得成功率曲线波动明显小很多，精度上更高。从图上同样能观察到时间复杂度（即主密钥枚举次数）与主密钥恢复成功率的关系。基于此，我们可以对密码芯片的安全水平作出估计。不过，基于子密钥相关的密钥排序算法给出的是最坏情况下密码芯片的安全水平。

通过密钥排序技术，我们可以得到一定测量复杂度（即泄漏信号数目）下，成功率与时间复杂度（即枚举次数）的关系曲线，从而可以让分析者或设计者了解到密码芯片的安全水平，并在对敌手的计算能力有所判断的前提下，判断敌手在将侧信道攻击与枚举技术联合的情况下，泄漏多少信息是可以容忍的，以及泄漏多少信息就应该及时更换密钥。因此，密钥排序技术对密码芯片的实际设计及应用具有重要意义，业已成为一个重要研究内容 [115]。

5.4 本章小结

本章研究了侧信息不足场景下的密码芯片安全水平的分析与检测技术，涉及了两个问题：密钥枚举问题和密钥排序问题。其中，现有的密钥枚举问题虽然已经有概率论意义上最优的密钥枚举算法，然而这类算法只是根据真实密钥联合概率的大小进行枚举。它们虽致力于提高枚举效率，但从未触及影响密钥枚举效率的根本问题，即如何提高真实密钥排序的位置，进而从根本上加速密钥枚举效率。本章对此做了研究，提出了两种通过提升真实子密钥排序位置来整体提升真实主密钥排序位置的算法。之后，本章对密钥排序问题也做了研究，比较了按密钥位置排序来估计真实主密钥位置和按密钥后验概率来估计真实主密钥位置的不同之处，并改进了一个现有的密钥排序算法。最后，本章提出了一种基于子密钥相关的密钥排序算法。该算法能评估最坏情况下密码芯片的安全水平。下一步，我们将会重点研究如何进一步提高本章所提密钥枚举算法及密钥排序算法的性能。

第六章　总结与展望

自差分能量分析提出以来，侧信道攻击对密码芯片的物理安全性已然构成严重威胁。针对密码芯片的侧信道分析与检测技术的研究也越来越受到国内外学术界及产业界的广泛关注和重视，展现出重大的学术和应用价值。

6.1　本文工作总结

本文围绕密码芯片的侧信道分析与检测技术分别展开研究，重点研究了泄漏信号对齐技术、多信道融合攻击技术、泄漏评估与泄漏检测技术，以及密钥枚举与密钥排序技术，取得了如下成果：

首先，本文较系统地研究了泄漏信号对齐技术，并从信息利用方式的角度将泄漏信号对齐技术分为两类：局部对齐技术和全局对齐技术，籍此在一个框架下研究了泄漏信号对齐技术。本文还分别提出了一种基于*shotgun*距离的局部泄漏信号对齐算法和一种基于加权编辑距离的全局泄漏信号对齐算法，并在多种常见密码芯片类型上及不同噪声环境下验证了它们的性能。总体上看，这两种方法在各方面的表现都超出了已有经典对齐算法。在目前所知有关泄漏信号对齐研究中，本文研究较为系统全面，能够为研究高效的泄漏信号对齐技术提供参考借鉴。

其次，本文将多信道融合攻击分为三类：数据级融合攻击、特征级融合攻击及决策级融合攻击，并在此框架下提出了六种多信道融合攻击算法，研究了不同种类多信道融合攻击在同一密码算法的不同实现下的性能表现，同时考察了不同融合方式对多信道融合攻击效率的影响。此外，本文提出了一个度量标准，用于判断不同信道是否宜于实施融合攻击。该度量指标较已有指标的实用性更强。总体上讲，本文的研究工作较为系统全面，有助于深入理解多信道融合攻击，能够为如何进行多信道融合攻击提供建议和帮助，推动了多信道融合攻击技术的发展。

随后，本文根据已有泄漏评估技术或者效率较高但精度不高、或者精度高但需要大量数据刻画的问题，综合二者优点，在侧信道通信信道模型的基础上，分别针对不同的噪声类型，较为高效、准确地评估了密码芯片的泄漏量，并提供了密码芯片泄漏量的粗糙上界。另外，我们发现如果将侧信道通信信道模型的信道特性与统计中的一致性检验结合，可以有效地检测出密码芯片侧信道泄漏信号中依赖于秘密信息的泄漏特征点。该泄漏检测技术效率很高，对泄漏信号的采集没有特殊要求，且检测出的泄漏特征点基本是POIs，能直接用于CPA攻击。这是目前很多泄漏检测技术（如基于T-test的泄漏检测技术）无法做到的。

最后，本文研究了侧信息不足场景下的密钥枚举技术及密钥排序技术。本文根据

目前密钥枚举算法只能按照密钥排序进行枚举，不能提升真实密钥排序位置的特点，提出了两种可以提升真实密钥排序位置的算法。本文方法能从根本上提高密钥枚举的效率。在对密钥排序技术的研究中，本文提出了两种利用子密钥候选值的位置排序来估计真实主密钥位置的算法。其中一种是对已有算法的改进，另一种则基于子密钥相关性来估计真实密钥排序位置，能评估最坏情况下密码芯片的安全水平。

6.2 下一步研究方向

虽然本文在密码芯片侧信道分析与检测方面取得了一定的研究成果，但仍有一些问题值得深入研究。在本文基础上，可从以下四点进一步拓展目前的研究。

一、本文提出的关于泄漏信号对齐的预处理技术，能被用来消除一些典型隐藏防御对策所引发的泄漏信号失调的影响。但在对同时采用了隐藏和掩码防御对策的密码芯片进行分析时，本文方法需要了解所用掩码信息。这在实践中可能难度不小。因此，我们希望在未来研究中消除这一限制。此外，我们也希望能对同时采用了更多不同种类防御对策的密码芯片展开分析，以期加强目前学术界关注较少的面向组合防御对策的预处理技术的研究。

二、本文关于多信道融合攻击的研究要求密码芯片所有侧信道的泄漏信号采样率相同，且每个侧信道泄漏函数已知。如果能更好地解决最优采样率不同及泄漏函数未知的多个信道的融合攻击问题，将会进一步推进多信道融合攻击的研究。

三、本文对第 4.4 节提出的四个扩展问题并未进行详细分析，且在对泄漏信号不做预处理的情况下，也未解决掩码实现方案的泄漏评估与检测问题。如果能解决以上问题，将会对拓展目前工作产生积极意义。

四、在对密钥枚举的研究中，本文所提方法只利用了两个指标，即密钥的排序位置及密钥排序位置变化所成曲线的积分。我们希望以后能结合新的指标，来进一步提升真实密钥排序位置，提高密钥枚举效率。另外在对密钥排序的研究中，本文虽然提出了基于子密钥相关性的密钥排序算法，但其只能给出最坏情况下密码芯片的安全水平。我们希望以后继续改进该方法，使之能更精细地检测密码芯片的安全水平。

参考文献

[1] P. C. Kocher, “Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems,”, in *Proc. CRYPTO 1996*, Santa Barbara, California, USA, Aug. 1996, pp. 104–113.

[2] P. C. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,”, in *Proc. CRYPTO 1999*, Santa Barbara, California, USA, Aug. 1999, pp. 388–397.

[3] K. Gandolfi, C. Mourtel, and F. Olivier, ”Electromagnetic Analysis: Concrete Results,”, in *Proc. CHES 2001*, Paris, France, May 2001, pp. 251-261.

[4] D. Genkin, A. Shamir, and E. Tromer, “RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis,”, in *Proc. CRYPTO 2014*, Santa Barbara, California, USA, Aug. 2014, pp. 444–461.

[5] G. M. Bertoni, L. Grassi, and F. Melzani, “Simulations of Optical Emissions for Attacking AES and Masked AES,”, in *Proc. SPACE 2015*, Jaipur, Rajasthan, India, Oct. 2015, pp. 172–189.

[6] E. Carmon, J.-P. Seifert, and A. Wool, “Simple Photonic Emission Attack with Reduced Data Complexity,”, in *Proc. COSADE 2016*, Graz, Austria, Apr. 2016, pp. 35–51.

[7] E. Carmon, J.-P. Seifert, and A. Wool, “Photonic Side Channel Attacks Against RSA,”, *IACR Cryptology ePrint Archive*, vol. 2017, pp. 108, Feb. 2017.

[8] M. Matsui, “Linear cryptanalysis method for DES cipher,”, in *Proc. EUROCRYPT 1993*, Lofthus, Norway, May 1993, pp. 386–397.

[9] A. A. Selçuk, “On probability of success in linear and differential cryptanalysis,”, *J. Cryptol.*, vol. 21, no. 1, pp. 131–147, Jan. 2008.

[10] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: revealing the secrets of smart cards*. New York, USA: Springer, 2007.

[11] (2015, Aug.) FIPS 140-3. [Online]. Available: http://csrc.nist.gov/groups/ST/FIPS140_3/

[12] (2012, Nov.) GM/T 0008-2012. [Online]. Available: http://www.oscca.gov.cn/Column/Column_32.htm

[13] F.-X. Standaert, T.G. Malkin, and M. Yung, “A unified framework for the analysis of side-channel key recovery attacks,”, in *Proc. EUROCRYPT 2009*, Cologne, Germany, Apr. 2009, pp. 443-461.

[14] N. Veyrat-Charvillon, B. Gérard, and F.-X. Standaert, “Security evaluations beyond computing power,”, in *Proc. EUROCRYPT 2013*, Athens, Greece, May 2013, pp. 126–141.

[15] D. Agrawal, J. Rao, and P. Rohatgi, “Multi-Channel Attacks,”, in *Proc. CHES 2003*, Cologne, Germany, Sep. 2003, pp. 2–16.

[16] W. Yang, Y. Zhou, Y. Cao, H. Zhang, and Q. Zhang, “Multi-channel fusion attacks,”, *IEEE Trans. Info. Foren. Sec.*, vol. 12, no. 8, pp. 1757–1771, Aug. 2017.

[17] F. Durvaux and F.-X. Standaert, “From improved leakage detection to the detection of points of interests in leakage traces,”, in *Proc. EUROCRYPT 2016*, Vienna, Austria, May 2016, pp. 240–262.

[18] T. Schneider, A. Moradi, F.-X. Standaert, and T. Güneysu, “Bridging the gap: Advanced tools for side-channel leakage estimation beyond gaussian templates and histograms,”, *IACR Cryptology ePrint Archive*, vol. 2016, pp. 719, Jul. 2016.

[19] V. Grosso and F.-X. Standaert, “Asca, SASCA and DPA with enumeration: Which one beats the other and when,”, in *Proc. ASIACRYPT 2015*, Auckland, New Zealand, Dec. 2015, pp. 291–312.

[20] N. Veyrat-Charvillon, B. Gérard, M. Renauld, and F.-X. Standaert, “An optimal key enumeration algorithm and its application to side-channel attacks,”, in *Proc. SAC 2012*, Windsor, Ontari, Canada, Aug. 2012, pp. 390–406.

[21] R. Poussier, V. Grosso, and F.-X. Standaert, “Comparing approaches to rank estimation for side-channel security evaluations,”, in *Proc. CARDIS 2015*, Bochum, Germany, Nov. 2015, pp. 125–142.

[22] C. Glowacz, V. Grosso, R. Poussier, J. Schüth, and F.-X. Standaert, “Simpler and more efficient rank estimation for side-channel security assessment,”, in *Proc. FSE 2015*, Istanbul, Turkey, Mar. 2015, pp. 117–129.

[23] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, “Towards sound approaches to counteract power-analysis attacks,”, in *Proc. CRYPTO 1999*, Santa Barbara, California, USA, Aug. 1999, pp. 398–412.

[24] T. D. Cnudde, O. Reparaz, B. Bilgin, S. Nikova, V. Nikov, and V. Rijmen, “Masking AES with d+1 shares in hardware,”, in *Proc. CHES 2016*, Santa Barbara, California, USA, Aug. 2016, pp. 194–212.

[25] A. Duc, S. Faust, and F.-X. Standaert, “Making masking security proofs concrete - or how to evaluate the security of any leaking device,”, in *Proc. EUROCRYPT 2015*, Sofia, Bulgaria, Apr. 2015, pp. 401–429.

[26] C.Herbst, E. Oswald, and S. Mangard, “An AES smart card implementation resistant to power analysis attacks,”, in *Proc. ACNS 2006*, Singapore, Jun. 2006, pp. 239–252.

[27] S. Mangard, T. Popp, and B. M. Gammel, “Side-channel leakage of masked CMOS gates,”, in *Proc. CT-RSA 2005*, San Francisco, California, USA, Feb. 2005, pp. 351–365.

[28] A. Moradi and T. Schneider, “Side-channel analysis protection and low-latency in action,”, in *Proc. ASIACRYPT 2016*, Hanoi, Vietnam, Dec. 2016, pp. 517–547.

[29] O. Reparaz, B. Bilgin, S. Nikova, B. Gierlichs, and I. Verbauwhede, “Consolidating masking schemes,”, in *Proc. CRYPTO 2015*, Santa Barbara, California, USA, Aug. 2015, pp. 764–783.

[30] M. Rivain and E. Prouff, “Provably secure higher-order masking of aes,”, in *Proc. CHES 2010*, Santa Barbara, USA, Aug. 2010, pp. 413–427.

[31] N. Veyrat-Charvillon, M. Medwed, S. Kerckhof, and F.-X. Standaert, “Shuffling against side-channel attacks: A comprehensive study with cautionary note,”, in *Proc. ASIACRYPT 2012*, Beijing, China, Dec. 2012, pp. 740–757.

[32] J. G. J. V. Woudenberg, M. F. Witteman, and B. Bakker, “Improving Differential Power Analysis by Elastic Alignment,”, in *Proc. CT-RSA 2011*, San Francisco, CA, USA, Feb. 2011, pp. 104–119.

[33] J. C. Ryoo, D. G. Han, S. K. Kim, and S. Lee, “Performance enhancement of differential power analysis attacks with signal expansion methods,”, *IEEE Signal Process. Lett.*, vol. 15, pp. 625–628, Oct. 2008.

[34] W. Yang, Y. Cao, Y. Zhou, H. Zhang, and Q. Zhang, “Distance based leakage alignment for side channel attacks,”, *IEEE Signal Process. Lett.*, vol. 23, no. 4, pp. 419–423, Jan. 2016.

[35] S. Chari, J. R. Rao, and P. Rohatgi, “Template attacks,”, in *Proc. CHES 2002*, Redwood Shores, California, USA, Aug. 2002, pp. 13–28.

[36] T.-H. Le, J. Clédière, C. Servière, and J.-L. Lacoume, “Noise reduction in side channel attack using fourth-order cumulant.,”, *IEEE Trans. Info. Foren. Sec.*, vol. 2, no. 4, pp. 710–720, Nov. 2007.

[37] M. Rivain, E. Prouff, and J. Doget, “Higher-order masking and shuffling for software implementations of block ciphers,”, in *Proc. CHES 2009*, Lausanne, Switzerland, Sep. 2009, pp. 171–188.

[38] J.-S. Coron and I. Kizhvatov, “Analysis and improvement of the random delay countermeasure of CHES 2009,”, in *Proc. CHES 2010*, Santa Barbara, USA, Aug. 2010, pp. 95–109.

[39] M. Tunstall and O. Benoît, “Efficient use of random delays in embedded software,”, in *Proc. WISTP 2007*, Heraklion, Crete, Greece, May 2007, pp. 27–38.

[40] S. Yang, W. H. Wolf, N. Vijaykrishnan, D. N. Serpanos, and Y. ie, “Power attack resistant cryptosystem design: A dynamic voltage and frequency switching approach,”, in *Proc. DATE 2005*, Munich, Germany, Mar. 2005, pp. 64–69.

[41] Y. Zafar, “A novel countermeasure to resist side channel attacks on fpga implementations,”, *International Journal on Advances in Security*, vol. 2, no. 1, pp. 1–7, Jun. 2009.

[42] Y. Zafar, J. Park, and D. Har, “Random clocking induced dpa attack immunity in FPGAs,”, in *Proc. ICIT*, Viña del Mar, Chile, Mar. 2010, pp. 1068–1070.

[43] R. A. Muijrers, J. Woudenberg, and L. Batina, “RAM: rapid alignment method,”, in *Proc. CARDIS 2011*, Leuven, Belgium, Sep. 2011, pp. 266–282.

[44] P. Hodgers, N. Hanley, and M. O’Neill, “Pre-processing power traces with a phase-sensitive detector,”, in *Proc. HOST 2013*, Austin, TX, USA, Jun. 2013, pp. 131–136.

[45] F. Durvaux, M. Renauld, F.-X. Standaert, LVOT. Oldenzeel, and N. Veyrat-Charvillon, “Cryptanalysis of the CHES 2009/2010 random delay countermeasure,”, *IACR Cryptology ePrint Archive*, vol. 2012, pp. 38, Mar. 2012.

[46] D. Strobel and C. Paar, “An efficient method for eliminating random delays in power traces of embedded software,”, in *Proc. ICISC 2011*, Seoul, Korea, Nov. 2011, pp. 48–60.

[47] Q. Tian, A. Shoufan, M. Stoettinger, and S. A. Huss, “Power trace alignment for cryptosystems featuring random frequency countermeasures,”, in *Proc. ICDIPC 2012*, Klaipeda, Lithuania, July 2012, pp. 51–55.

[48] Q. Tian and S. A. Huss, “A general approach to power trace alignment for the assessment of side-channel resistance of hardened cryptosystems,”, in *Proc. IIH-MSP 2012*, Piraeus-Athens, Greece, Jul. 2012, pp. 465–470.

[49] Q. Tian and S. A. Huss, “On clock frequency effects in side channel attacks of symmetric block ciphers,”, in *Proc. NTMS 2012*, Istanbul, Turkey, May 2012, pp. 1–5.

[50] S. Guilley, K. Khalfallah, V. Lomne, and J. L. Danger, “Formal framework for the evaluation of waveform resynchronization algorithms,”, in *Proc. WISTP 2011*, Heraklion, Crete, Greece, Jun. 2011, pp. 100–115.

[51] C. H. Gebotys, S. Ho, and C. C. Tiu, “EM analysis of rijndael and ECC on a wireless java-based PDA,”, in *Proc. CHES 2005*, Edinburgh, UK, Aug. 2005, pp. 250–264.

[52] P. Hodgers, K. Boey, and M. O’Neill, “Power spectral density side channel attack overlapping window method,”, in *Proc. DSD 2011*, Oulu, Finland, Aug. 2011, pp. 274–278.

[53] C. Clavier, J.-S. Coron, and N. Dabbous, “Differential power analysis in the presence of hardware countermeasures,”, in *Proc. CHES 2000*, Massachusetts, USA, Aug. 2000, pp. 252–263.

[54] T. H. Le, J. Clediere, C. Servière, and J.-L. Lacoume, “Efficient solution for misalignment of signal in side channel analysis,”, in *Proc. ICASSP 2007*, Honolulu, HI, Apr. 2007, pp. 257–260.

[55] N. Debande, Y. Souissi, M. Nassar, S. Guilley, T. H. Le, and J. L. Danger, "Re-synchronization by moments: An efficient solution to align side-channel traces,", in *Proc. WIFS 2011*, Foz do Iguaçu, Brazil, Nove. 2011, pp. 1–6.

[56] C. H. Gebotys and B. A. White, "Methodology for attack on a java-based PDA,", in *Proc. CODES+ISSS 2006*, Seoul, Korea, Oct. 2006, pp. 94–99.

[57] C. H. Gebotys and B. A. White, "A phase substitution technique for DEMA of embedded cryptographic systems,", in *Proc. ITNG 2007*, Las Vegas, Nevada, USA, Apr. 2007, pp. 868–869.

[58] C. Gebotys and B. A. White, "EM alignment using phase for secure embedded systems,", *Design Automation for Embedded Systems*, vol. 12, no. 3, pp. 185–206, Sep. 2008.

[59] C. H. Gebotys and B. A. White, "EM analysis of a wireless java-based PDA,", *ACM Trans. Embedded Comput. Syst.*, vol. 7, no. 4, pp. 1–28, Jul. 2008.

[60] P. Hodgers, K. Boey, and M. O'Neill, "Variable window power spectral density attack,", in *Proc. WIFS 2011*, Washington, DC, USA, Nov. 2011, pp. 1–6.

[61] N. Homma, S. Nagashima, Y. Imai, T. Aoki, and A. Satoh, "High-resolution side-channel attack using phase-based waveform matching,", in *Proc. CHES 2006*, Yokohama, Japan, Oct. 2006, pp. 187–200.

[62] J. Waddle and D. Wagner, "Towards efficient second-order power analysis,", in *Proc. CHES 2004*, Cambridge, Massachusetts, USA, Aug. 2004, pp. 1–15.

[63] P. Schäfer, "Towards time series classification without human preprocessing,", in *Proc. MLDM 2014*, St. Petersburg, Russia, Jul. 2014, pp. 228–242.

[64] L. Mather, E. Oswald, and C. Whitnall, "Multi-target DPA Attacks: Pushing DPA Beyond the Limits of a Desktop Computer,", in *Proc. ASIACRYPT 2014*, Kaoshiung, Taiwan, R.O.C., Dec. 2014, pp. 243–261.

[65] C. Carlet, J.-C. Faugère, C. Goyet, and G. Renault, "Analysis of the algebraic side channel attack,", *J. Cryptogr. Eng.*, vol. 2, no. 1, pp. 45–62, May 2012.

[66] I. Dinur, P. Morawiecki, J. Pieprzyk, M. Srebrny, and M. Straus, "Cube attacks and cube-attack-like cryptanalysis on the round-reduced keccak sponge function,", in *Proc. EUROCRYPT 2015*, Sofia, Bulgaria, Apr. 2015, pp. 733–761.

[67] Z. Li, B. Zhang, J. Fan, and I. Verbauwhede, "A new model for error-tolerant side-channel cube attacks,", in *Proc. CHES 2013*, Santa Barbara, California, USA, Aug. 2013, pp. 453–470.

[68] M. S. E. Mohamed, S. Bulygin, M. Zohner, A. Heuser, M. Walter, and J. A. Buchmann, "Improved algebraic side-channel attack on AES,", *J. Cryptogr. Eng.*, vol. 3, no. 3, pp. 139–156, Sep. 2013.

[69] N. Veyrat-Charvillon, B. Gérard, and F.-X. Standaert, "Soft analytical side-channel attacks,", in *Proc. ASIACRYPT 2014*, Kaoshiung, Taiwan, Dec. 2014, pp. 282–296.

[70] X. Zhao, F. Zhang, S. Guo, T. Wang, Z. Shi, H. Liu, and K. Ji, "MDASCA: an enhanced algebraic side-channel attack for error tolerance and new leakage model exploitation,", in *Proc. COSADE 2012*, Darmstadt, Germany, May 2012, pp. 231–248.

[71] M. A. Elaabid, O. Meynard, S. Guilley, and J. L. Danger, "Combined side-channel attacks,", in *Proc. WISA 2010*, Jeju Island, Korea, Aug. 2010, pp. 175–190.

[72] Z. Guo, Da. Gu, H. Lu, J. Liu, S. Xu, S. Bao, and H. Gu, "A combinational power analysis method against cryptographic hardware,", *China Commun.*, vol. 12, no. 1, pp. 99–107, Jan. 2015.

[73] C. Polhl, and J. L. Van Genderen, "Multisensor image fusion in remote sensing: Concepts, methods and applications,", *Journal of Remote Sensing*, vol. 19, no. 5, pp. 823–854, Jan. 1998.

[74] J. Heyszl, A. Ibing, S. Mangard, F. D. Santis, and G. Sigl, “Clustering algorithms for non-profiled single-execution attacks on exponentiations,”, in *Proc. CARDIS 2013*, Berlin, Germany, Nov. 2013, pp. 79–93.

[75] R. Specht, J. Heyszl, M. Kleinsteuber, and G. Sigl, “Improving Non-profiled Attacks on Exponentiations Based on Clustering and Extracting Leakage from Multi-channel High-Resolution EM Measurements,”, in *Proc. COSADE 2015*, Berlin, Germany, Apr. 2015, pp. 3–19.

[76] F.-X. Standaert and C. Archambeau, “Using subspace-based template attacks to compare and combine power and electromagnetic information leakages,”, in *Proc. CHES 2008*, Washington, D.C., USA, Aug. 2008, pp. 411–425.

[77] W. Schindler, “A Combined Timing and Power Attack,”, in *Proc. PKC 2002*, Paris, France, Feb. 2002, pp. 263–279.

[78] Y. Souissi, S. Bhasin, S. Guilley, M. Nassar, and J.-L. Danger, “Towards Different Flavors of Combined Side Channel Attacks,”, in *Proc. CT-RSA 2012*, San Francisco, California, USA, Feb. 2012, pp. 245–259.

[79] C. Carlet, E. Prouff, M. Rivain, and T. Roche, “Algebraic Decomposition for Probing Security,”, in *Proc. CRYPTO 2015*, Santa Barbara, California, USA, Aug. 2015, pp. 742–763.

[80] A. Moradi, M. Kasper, and C. Paar, “Black-box side-channel attacks highlight the importance of countermeasures - an analysis of the xilinx virtex-4 and virtex-5 bitstream encryption mechanism,”, in *Proc. CT-RSA 2012*, San Francisco, California, USA, Feb. 2012, pp. 1–18.

[81] D. Oswald and C. Paar, “Breaking mifare desfire MF3ICD40: power analysis and templates in the real world,”, in *Proc. CHES 2011*, Nara, Japan, Sep. 2011, pp. 207–222.

[82] F.-X. Standaert, T. Malkin, and M. Yung, “A unified framework for the analysis of side-channel key recovery attacks (extended version),”, *IACR Cryptology ePrint Archive*, vol. 2006, pp. 139, Apr. 2006.

[83] Y. Fei, Q. Luo, and A. A. Ding, “A statistical model for DPA with novel algorithmic confusion analysis,”, in *Proc. CHES 2012*, Leuven, Belgium, Sep. 2012, pp. 233–250.

[84] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, “Mutual Information Analysis”, in *Proc. CHES 2008*,Washington, D.C., USA, Aug. 2008, pp. 426–442.

[85] V. Lomné, E. Prouff, M. Rivain, T. Roche, and A. Thillard, “How to Estimate the Success Rate of Higher-Order Side-Channel Attacks,”, in *Proc. CHES 2014*, Busan, South Korea, Sep. 2014, pp. 35–54.

[86] D. P. Martin, J. F. O’Connell, E. Oswald, and M. Stam, “Counting keys in parallel after a side channel attack,”, in *Proc. ASIACRYPT 2015*, Auckland, New Zealand, Nov. 2015, pp. 313–337.

[87] S. Mangard, “Hardware Countermeasures against DPA? A Statistical Analysis of Their Effectiveness,”, in *Proc. CT-RSA 2004*, San Francisco, California, USA, Feb. 2004, pp. 222–235.

[88] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,”, in *Proc. CHES 2004*, Massachusetts, USA, Aug. 2004, pp. 16–29.

[89] F. Durvaux, F.-X. Standaert, and N. Veyrat-Charvillon, “How to Certify the Leakage of a Chip,”, in *Proc. EUROCRYPT 2014*, Copenhagen, Denmark, May 2014, pp. 459–476.

[90] S. Bhasin, J. L. Danger, S. Guilley, and Z. Najm, “Nicv: Normalized inter-class variance for detection of side-channel leakage,”, in *Proc. EMC 2014*, Tokyo, Japan, May 2014, pp. 310–313.

[91] S. Bhasin, J. L. Danger, S. Guilley, and Z. Najm, "Side-channel leakage and trace compression using normalized inter-class variance,", in *Proc. HASP 2014*, Minneapolis, Minnesota, USA, Jun. 2014, pp. 7:1–-7:9.

[92] A. Moradi and F.-X. Standaert, "Moments-correlating DPA,", *IACR Cryptology ePrint Archive*, vol. 2014, pp. 409, Sep. 2016.

[93] M. Renauld, F.-X. Standaert, N. Veyrat-Charvillon, D. Kamel, and D. Flandre, "A Formal Study of Power Variability Issues and Side-Channel Attacks for Nanoscale Devices,", in *Proc. EUROCRYPT 2011*, Tallinn, Estonia, May 2011, pp. 109–128.

[94] F. Durvaux, F.-X. Standaert, and S. Pozo, "Towards Easy Leakage Certification,", in *Proc. CHES 2016*, Santa Barbara, California, USA, Aug. 2016, pp. 40–60.

[95] A. Moradi, S. Guilley, and A. Heuser, "Detecting hidden leakages,", in *Proc. ACNS 2014*, Lausanne, Switzerland, Jun. 2014, pp. 324–342.

[96] L. Batina, B. Gierlichs, E. Prouff, M. Rivain, F.-X. Standaert, and N. Veyrat-Charvillon, "Mutual information analysis: a comprehensive study,", *J. Cryptol.*, vol. 24, no. 2, pp. 269–291, Apr. 2011.

[97] G. Becker, J. Cooper, E. DeMulder, G. Goodwill, J. Jaffe, G. Kenworthy, T. Kouzminov, A. Leiserson, M. Marson, P. Rohatgi, and S. Saab. (2013, Sep.) Test vector leakage assessment (TVLA) methodology in practice. [Online]. Available: http://icmc-2013.org/wp/wp-content/uploads/2013/09/Rohatgi_Test-Vector-Leakage-Assessment.pdf

[98] A. A. Ding, C. Chen, and T. Eisenbarth, "Simpler, faster, and more robust t-test based leakage detection,", in *Proc. COSADE 2016*, Graz, Austria, Apr. 2016, pp. 163–183.

[99] G. Goodwill, B. Jun, J. Jaffe, and P. Rohatgi. (2011, Sep.) A testing methodology for side-channel resistance validation. [Online]. Available: http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/papers/08_Goodwill.pdf

[100] J. Longo, E. D. Mulder, D. Page, and M. Tunstall, "Soc it to EM: electromagnetic side-channel attacks on a complex system-on-chip,", in *Proc. CHES 2015*, Saint-Malo, France, Sep. 2015, pp. 620–640.

[101] L. Mather, E. Oswald, J. Bandenburg, and M. Wójcik, "Does my device leak information? an a priori statistical power analysis of leakage detection tests,", in *Proc. ASIACRYPT 2013*, Bengaluru, India, Dec. 2013, pp. 486–505.

[102] T. Schneider and A. Moradi, "Leakage assessment methodology - a clear roadmap for side-channel evaluations,", in *Proc. CHES 2015*, Saint-Malo, France, Sep. 2015, pp. 495–513.

[103] S. Bhasin, N. Bruneau, J.-L. Danger, S. Guilley, and Z. Najm, "Analysis and improvements of the DPA contest v4 implementation,", in *Proc. SPACE 2014*, Pune, India, Oct. 2014, pp. 201–218.

[104] S. Hajra and D. Mukhopadhyay, "On the optimal pre-processing for non-profiling differential power analysis,", in *Proc. COSADE 2014*, Paris, France, Apr. 2014, pp. 161–178.

[105] A. B. Levina and P. S. Borisenko, "Implementation of side-channel leakage detection technique based on normalized inter-class variance method,", *Scientific and Technical Herald of Information Technologies, Mechanics and Optics*, vol. 16, no. 4, pp. 697–702, Jul. 2016.

[106] P. Mishra, S. Bhunia, and M. Tehranipoor, *Hardware IP Security and Trust*. Gewerbestrasse, Switzerland: Springer, 2017.

[107] S. Mangard, E. Oswald, and F.-X. Standaert, "One for all - all for one: unifying standard differential power analysis attacks,", *IET Information Security*, vol. 5, no. 2, pp. 100–110, Jun. 2011.

[108] W. Schindler, K. Lemke, and C. Paar, “A stochastic model for differential side channel cryptanalysis,”, in *Proc. CHES 2005*, Edinburgh, UK, Sep. 2005, pp. 30–46.

[109] V. Banciu and E. Oswald, “Pragmatism vs. elegance: Comparing two approaches to simple power attacks on AES,”, in *Proc. COSADE 2014*, Paris, France, Apr. 2014, pp. 29–40.

[110] Y. Fei, Q. Luo, and A. A. Ding, “A statistical model for DPA with novel algorithmic confusion analysis,”, in *Proc. CHES 2012*, Leuven, Belgium, Sep. 2012, pp. 233–250.

[111] M. Rivain, “On the exact success rate of side channel analysis in the gaussian model,”, in *Proc. SAC 2008*, Sackville, New Brunswick, Canada, Aug. 2008, pp. 165–183.

[112] F.-X. Standaert, E. Peeters, G. Rouvroy, and J.-J. Quisquater, “An overview of power analysis attacks against field programmable gate arrays,”, *Proceedings of the IEEE*, vol. 94, no. 2, pp. 383–394, Feb. 2006.

[113] A. Thillard, E. Prouff, and T. Roche, “Success through confidence: Evaluating the effectiveness of a side-channel attack,”, in *Proc. CHES 2013*, Santa Barbara, California, USA, Aug. 2013, pp. 21–36.

[114] A. A. Ding, L. Zhang, Y. Fei, P. Luo, “A statistical model for higher order dpa on masked devices,”, in *Proc. CHES 2014*, Busan, South Korea, Sep. 2014, pp. 147–169.

[115] R. Poussier, F.-X. Standaert, and V. Grosso, “Simple key enumeration (and rank estimation) using histograms: An integrated approach,”, in *Proc. CHES 2016*, Santa Barbara, California, USA, Aug. 2016, pp. 61–81.

[116] J. Pan, J. G. J. V. Woudenberg, J. I. D. Hartog, and M. F. Witteman, “Improving DPA by peak distribution analysis,”, in *Proc. SAC 2010*, Waterloo, Ontario, Canada, Aug. 2010, pp. 241–261.

[117] W. Meier and O. Staffelbach, “Analysis of pseudo random sequences generated by cellular automata,”, in *Proc. EUROCRYPT 1991*, Brighton, UK, Apr. 1991 , pp. 186–199.

[118] M. Dichtl, “A new method of black box power analysis and a fast algorithm for optimal key search,”, *J. Cryptogr. Eng.*, vol. 1, no. 4, pp. 255–264, Dec. 2011.

[119] A. Bogdanov, I. Kizhvatov, K. Manzoor, E. Tischhauser, and M. Witteman, “Fast and memory-efficient key recovery in side-channel attacks,”, in *Proc. SAC 2015*, Sackville, New Brunswick, Canada, Aug. 2015, pp. 310–327.

[120] D. P. Martin, J. F. O’Connell, E. Oswald, and M. Stam, “How to enumerate your keys accurately and efficiently after a side channel attack,”, *IACR Cryptology ePrint Archive*, vol. 2015, pp. 689, Jul. 2015.

[121] L. David and A. Wool, “A bounded-space near-optimal key enumeration algorithm for multi-subkey side-channel attacks,”, in *Proc. CT-RSA 2017*, San Francisco, California, USA, Feb. 2017, pp. 311–327.

[122] Publication Moved. (2001, Nov.) FIPS 197, Advanced Encryption Standard (AES). [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[123] D. J. Bernstein, T. Lange, and C. V. Vredendaal, “Tighter, faster, simpler side-channel security evaluations beyond computing power,”, *IACR Cryptology ePrint Archive*, vol. 2015, pp. 221, Jul. 2015.

[124] X. Ye, T. Eisenbarth, and W. Martin, “Bounded, yet sufficient? how to determine whether limited side channel information enables key recovery,”, in *Proc. CARDIS 2014*, Paris, France, Nov. 2014, pp. 215–232.

[125] D. P. Martin, L. Mather, E. Oswald, and M. Stam, “Characterisation and estimation of the key rank distribution in the context of side channel evaluations,”, in *Proc. ASIACRYPT 2016*, Hanoi, Vietnam, Dec. 2016, pp. 548–572.

[126] D. Jurafsky. (2012, Jan.) Minimum edit distance. [Online]. Available: https://web.stanford.edu/class/cs124/lec/med.pdf

[127] M. Adams, "The sequence of the human genome (abstract only),", in *Proc. RECOMB 2001*, Montreal, Quebec, Canada, April 2001, pp. 1.

[128] G. Navarro, "A guided tour to approximate string matching,", *ACM Comput. Surv.*, vol. 33, no. 1, pp. 31–88, Mar. 2001.

[129] (2003, Sep.) Multiple sequence alignment. [Online]. Available: https://www.cs.umd.edu/class/spring2003/cmsc838t/lec4.pdf

[130] P. Schäfer, "The BOSS is concerned with time series classification in the presence of noise,", *Data Mining and Knowledge Discovery*, vol. 29, no. 6, pp. 505–1530, Nov. 2015.

[131] G. E. A. P. A. Batista，X. Wang，and E.J. Keogh, "A complexity-invariant distance measure for time series,", in *Proc. SDM 2011*, Mesa, Arizona, Apr. 2011, pp. 699–710.

[132] F.-X. Standaert, B. Gierlichs, and I. Verbauwhede, "Partition vs. comparison side-channel distinguishers: an empirical evaluation of statistical tests for univariate side-channel attacks against two unprotected CMOS devices,", in *Proc. ICISC 2008*, Seoul, Korea, Dec. 2008, pp. 253–267.

[133] S. Salvador and P. Chan, "Toward accurate dynamic time warping in linear time and space,", *Intelligent Data Analysis*, vol. 11, no. 5, pp. 561–580, Oct. 2007.

[134] M. Nassar, Y.Souissi, S. Guilley, and J.-L. Danger, "RSM: A small and fast countermeasure for AES, secure against 1st and 2nd-order zero-offset SCAs", in *Proc. DATE 2012*, Dresden, Germany, pp. 1173-1178.

[135] Eric Peeters, *Advanced DPA theory and practice*. New York, USA: Springer, 2013.

[136] K. S. Arvind, S. P. Mishra, B. M. Suri, and A. Khosla, "Investigations of Power and EM Attack on AES Implemented in FPGA,", in *Proc. SocProS 2015*, Apr. 2016, pp. 555-567.

[137] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side-channel(s),", in *Proc. CHES 2002*, Redwood Shores, California, USA, Aug. 2002, pp. 29–45.

[138] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): measures and counter-measures for smart cards,", in *Proc. ICRSC 2001*, Cannes, France, Sep. 2001, pp. 200–210.

[139] B. Siciliano, O. Khatib, *Springer handbook of robotics* Heidelberg, Germany: Springer, 2016.

[140] P. A. Priyadharsini, "Multimodal medical image fusion based on svd,", *IOSR-JCE*, vol. 1, no. 16, pp. 27–31, Jan. 2014.

[141] D. Lahat, T. Adali, and C. Jutten, "Multimodal data fusion: An overview of methods, challenges, and prospects,", *Proceedings of the IEEE*, vol. 103, no. 9, pp. 1449–1477, Sep. 2015.

[142] D. Groutage and D. Bennink, "A new matrix decomposition based on optimum transformation of the singular value decomposition basis sets yields principal features of time-frequency distributions,", in *Proc. IEEE SSAP-2000*, Pennsylvania, USA, Aug. 2000, pp. 598–602.

[143] H. Hassanpour, M. Mesbah, and B. Boashash, "Time-frequency feature extraction of newborn eeg seizure using svd-based techniques,", *EURASIP Journal on Advances in Signal Processing*, vol. 2004, no. 16, pp. 1–11, Dec. 2004.

[144] I. Orovi, S. Stanković, and A. Draganić, "Time-frequency analysis and singular value decomposition applied to the highly multicomponent musical signals,", *Acta acustica united with acustica*, vol. 100, no.1, pp. 93–101, Jan. 2014.

[145] L. Moisan, “How to discretize the total variation of an image,”, *PAMM*, vol. 7, no. 1, pp. 1041907–1041908, Dec. 2007.

[146] G. H. Golub and V. Loan, *Matrix computations*. Baltimore, USA: JHU Press, 2012.

[147] M. W. Berry, M. Browne, A. N. Langville, V. P. Pauca, and R. J. Plemmons, “Algorithms and applications for approximate nonnegative matrix factorization,”, *Elsevier CSDA*, vol. 52, no. 1, pp. 155–173, Nov. 2007.

[148] A. N. Langville, C. D. Meyer, R. Albright, J. Cox, and D. Duling, “Algorithms, initializations, and convergence for the nonnegative matrix factorization,”, *CoRR*, abs/1407.7299, Jul. 2014.

[149] A. V. Oppenheim and R. W. Schafer, *Discrete-time signal processing*, 3rd ed. New York, USA: Pearson, 2010.

[150] H. Liu, X. Jin, Y. Tsunoo, and S. Goto, “Correlated Noise Reduction for Electromagnetic Analysis,”, *IEICE Trans. Fund. Electr.*, vol. 96-A, no.1, pp. 185–195, Jan. 2013.

[151] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, “Mutual information analysis: a generic side-channel distinguisher,”, in *Proc. CHES 2008*, Washington, D.C., USA, Aug. 2008, pp. 426–442.

[152] H. Kim, D. G. Han, and S. Hong, “Mutual information analysis for three-phase dynamic current mode logic against side-channel attack,”, *Etri Journal*, vol. 37, no. 3, Jun. 2015.

[153] A. Moradi, “Statistical tools flavor side-channel collision attacks,”, in *Proc. EUROCRYPT 2012*, Cambridge, UK, Apr. 2012, pp. 428–445.

[154] O. Rioul, A. Heuser, S. Guilley, and J.-L. Danger, “Inter-class vs. mutual information as side-channel distinguishers,”, in *Proc. ISIT 2016*, Barcelona, Spain, Jul. 2016, pp. 805–809.

[155] C. Whitnall and E. Oswald, “A comprehensive evaluation of mutual information analysis using a fair evaluation framework,”, in *Proc. CRYPTO 2011*, Santa Barbara, California, USA, Aug. 2011, pp. 316–334.

[156] P. Chen, *Digital signal processing*. Beijing, China: Tsinghua University Press, 2007.

[157] S. Endre and M. David, *An introduction to numerical analysis*. Cambridge, UK: Cambridge University Press, 2003.

[158] B. Gierlichs, K. Lemke-Rust, and C. Paar, “Templates vs. stochastic methods,”, in *Proc. CHES 2006*, Yokohama, Japan, Oct. 2006, pp. 15–29.

[159] J. P. Guilford and B. Fruchter, *Fundamental statistics in psychology and education*. Tokyo, Japan: McGraw-Hill Kogakusha, LTD, 1973.

[160] W. Yang, Y. Cao, K. Ma, H. Zhang, “Side-Channel Leakage Evaluation and Detection Based on Communication Theory,”, *IACR Cryptology ePrint Archive*, vol. 2016, pp. 922, Sep. 2016.

[161] I. Gesteira C. Filho, *Mixture models for the analysis of gene expression*. Berlin, Germany: Freie Universität Berlin, 2008.

[162] X. Chen, X. Liu, and Y. Jia, “Unsupervised selection and discriminative estimation of orthogonal gaussian mixture models for handwritten digit recognition,”, in *Proc. ICDAR 2009*, Barcelona, Spain, Jul. 2009, pp. 1151–1155.

[163] G. McLachlan and D. Peel, *Finite mixture models*. New York, USA: John Wiley and Sons, 2004.

[164] A. P. Dempster, N. M. Laird, and D. B. Rubin, “Maximum likelihood from incomplete data via the em algorithm,”, *J. Roy. Statist. Soc. Ser. B*, vol. 39, no. 1, pp. 1–38, Jan. 1977.

[165] R. Bose, *Information Theory, Coding and Cryptography, 2nd Edition*. Columbus, USA: Tata McGraw-Hill Education Pvt. Ltd., 2008.

[166] M. F. Huber, T. Bailey, H. Durrant-Whyte, and U. D. Hanebeck, "On entropy approximation for Gaussian mixture random vectors,", in *Proc. MFI 2008*, Seoul, Korea, Aug. 2008, pp. 181–188.

[167] M. Zhang and Q. Cheng, "Determine the number of components in a mixture model by the extended KS test,", *Pattern Recognition Letters*, vol. 25, pp. 211–216, Jan. 2004.

[168] C. Xie, J. Chang, and Y. Liu, "Estimating the number of components in Gaussian mixture models adaptively for medical image,", *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 23, pp. 6216–6221, Dec. 2013.

[169] Y. I. Moon, B. Rajagopalan, and U. Lall, "Estimation of mutual information using kernel density estimators,", *Phys Rev E Stat Phys Plasmas Fluids Relat Interdiscip Topics*, vol. 52, pp. 2318–2321, Oct. 1995.

[170] L. Wei. (2012, May.) Channel capacity and constellation optimization of M-PAM input AWGN channels with non-equiprobable symbols. [Online]. Available: http://people.cecs.ucf.edu/lei/letter_ieee_capacityMPSK_v2.pdf.

[171] S. Mao, J. Wang, and X. Pu, *Advanced Mathematical Statistics*. Beijing, China: Higher Education Press, 2009.

[172] R. McEliece, *The theory of information and coding*. Cambridge, UK: Cambridge University Press, 2002.

[173] G. Dabosville, J. Doget, and E. Prouff, "A new second-order side channel attack based on linear regression,", *IEEE Trans. Computers*, vol. 62, no. 8, pp. 1629–1640, Aug. 2013.

[174] M. A. Tanner, "Tools for statistical inference : methods for the exploration of posterior distributions and likelihood functions,", *Biometrics*, vol. 54, no. 2, pp. 560-563, Jun. 1998.

[175] H. W. Kuhn, *The Hungarian method for the assignment problem*. Heidelberg, Germany: Springer, 2010.

附录 A　附录

A.1　第二章附录内容

A.1.1　加权编辑距离的求解算法

详见算法 13。

Algorithm 13 动态规划求解两个字符串之间的加权编辑距离

输入： 两个字符串S及T，插入、删除及置换三个编辑操作的权重$\omega_{ins}, \omega_{del}, \omega_{sub}$

输出： S及T之间的加权编辑距离$EditDist$

初始化：

$Dist(0,0) = 0$

$Dist(i,0) = Dist(i-1,0) + \omega_{del}(S(i)),\ 1 < i \leq length(S)$

$Dist(0,j) = Dist(0,j-1) + \omega_{ins}(T(j)),\ 1 < j \leq length(T)$

循环：

$$Dist(i,j) = min \begin{cases} Dist(i-1,j) + \omega_{del}(S(i)) \\ Dist(i,j-1) + \omega_{ins}(T(j)) \\ Dist(i-1,j-1) + \omega_{sub}(S(i),T(j)) \end{cases}$$

终止：

$EditDist = Dist(length(S), length(T))$

返回 S及T之间的加权编辑距离 $EditDist$

A.1.2　字符串“WITTEN”和“BITTING”的加权编辑距离代价矩阵

表 A.1　字符串“WITTEN”和“BITTING”的加权编辑距离代价矩阵

	#	B	I	T	T	I	N	G
#	0	1	2	3	4	5	6	7
W	1	1	2	3	4	5	6	7
I	2	2	1	2	3	4	5	6
T	3	3	2	1	2	3	4	5
T	4	4	3	2	1	2	3	4
E	5	5	4	3	2	2	3	4
N	6	6	5	4	3	3	2	3

A.1.3 后向回溯算法

详见算法 14。

A.2 第三章附录内容

A.2.1 贝叶斯融合“更新形式”推导过程

当有新的单信道泄漏信息加入时，有

$$\begin{aligned} P(k_i|L_{M+1}) =& \frac{\prod_{j=1}^{M+1} P(\boldsymbol{l_j})}{P(L_{M+1})\,[P(k_i)]^M} \prod_{j=1}^{M+1} P(k_i|\boldsymbol{l_j}) \\ =& \frac{\prod_{j=1}^{M} P(\boldsymbol{l_j})P(\boldsymbol{l_{M+1}})}{P(L_M)P(\boldsymbol{l_{M+1}}|L_M)\,[P(k_i)]^{M-1}} \times \\ & \frac{1}{P(k_i)} \prod_{j=1}^{M} P(k_i|\boldsymbol{l_j})P(k_i|\boldsymbol{l_{M+1}}) \\ =& \frac{P(\boldsymbol{l_{M+1}})}{P(k_i)P(\boldsymbol{l_{M+1}}|L_M)} P(k_i|\boldsymbol{l_{M+1}}) \times \\ & \frac{\prod_{j=1}^{M} P(\boldsymbol{l_j})}{P(L_M)\,[P(k_i)]^{M-1}} \prod_{j=1}^{M} P(k_i|\boldsymbol{l_j})\,. \end{aligned} \tag{A-1}$$

若令上式中

$$C = \frac{P(\boldsymbol{l_{M+1}})}{P(k_i)P(\boldsymbol{l_{M+1}}|L_M)},$$

则得到贝叶斯融合另一种表达形式

$$P(k_i|L_{M+1}) = CP(k_i|L_M)P(k_i|\boldsymbol{l_{M+1}})\,. \tag{A-2}$$

A.2.2 基于贝叶斯推断乘法融合律与加法融合律的等价性证明

分别用符号$P(k_i)$表示子密钥候选值k_i的先验概率，$P(k_i|\boldsymbol{l_j})$表示k_i的已知某侧信道泄漏$\boldsymbol{l_j}$后的后验概率。假设$P(k_i)$和$P(k_i|\boldsymbol{l_j})$之间存在一个很小的差值ϵ_{ij} ($\epsilon_{ij} \ll 1$)，亦即

$$P(k_i|\boldsymbol{l_j}) = P(k_i)(1+\epsilon_{ij}),\ \epsilon_{ij} \ll 1. \tag{A-3}$$

上述假设实际中很容易成立，因为相比1而言，子密钥的先验概率与其后验概率的差别小得多。于是有

$$\begin{aligned} \prod_{j=1}^{M} P(k_i|\boldsymbol{l_j}) &= \prod_{j=1}^{M} P(k_i)(1+\epsilon_{ij}) \\ &= P^M(k_i) \prod_{j=1}^{M} (1+\epsilon_{ij})\,. \end{aligned} \tag{A-4}$$

Algorithm 14 后向回溯算法

输入： 两个字符串S及T的编辑距离代价矩阵$Cost$，其中T为参考字符串

输出： 两个字符串S及T的一个最优对齐字符串对$alignS$及$alignT$

$alignS \longleftarrow S, alignT \longleftarrow T$
定位到矩阵$Cost$右下角的单元格，即表中坐标为$(length(S)+2, length(T)+2)$的单元格，作为起点
for $i = length(S)-1, \ldots, 0$ **do**
    for $j = length(T)-1, \ldots, 0$ **do**
        if $j == 0$ **then**
            定位到上一步起点单元格左侧的单元格，终止
        end if
        if $i == 0$ **then**
            定位到上一步起点单元格上方的单元格，终止
        end if
        if $S(i) == T(j)$ **then**
            定位到上一步起点单元格左上角的单元格，作为新的起点
        end if
        if $S(i) \neq T(j)$ **then**
            定位到上一步起点单元格左侧、上方及左上角单元格中值最小的单元格，作为新的起点——若三个单元格的值相同，则选择优先级依次是左上角、上方及左侧单元格
            if *backtracking to the left cell* **then** //定位到上一步起点单元格左侧的单元格
                向$alignS$相应字符后插入符号“_” //“_”表示将$T(j)$插入S中
            else if *backtracking to the upper cell* **then** //定位到上一步起点单元格上方的单元格
                向$alignT$相应字符后插入符号“_” //“_”表示将$S(i)$删除
            else
                将$S(i)$置换为$T(j)$
            end if
        end if
    end for
end for
返回 最优对齐字符串对$alignS$及$alignT$

之后，展开上式右边的乘积项，得到一个常数项1、变量ϵ_{ij}的一次项及大量的关于ϵ_{ij}二次项及高阶项。因为$\epsilon_{ij} \ll 1$，所以与其有关的二次项及高阶项可近似视为0。于是，式 A-4 右侧乘积项可以近似为其线性项，而式 A-4 亦可近似为

$$\begin{aligned}\prod_{j=1}^{M} P(k_i|\boldsymbol{l_j}) &\approx P^M(k_i)[\sum_{j=1}^{M}(1+\epsilon_{ij}) - (M-1)] \\ &= P^M(k_i)[\sum_{j=1}^{M}\frac{P(k_i|\boldsymbol{l_j})}{P(k_i)} - (M-1)] \\ &= P^{M-1}(k_i)\sum_{j=1}^{M}P(k_i|\boldsymbol{l_j}) - (M-1)P^M(k_i)\ .\end{aligned} \tag{A-5}$$

又因为$P(k_i)$服从均匀分布，所以可得

$$\begin{aligned}k_{guess} &= \underset{k_i \in K}{\operatorname{argmax}} \prod_{j=1}^{M} P(k_i|\boldsymbol{l_j}) \iff \\ k_{guess} &= \underset{k_i \in K}{\operatorname{argmax}} \sum_{j=1}^{M} P(k_i|\boldsymbol{l_j})\ .\end{aligned} \tag{A-6}$$

致　谢

这里，我对攻读博士学位期间所有关心以及帮助过我的人表示衷心的感谢。

首先，深深感谢我的导师焦建彬教授。焦老师一直是我的榜样。在科研上，焦老师严谨细致、一丝不苟，充分尊重学生的自由探索，给予了我许多指导和帮助。在生活中，焦老师是一位宽和的长者，给予了我无私的关心、教诲与帮助，不仅促进了我个人的成长进步，而且助我顺利迈过了不少坎儿。其中感激之情，言语已然无法说清。他的言传身教将使我在今后无论面对科研还是生活，都将积极乐观、坦然自信、受益终生。在此谨向焦老师致以诚挚的谢意和崇高的敬意！

同时，由衷感谢叶齐祥教授。叶老师开阔的眼界和胸襟，以及对学术的态度、要求和能力，向来令我钦敬。他不但在生活中为我提供了不少帮助，而且对如何做研究提出了许多宝贵意见与建议，使我受益匪浅。随着研究深入，我越发体会到这些意见与建议的价值。

一直以来，模式识别与系统开发实验室的同门，如立国师兄、孝罡师兄、刘一飞师兄、高山等，在科研及生活中对我关心不断，给予了不少有力帮助和支持。每每念及，总让我感到温暖。这里一并献上个人由衷的祝福及深深的谢意。

“独学而无友，则孤陋而寡闻。”在此，感谢我的同学徐玉威、李明、王海燕等人。不管是在科研、还是生活及为人处事上，他们都让我学习到了很多。而且他们的耐心与支持，让我深切体会到了同学的含义。

此外，特别感谢信息工程研究所周永彬研究员、张海龙老师、张倩老师、曹雨晨师妹、王欢师妹等在科研上的热心帮助与支持。

另外，非常感谢北京理工大学计算机科学学院王安老师在科研探讨中的无私帮助，让我厘清了不少概念及认识，使我获益良多。除此之外，他还在学术论文修改方面给了我不少有益建议。

也十分感谢几个老友、硕士舍友在生活中对我的热切帮助和关心。这不仅为我增加了坚持的动力，而且对我提高解决生活中问题的能力大有裨益。

最后，要特别感谢我的父母及家人的默默支持。有了他们，于我才得始终。

作者简介

姓名：杨威　　性别：男　　籍贯：河南省

2013.9 – 至今	中国科学院大学攻读博士研究生
2010.9 – 2013.7	中国科学院大学硕士研究生
2006.9 – 2010.7	中国人民解放军信息工程大学本科生

【攻读博士学位期间发表的论文与研究成果】

[1] **W. Yang**, Y. Cao, Y. Zhou, H. Zhang, and Q. Zhang, "Distance based leakage alignment for side channel attacks,", *IEEE Signal Process. Lett.*, vol. 23, no. 4, pp. 419–423, Jan. 2016.

[2] **W. Yang**, Y. Zhou, Y. Cao, H. Zhang, and Q. Zhang, "Multi-channel fusion attacks,", *IEEE Trans. Info. Foren. Sec.*, vol. 12, no. 8, pp. 1757–1771, Aug. 2017.

[3] **W. Yang**, Y. Cao, K. Ma, H. Zhang, "Side-Channel Leakage Evaluation and Detection Based on Communication Theory,", *IACR Cryptology ePrint Archive*, vol. 2016, pp. 922, Sep. 2016.

[4] Y. Cao, Y. Zhou, H. Zhang, and **W. Yang**, "Hilbert Transform based Vertical Preprocessing for Side Channel Analysis,", in *Proc. ICCCN 2016*, Hawaii, USA, Aug. 2016, pp. 1–7.

[5] S. Qiu, R. Zhang, Y. Cao, **W. Yang**, Y. Zhou, and T. Ding, "A Statistical Model for DPA When Algorithmic Noise Is Dependent on Target,", *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 4882-4896, Dec. 2016.