密码芯片硅前安全测评与增强技术研究

Research on Pre-Silicon Security Evaluation and Protection Techniques for Cryptographic Chip

一级学科：电子科学与技术

研究方向：硬件安全

作者姓名：马浩诚

指导教师：赵毅强 教授

答辩日期	2023 年 02 月 16 日		
答辩委员会	姓名	职称	工作单位
主席	戴紫彬	教授	战略支援部队信息工程大学
委员	解晓东	教授	北京大学
	刘雷波	教授	清华大学
	金意儿	教授	中国科学技术大学
	陈波	研究员	中国航天科工集团二院 201 所

天津大学微电子学院

二〇二三年三月

独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作和取得的研究成果，除了文中特别加以标注和致谢之处外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得 天津大学 或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

学位论文作者签名：马浩诚 签字日期：2023 年 2 月 16 日

学位论文版权使用授权书

本学位论文作者完全了解天津大学有关保留、使用学位论文的规定。特授权天津大学 可以将学位论文的全部或部分内容编入有关数据库进行检索，并采用影印、缩印或扫描等复制手段保存、汇编以供查阅和借阅。同意学校向国家有关部门或机构送交论文的复印件和磁盘。

(保密的学位论文在解密后适用本授权说明)

学位论文作者签名：马浩诚 导师签名：

签字日期：2023 年 2 月 16 日 签字日期：2023 年 2 月 16 日

摘 要

密码芯片是具备密码算法功能的集成电路，用于数据加密和安全认证，是保障信息系统安全的底层硬件载体。然而，密码芯片工作产生的时间、功耗和电磁辐射等信息，容易被侧信道分析攻击所利用，对密码芯片的物理安全造成严重威胁。其中，电磁分析攻击能够非接触地采集电磁辐射，从时域、频域和空间域多个维度进行密钥分析，是目前侧信道分析攻击的代表性手段。为了抵御电磁分析攻击，对密码芯片进行安全测评和防护，得到了学术界和工业界的共同关注。

目前，安全测评和防护技术还面临着如下问题。一方面，当前的安全测评集中在硅后阶段，如若密码芯片未通过合规性检测，就需要重新经历设计与制造环节，极大增加了芯片的研发周期和流片成本。另一方面，目前的安全防护会显著增加功耗、性能或面积开销，部分硬件实现还需要全定制或半定制的电路模块，限制了这些方法的应用效果。为此，本论文聚集硅前阶段的安全测评，提出了芯片电磁仿真和安全测评优化方法，并且结合安全溯源与靶向增强，设计了兼顾安全与开销的芯片防护方案。

1. 集成电路大量的晶体管和互连线，使其电磁辐射变得非常复杂。尽管业界推出了多种电磁仿真工具，但它们主要用于电路板级或系统级设计，而无法仿真集成电路的电磁辐射。针对此，本论文开展了集成电路版图级电磁仿真方法研究。根据物理版图建立了芯片电气模型，通过电流聚合效应和金属屏蔽效应的数学推导，阐明了电磁信息的根本来源和主导因素。基于此，提出了版图级芯片电磁仿真方法，采用器件模型近似、寄生网络约减和GPU并行计算，优化了电流分析和电磁计算环节，相较于传统方法效率提升了32倍。基于SMIC 180nm CMOS工艺设计了S-Box和AES芯片，从仿真精度、测评准确度和计算成本方面，验证了版图级电磁仿真方法的有效性，仿真结果的时域准确度高于74%，空间域准确度高达98%，对信息泄露风险的测评准确度为93%。

2. 为适应大规模数据量的安全测评场景，将机器学习和电磁仿真相结合，开展了基于生成对抗网络的测评优化方法研究。设计了生成对抗网络的模型结构，提取了单元电流、电源网格到空间磁场的瞬态映射，通过生成器和判别器的对抗训练，使合成数据逼近真实的磁场分布。在进行硅前风险量化时，使用生成器快速合成规定的数据量，实现密码芯片的高效评估。采用AES、Kyber以及

两种防护电路开展验证实验，结果表明，优化方法在准确评估安全性的同时，提升了大规模数据量的测评效率。当数据量为1万曲线时，测评效率提升了9.22 ~ 9.62倍，数据量增加到10万曲线时，测评效率提升了73.48 ~ 86.05倍。

3. 针对当前防护方法的电路开销和设计成本问题，开展了密码芯片安全溯源和靶向增强方法研究。从敏感信息的泄露路径入手，提出了实现安全溯源的泄露路径识别技术，采用动态关联度分析定位具有高泄露风险的逻辑单元，借助静态安全性检验构建完整的泄露路径。对于安全溯源的结果，组合布尔掩码和随机预充电的优点，提出了局部路径掩码方案，形成了自动部署防护方案的逻辑映射算法，实现了密码芯片的靶向增强。根据以上技术，设计了抵御电磁分析攻击的增强型AES电路，验证结果表明，侧信道安全水平提升了1066倍，而在电路面积、功耗和性能方面，仅产生了6.53%、4.51%和3.1%的额外开销。

关键词： 密码芯片，电磁分析攻击，硅前安全测评，芯片电磁仿真，侧信道防护

ABSTRACT

Cryptographic integrated circuits (ICs) provide services of data encryption and identity authentication, playing an essential role in modern information security scenarios. However, cryptographic ICs will leak side-channel information including power consumption, timing delay, electromagnetic (EM) emanations, etc. This information can be exploited by an attacker to steal secret information from fabricated ICs, causing side-channel analysis (SCA) attacks. Among them, EM emanations contain rich information in spatial and temporal domains and can be measured without direct physical contact. This makes cryptographic ICs more vulnerable to EM SCA attacks. To address this threat, security evaluation and protection on cryptographic ICs are important.

Current security evaluation and protection technologies face the following issues. On one hand, existing security evaluations often happen at the post-silicon stage. Any identification of side channel vulnerability may lead to high costs and delay the time-to-market. On the other hand, many existing countermeasures are costly in terms of area, power or performance, and may require full-custom circuit design for proper implementations. Therefore, we propose the EM simulation framework and optimize the security evaluation method, which supports security evaluations at the early design stage. Meanwhile, through leaky paths identification and obfuscation, we design the protection scheme balancing security and overheads.

Due to a large number of metal wires and standard cells, it is hard to predict the EM behavior of ICs at the design stage, even for those commercial tools. We develop the EM simulation framework at the layout level, making pre-silicon security verification practical. To achieve this goal, we provide an in-depth view of EM emanations from ICs and an understanding of which elements contribute with more proportion. Guiding by this, we implement multiple techniques, including device model approximation and parasitic network reduction for the current analysis and GPU acceleration for EM computation. These techniques speed up the EM simulation process by a factor of 32. To verify the efficacy of the simulation framework, we fabricate S-Box and AES chips using SMIC 180nm CMOS technology. Results show that simulation results are consistent with physical measurements. Specifically, the intrinsic accuracy reaches 74% in the time domain and 98% in the spatial domain. Also, the security evaluation results

have a prediction accuracy of 93%.

For evaluation scenarios with large data volumes, we integrate the layout-level EM simulation with machine learning, and optimize the security evaluation via the generative adversarial network (GAN). The designed GAN model will extract the mapping from the physical layout to EM emanations. Thereinto, the generator creates EM emanations while the discriminator evaluates them. Through iterative adversarial training between them, predicted data from the generator are close to real EM distributions. Then in process of the security evaluation, the GAN model can quickly produce specified amounts of EM emanations. The validation experiments are performed using AES, Kyber and other two protected designs. Results show that the optimized framework improves the efficiency of security measurements with large-scale data, while maintaining accurate evaluation results. When evaluation data increase to 100K, this prompts the efficiency by a factor of 73.48 $\sim$ 86.05.

Most of the existing countermeasures result in high circuit overhead and design costs. To address these issues, we propose side-channel protection through automatic leaky paths identification and obfuscation. In techniques of path identification, we first locate partial logic cells that leak the most information through dynamic correlation analysis. Then we exploit static security checking to construct complete leaky paths based on these cells. In techniques of path obfuscation, we design the local path masking by combining Boolean masking and random precharge. Logic transformation is exploited to deploy protection solutions on leaky paths automatically. Based on the above techniques, we design a hardened AES circuit against EM SCA attacks. Experimental results demonstrate more than 1066× improvements in side-channel resistance. With respect to area, power and performance, this hardware protection only incurs 6.53%, 4.51% and 3.1% overheads.

KEY WORDS： Cryptographic integrated circuits, Electromagnetic analysis attack, Pre-silicon security evaluation, Electromagnetic emanation simulation, Side channel countermeasure

目　录

第 1 章　绪论

1.1　研究背景与意义

随着现代社会信息化进程的不断深入，信息技术已经渗透到金融政务、移动通信、工业生产、社会保障等关系国计民生的各个领域。同时，信息技术与各领域多学科的深度交叉融合，催生出物联网、云计算、大数据、人工智能等高新技术和产业。可以说，没有信息化就没有现代化，信息技术已经成为建设现代化国家的战略性、基础性和先导性力量。然而，由于固有的复杂性与脆弱性，信息技术在引领社会发展的同时，也引发了日益突出的信息安全问题，如网络黑客、隐私侵犯、远程监控、网络威慑等。例如，“震网”病毒控制离心机转速破坏了伊朗核设施，使得伊朗核计划被迫流产。妥善地解决信息安全问题，是确保人民生活和国家安全的迫切需要。

密码技术是信息安全的压舱石，能够提供数据加密和安全认证服务，从而保障信息的机密性、完整性和可用性等要素。典型的密码算法包括对称密码算法、公钥密码算法和摘要算法，例如高级加密标准 (Advanced Encryption Standard，AES) 算法、RSA算法和椭圆曲线密码 (Elliptic Curve Cryptography，ECC) 算法。鉴于每类密码算法各有优缺点，绝大多数的实际应用采用混合加密方案，对称密码算法负责数据传输，而公钥密码算法用于密钥配送。这样既解决了公钥密码算法处理速度慢的问题，又解决了对称密码算法密钥配送难的问题，实现了两类密码算法的优势互补。依据柯克霍夫原则，除密钥之外，现代商用密码系统都是公开且已知的。在密钥安全的前提下，即使攻击者知晓了所有设计与应用细节，密码算法依旧安全。因此，密码技术的安全应用可以归结为密钥安全性问题。该问题贯穿密码算法的理论设计和物理实现，并与不同层面的密码分析方法相对应。

经典密码分析集中在密码算法的理论设计层面，通过数学分析法和蛮力攻击法降低密钥恢复的复杂度。常见的数学分析方法包括差分密码分析、线性密码分析和代数密码分析等。经典密码分析依托于黑盒攻击模型，即攻击者只能掌握密码算法的输入与输出信息，如明文与密文，而无法获取密码算法的任何中间变量。随着设计复杂度和密钥长度的增加，在量子计算发展成熟前，现代密码算法的安全强度已经足够抵抗经典密码分析。以对称密码算法为例，在现有计算资源下，攻击者需要几十年才能破解128位的算法密钥。

然而，严格论证的理论安全无法保证密码算法的物理安全。在实际应用中，密码算法通常以产品实体的形态存在，具体可分为密码软件、芯片、模块、板卡、整机和系统。其中，密码芯片是承载密码算法的集成电路。与密码软件相比，密码芯片具有更高的安全性和更快的运算速度。同时，密码芯片还是密码模块乃至密码系统的底层硬件基础。随着微电子技术的快速发展，基于专用集成电路 (Application Specific Integrated Circuit，ASIC) 的密码芯片已广泛应用到信息安全产业。根据数据预测，我国密码芯片行业的市场销量将于2023年增长至1793.9亿颗。因此，密码芯片作为信息安全的重要载体，其物理实现的安全性需要得到充分分析。在运行过程中，密码芯片与周边环境始终存在物理交互，不可避免地泄露功耗、电磁、延时、声音和光子等物理信息。上述物理信息统称为侧信道信息，能够侧面反映密码算法的中间变量。依托于灰盒攻击模型，攻击者通过采集密码芯片的侧信道信息，借助统计分析方法即可破解算法密钥，具体流程如图1-1所示。区别于经典密码分析，侧信道分析 (Side Channel Analysis，SCA) 有效利用了侧信道信息和算法密钥的内部关联，极大地降低了算法密钥的搜索难度。侧信道分析自提出伊始，由于实施成本低、操作隐蔽性强、攻击效果显著等优势，引起了学术界和工业界的持续关注。

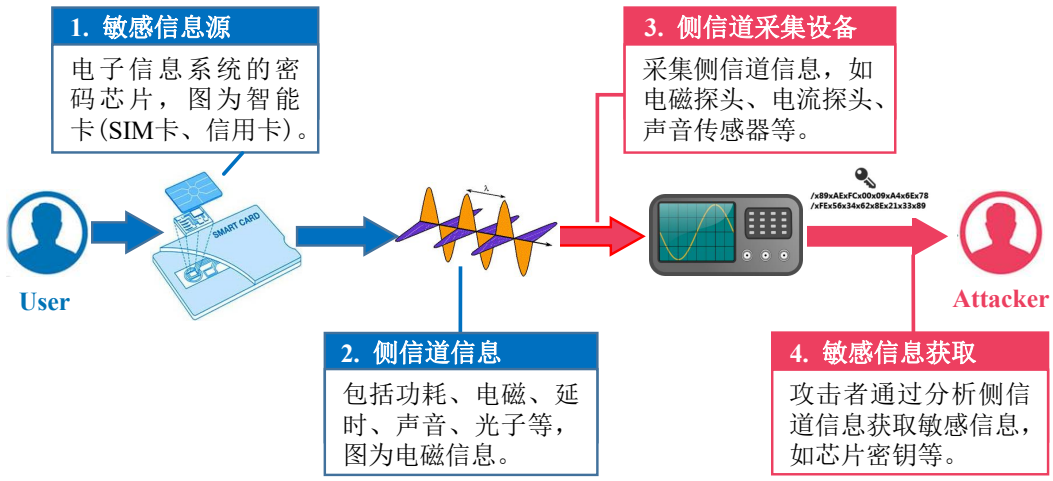


图 1-1　针对密码芯片的侧信道攻击流程

在诸多侧信道信息中，关于功耗和电磁的研究与应用最为广泛。两者都根源于芯片内部的电流效应，但是具备不同的表现形式。功耗反映了芯片电流的整体行为，通常是所有电路模块功耗的总贡献，这意味着攻击者很难将密码模块的功耗从中分离开。同时，功耗的测量需要改动芯片电源端的电路，如在电源支路串联电阻器。因此，对于采用内置电源供电的芯片，功耗信息的应用具有一定的局限性。而电磁反映了芯片电流的空间行为，攻击者能够借助近场探头定位到芯片的局部区域，非接触式地采集密码模块的电磁场信息。这种测量

方式可以剥离其他模块引入的噪声影响，从而获得具有较高信噪比的电磁数据。近年来，电磁分析攻击是最具威胁性的侧信道攻击手段之一，相继破解了众多智能终端芯片的密码算法，如德州仪器AM335x处理器 [1]、海思麒麟620处理器 [2]、恩智浦LPC55S6x处理器 [3]和苹果A10 Fusion处理器等 [4]。

表 1-1 密码芯片的安全标准

序号	标准号	标准名称
1	GB/T 40653-2021	信息安全技术 安全处理器技术要求
2	GM/T 0082-2020	密码模块非入侵式攻击缓解技术指南
3	GB/T 38625-2020	信息安全技术 密码模块安全检测要求
4	GB/T 36950-2018	信息安全技术 智能卡安全技术要求 (EAL4+)
5	GB/T 37092-2018	信息安全技术 密码模块安全要求
6	GB/T 22186-2016	信息安全技术 具有中央处理器的IC卡芯片安全技术要求
7	ISO/IEC 17825-2016	信息安全技术 缓解非侵入性攻击对密码模块的测试方法
8	YD/T 1886-2015	移动终端芯片安全技术要求和测试方法
9	JR/T 0098.2-2012	中国金融移动支付 检测规范 第2部分：安全芯片
10	GM/T 0008-2012	安全芯片密码检测准则

电磁分析攻击对密码芯片提出了更高的安全需求。国内外制定了众多国家和行业标准，用以指导密码芯片的安全技术与安全检测，如表 1-1所示。上述标准指出，高安全等级的密码芯片应具有抵抗电磁分析攻击的能力。例如，GB/T 37092-2018标准规范了通用的安全测评流程，ISO/IEC 17825-2016标准规定了高安全等级对测评数据量的要求，GM/T 0082-2020标准给出了电磁分析攻击的部分缓解技术。随着《密码法》的颁布与实施，密码上升到国家法律层面，合规成为密码芯片的刚性需求。在投入使用之前，高安全等级的密码芯片必须配备安全防护方法，并通过国家和行业标准的安全性测评。需要注意的是，随着芯片集成度越来越高，其设计和制造环节变得异常复杂，导致芯片研发具有冗长的时间周期和高昂的流片成本。然而，当前的安全测评集中在硅后阶段，如果在该阶段发现信息泄露问题，密码芯片只能重新经历设计与制造环节，“设计-生产-测评”的多轮迭代极大增加了研发周期和流片成本。除此之外，当前的安全防护缺乏对信息泄露源头的认知，设计者无法针对性地应用防护技术，导致大量的功耗、性能和面积开销。在此背景下，本论文的研究围绕安全测评与增强两个方面，将侧信道安全融入到芯片设计和验证环节，构建测评与增强相结合的密码芯片开发流程，有效解决阻碍信息安全领域进一步发展的关键问题。本论文的研究将提高密码芯片的安全性，夯实社会信息化发展的基石，具有十分重要的理论意义和应用价值。

1.2 国内外研究现状

密码学家Paul Kocher于1999年提出了差分功耗分析 (Differential Power Analysis，DPA) [5]，开辟了侧信道分析这一全新的研究领域。在此之后，研究者将侧信道信息的概念从功耗延伸至电磁、延时、声音、光子和缓存等众多物理信息，拓展了侧信道分析的应用范围。其中，电磁信息具有空间定位精确、测量方式灵活和信息量丰富的优点，得到愈加广泛的研究与应用，也使得电磁信息安全成为密码芯片的实际需求。本节围绕电磁信息安全的测评与增强两个方面，对相关技术的国内外现状进行梳理和分析。

1.2.1 安全测评研究进展

安全测评在密码行业中发挥着至关重要的作用，目的是衡量密码产品是否足够安全，并辅助进行安全缺陷的定位和解析。具体到密码芯片面临的电磁分析攻击，安全测评通常分为电磁采集和电磁分析两个阶段，如图1-2所示。电磁采集阶段采集密码芯片工作泄露的电磁信息，而电磁分析阶段对采集到的电磁信息进行数据处理和安全评估。根据电磁采集阶段的差异，本论文将安全测评分为硅后安全测评和硅前安全测评。在硅后安全测评中，密码芯片已完成制造环节，通过对实体产品进行测试获取电磁信息。相对应地，在硅前安全测评中，密码芯片尚处于设计环节，通过对设计数据进行仿真获取电磁信息。

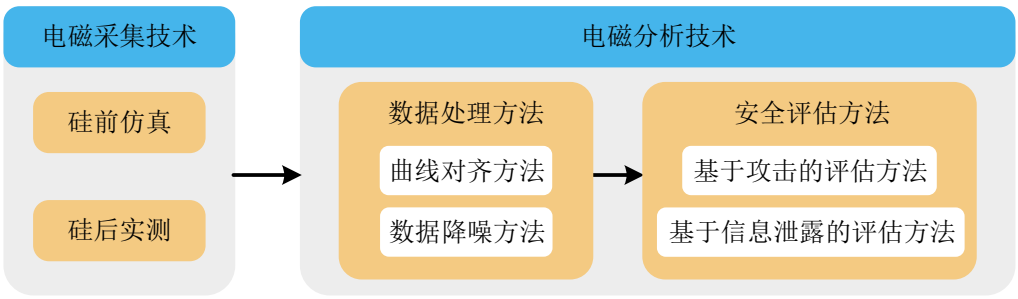


图 1-2 电磁安全测评技术概述

1.2.1.1 硅后安全测评技术

早在20世纪50年代初期，美国军方发现信息设备无意发射的电磁波会导致敏感信息的泄露，随即启动了名为信息设备的电磁信息泄露防护与收集技术 (Transient Electromagnetic Pulse Emanation Surveillance Technology，TEMPEST) 的研究计划。针对处理、传输和存储敏感信息的电子设备，TEMPEST计划通过制定技术标准和测试方法降低电磁辐射带来的泄密风险。2001年，Gandolfi等人对

电磁信息泄露进行了原理分析，并针对微控制器运行的密码算法开展了实际的电磁分析攻击 [6]。同年，Quisquater等人规范了电磁分析方法，提出简单电磁分析 (Simple Electromagnetic Analysis，SEMA) 和差分电磁分析 (Differential Electromagnetic Analysis，DEMA) [7]。他们指出，电磁信息相对于功耗信息具有额外的信息维度，即随时域变化的空间信息。2002年，Agrawal等人将电磁信息分类为直接辐射和间接辐射，间接辐射表现为幅度调制和角度调试信号 [8]。同时，他们的实验表明电磁分析攻击能够攻破抗功耗分析攻击的智能卡芯片。2004年，Brier等人将汉明重量模型推广为汉明距离模型，以皮尔逊相关系数作为区分函数，提出了相关电磁分析 (Correlation Electromagnetic Analysis，CEMA) [9]。同年，Rechberger等人优化了模板攻击的流程，通过主成分分析选取建模泄漏点，采用离散傅里叶变换降低电磁数据噪声，提升了传统模板攻击的攻击效果 [10]。

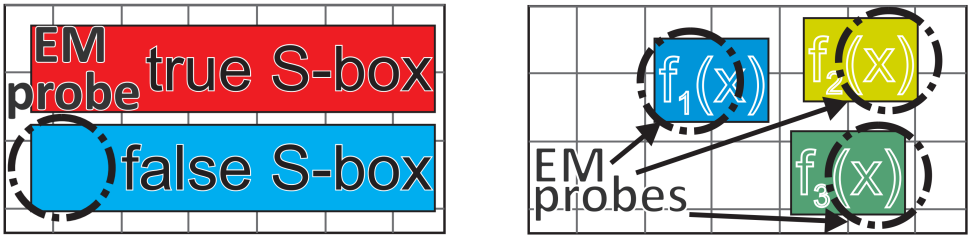
(1) 电磁分析技术

为了提升电磁分析阶段的效率，研究者在数据处理和安全评估方面做了大量改进和创新。通常来说，涉及这两方面的研究不局限于某种特定的侧信道信息，大部分方法同时适用于密码芯片的功耗和电磁信息。本节仅列出了采用电磁信息进行效果验证的研究工作。2005年，Gebotys等人将电磁分析攻击建立在频域之上，有效避开了随机延迟对时域信号的影响 [11]。2006年，Homma等人提出了基于相位的波形匹配技术，选择特定样本曲线做参考基准，通过离散傅里叶变换的相位分量来预测位移偏差并实现曲线对齐 [12]。2011年，Meynard等人运用信号解调技术来提高SEMA的攻击效率，由基于互信息的特征化方法确定解调频率和带宽 [13]。在此基础上，Perin等人提出了全数字幅度解调技术，有效提取出公钥算法中多种硬件运算的泄露信息 [14]。同年，Hospodar等人首次将机器学习引入模板攻击，用支持向量机算法解决密钥恢复的分类问题 [15]。机器学习与模板攻击的结合，赋予了电磁分析攻击新的活力。2013年，Heyszl等人引入无监督聚类算法，攻击者无需对相同设备进行事先建模，从而降低了实际攻击的复杂度 [16]。2016年，Özgen等人比较了朴素贝叶斯分类、K最近邻分类和支持向量机分类在模板攻击中的成功率 [17]。2019年，Picek等人优化了卷积神经网络在模板攻击中的应用，通过合成少数类过采样技术解决了非平衡数据问题 [18]。2021年，Yu等人采用元学习和迁移学习实现了跨设备跨域攻击，极大地拓展了模板攻击的应用场景 [19]。区别于上述攻击性评估方法，基于信息泄露的评估方法不以密钥恢复为目的，而是通过统计检验来探测密码实现是否存在某种敏感信息泄露。这类研究致力于摆脱攻击场景的限制，如Standaert等人于2009年提出的通用测评框架，通过互信息形式化地度量攻击者可利用的信息泄露 [20]。2011年，Gilbert等人提出了测试向量泄露评估 (Test Vector Leakage Assessment，TVLA) 技术，使用t检验摆脱了攻击性评估的先验知识，得到了学术界和工业界

的广泛重视[21]。2015年，Schneider等人完善了TVLA技术的理论背景，并提出了规范的高阶评估流程[22]。2018年，Moradi等人用卡方检验作为t检验的补充，降低了TVLA技术的误报率，有效提高了实际评估的准确度[23]。

(2) 电磁采集技术

作为安全测评的主体，电磁信息的质量与采集设备和测试手段密切相关。2012年，Heyszl等人提出了局部电磁分析的概念，该方法采用高分辨率的近场探头，近距离地采集密码芯片表面的电磁信息[24, 25]。作者通过实验归纳出以下结论，首先，电磁曲线具有比功耗曲线更高的信噪比，可以揭示更多的信息泄露。其次，电磁曲线能够反映不同的电路布局，具有额外的空间信息维度。2017年，Unterstein等人采用局部电磁分析聚焦目标电路的泄露信息，实现了电路并行噪声的有效隔离[26]。同年，Immler等人借助局部电磁分析破解了双轨预充电逻辑[27]。如图1-3 (a)所示，双轨预充电逻辑具有互补输出的逻辑门结构，通过功耗平坦化能够有效抵抗功耗分析攻击。然而，局部电磁分析可以利用电路布局和布线的特征，绕过互补逻辑门直接测量原始逻辑门的电磁信息，从而降低了双轨预充电逻辑的保护效果。2018年，针对抗功耗分析的二阶门限掩码方案，如图1-3 (b)所示，Specht等人分别定位到各个掩码变量的电磁信息，通过局部信息的时域合成实现了二阶门限掩码的破解[28]。总结来说，成功的局部电磁分析需要考虑三个因素，首先将近场探头放置在尽可能靠近芯片表面的位置。在相同的噪声环境下，探头距离越近磁场强度便越高，意味着采集数据具有较高的信噪比。其次，要合理的选择近场探头的尺寸，尺寸较小的近场探头具有较高的分辨率，而尺寸较大的近场探头具备良好的灵敏度。需要注意的是，采用直径为3mm的探头进行电磁分析攻击时，显示出与功耗分析攻击相似的结果[27]。最终，将近场探头定位到泄露更多信息的位置，即信息泄露热点，能够最大化地利用电磁信息的空间特性。



(a) 双轨预充电逻辑[27]　　(b) 门限实现掩码[28]

图 1-3　局部电磁分析攻击实例

2019年，Iyer等人提出了一种自适应的近场扫描方法，在探头坐标、方向和曲线数量组成的四维空间中，采用贪心算法搜索最佳参数配置[29]。2020年，

Danial等人提出了自动化的电磁分析攻击框架，该框架以TVLA作为泄露度量，使用贪婪梯度搜索定位信息泄露热点[30]。在工业界，德国Langer公司研制出多款近场探头，包括ICR HH系列近场微探头和RF系列无源近场探头，大幅度推动了电磁采集技术的发展。荷兰Riscure公司和法国Secure-IC公司也相继推出了电磁采集和分析设备，用于测评密码产品的侧信道安全性。结合先进的电磁采集和分析技术，eShard公司于2019年破解了智能手机的密码协处理器芯片[31]。

(3) 国内研究现状

相对来说，国内的相关研究工作起步较晚，早期研究处于技术追赶阶段。但是经过多年的发展，在电磁采集和电磁分析技术方面取得了长足进步。2009年，邓高明等人组合电磁频率分析和传统模板攻击的优点，成功降低了随机延迟插入的防护效果[32]。随后，陈开颜等人分别研究了远场和近场电磁信息，并开展了密码芯片的CEMA和DEMA攻击[33, 34]。2012年，段二朋等人分析了电磁信息泄露机理，提出了DEMA和CEMA尖峰模拟分析方法[35, 36]。2013年，孙春辉等人通过电磁分析攻击破解了PRESENT密码算法的全部密钥[37]。2014年，刘飚等人提出了多种电磁模板攻击方法，包括单比特电磁模板攻击、快速电磁模板攻击、基于监督学习的电磁攻击和基于无监督学习的电磁攻击[38]。2015年，Zhang Hongxin等人组合小波变换和主成分分析的优点，提升了电磁模板攻击的分类效率[39]。2016年，Zhou Xinping等人提出了基于奇异值分解的预处理方法，挑选部分有用的电磁曲线以提高电磁分析效率[40]。同年，Ou Changhai等人提出了多兴趣点组合的区分函数，用于减少DEMA和CEMA攻击所需的电磁曲线数目[41]。2019年，Zhou Wenhai等人通过明文筛选减少了CEMA攻击执行的时间开销[42]。在工业界，观源科技、纽创信安和智慧云测等信息安全公司纷纷推出了用于电磁安全测评的采集与分析平台。2020年，南方电网科学研究院采用电磁分析攻击破解了海思麒麟620处理器芯片运行的密码算法[2]。

1.2.1.2 硅前安全测评技术

在硅前电磁安全测评中，由电磁仿真模拟真实芯片的电磁信息，在设计阶段评估密码芯片的安全性。得益于计算电磁学的发展，已经有多种麦克斯韦理论的数值算法，衍生出以Ansys HFSS为代表的电磁仿真工具，适用于设计和仿真高频电子产品，例如天线、射频或微波组件、高速封装和印刷电路板。然而，由于复杂的物理结构和电气行为，现有工具无法仿真集成电路的电磁辐射，只能用来分析简单互连线的电磁场。例如，Khan等人利用Ansys HFSS探索了电源网络简化模型的电磁幅频特性[43]。总结来说，芯片电磁仿真面临着诸多挑战。首先，晶体管的伏安特性受到多种非理想效应的影响，例如衬底偏置效应、沟道长度调制效应和亚阈值效应等。其次，金属线的寄生阻抗随尺寸缩小急剧增

大，线间距的减小带来了更大的寄生电容，形成了规模庞大的寄生参数网络。因此，晶体管和互连线的精确建模对电流分析尤为重要。与此同时，电流元的激发磁场会相互叠加或抵消，在芯片内部传播时还会遇到多层金属，很大程度上影响了最终的电磁信息。为实现硅前安全测评，研究人员陆续提出了很多技术，用于仿真密码芯片的电磁辐射。该类技术最早起源于剑桥大学的EMA项目，Li等人构建了全局电磁信息的建模流程，包括瞬态电流仿真、寄生参数提取和电磁辐射计算等环节，成功预测了同步处理器和异步处理器的信息泄露差异 [44]。2007年，Peeters等人提出了基于翻转距离的信息泄露模型，适用于门级网表层次的电磁仿真，在一定程度上可以反映敏感信息的泄露情况 [45]。2008年，Ordas等人通过对芯片表面的近场扫描，证实较高金属层的电源网络流动着较大电流 [46]。在上述实验结果的基础上，Lomné等人初步提出了版图级电磁仿真流程，由Ansys RedHawk仿真电源网络的瞬态电流，叠加电磁场获取任意位置的电磁信息 [47]。2017年，Kumar等人提出了混合层级的电流分析方法，结合Synopsys FineSim的并行运行机制，提升了版图级电磁仿真效率 [48]。2021年，意法半导体从空间信息和安全测评角度，通过仿真数据与实际测试的对比，验证了版图级电磁仿真流程的准确度 [49]。

2019年，美国国防高级研究计划局 (Defense Advanced Research Projects Agency，DARPA) 正式启动“安全硅的自动实现” (Automatic Implementation of Secure Silicon，AISS) 计划，组建了包括Synopsys公司、ARM公司、IBM公司、佛罗里达大学和诺斯罗普·格鲁曼公司等在内的研究团队。作为AISS计划的重要环节，SCATE项目旨在研究电磁和功耗信息的硅前安全测评技术。近几年，通过学术界和工业界的协同合作，国外已从点到面融合各领域的研究工作，实现了硅前安全测评的快速发展。相对来说，我国在该方面的研究还处于起步工作，只有少数高校和科研单位进行了初步研究。2014年，芯和半导体推出面向片上无源器件的电磁仿真软件IRIS。2016年，杜逸璇等人针对高频集成电路，结合等效偶极子模型和时域有限差分法，提出了集成电路电磁干扰建模与预测方法 [50]。2020年，He Jiaji等人提出了基于权重的汉明距离模型，优化了传统电磁辐射模型，构建了寄存器传输级 (Register Transfer Level，RTL) 电磁信息预测与评估流程 [51]。

综上所述，相比于硅后阶段的安全测评，硅前阶段的安全测评技术具有以下优势。首先，一切测评是为了更安全的设计，安全测评发生在密码芯片的设计环节，有利于尽早发现信息泄露问题，以更高的灵活性开展安全设计。其次，硅后安全测评受实际采集设备的影响，特别是近场探头的性能和采集点的位置，而硅前阶段的安全测评摆脱了上述限制，通过仿真定位任意位置的电磁信息，以更高的分辨率检测信息泄露问题。因此，从设计者的角度出发，将安全测评

移至硅前设计阶段，集成到传统的验证环节，是缩短研发周期和降低流片成本的必然选择。可以看出，硅前阶段的电磁安全测评需要多项学科的交叉融合，覆盖集成电路、电磁学、电子设计自动化 (Electronic Design Automation，EDA) 和密码学等领域。其中，电磁分析技术的发展已较为成熟，但芯片电磁仿真的研究还存在很多问题。一方面，很多方法缺乏充足的理论依据，相应的电磁仿真流程也不够完善，不仅无法充分刻画电磁信息特征，还具有沉重的时间和资源负担，限制了其在安全测评的实际效果。另一方面，测试高安全等级的密码芯片时，往往需要数万乃至上百万条电磁曲线，这对电磁仿真效率提出了更高要求，以保证硅前安全测评的实用性。因此，在设计阶段获得准确的电磁数据，降低芯片电磁仿真的计算成本，优化大规模数据量的测评效率，是硅前安全测评亟需解决的关键问题。

1.2.2 安全增强研究进展

为了抵抗电磁分析攻击，研究者已提出多种安全增强方法，分别作用于密码芯片、传播路径和近场探头。一般来说，可以采用屏蔽材料切断电磁信息的传播路径，或通过片上感知单元探测近场探头的存在 [52–54]。对于密码芯片本身的安全增强，核心思想包括隐藏和掩码两类。与功耗分析防护不同的是，电磁安全增强需要考虑电磁信息的空间特点。本节仅列出经过电磁分析攻击验证的研究工作。

(1) 隐藏技术

隐藏技术旨在减弱电磁信息泄露和密码中间值的相关性，包括时间维度的隐藏技术和振幅维度的隐藏技术。通常来说，电磁分析攻击需要收集固定时刻的电磁信息进行密钥恢复，若该条件不能满足，则攻击难度大幅提高。振幅维度的隐藏则致力于降低敏感信息在全部电磁信息的比例，使攻击者难以捕获到有用信息。2016年，Ngo等人验证了主动屏蔽层附带的电磁安全抗性 [55]。2018年，Singh等人提出了抗电磁分析攻击的随机快速电压抖动架构，利用高频高带宽的集成稳压电路随机化密码模块的电源供应，随后借助全数字时钟调制电路随机化密码模块的时钟频率 [56]。在此基础上，Singh等人增加了噪声植入电路和电压随机化电路，构成了安全敏感的片上低压差线性稳压器 [57]。2019年，Das等人提出了用于消除电磁信息泄露的STELLAR方法，采用较低金属层的局部电源网格为密码模块供电，并将密码模块嵌入到电流衰减电路中，使得敏感信息难以通过较高层的全局电源网格发射到外界 [58]。随后，Das等人优化了STELLAR方法的电流衰减电路，将密码模块的电磁信息减弱350倍以上，远远低于实验环境的噪声水平 [59, 60]。2020年，Li等人提出了数据流空间随机化方法，将状态寄存器和字节替换模块随机映射，通过仿真实验证明了抗局部电磁分析效果 [61]。

2021年，Blackstone等人研究了STELLA的调度算法iSTELLAR，在保持安全性的同时降低了功耗开销 [62]。Ghosh等人提出了综合友好的Syn-STELLAR方法，优化了电流衰减电路的工艺迁移性，并进一步提升了电磁安全抗性 [63, 64]。同年，Nath等人探索了电源网络的布局模式对电磁信息泄露的影响，并进行了概念原型验证 [65]。Wang等人提出了电源网格屏蔽、电源网格扭转、局部去耦电容和模块隔离布局等物理防护策略，具有一定的抗局部电磁分析效果 [66]。2022年，Fang等人提出了自适应的电磁安全修复架构，由特征提取、信息预测和能量补偿电路构成 [67]。

(1) 掩码技术

掩码技术通过随机化密码中间值来切断其与电磁信息的依赖关系。具体来说，该技术将密码中间值拆分成$n+1$份变量，包括1个掩码型中间值和n个掩码，其中n代表掩码方案的阶数。根据秘密共享的思想，只给定$n+1$份变量中的任意n个，不会泄露关于原始值的任何信息。布尔掩码和算术掩码是两类典型的掩码实现，多应用于算法层次，且跟密码算法的类型密切相关。2005年，Oswald等人以AES算法为研究对象，通过改进有限域求逆对字节替换盒S-Box实施了掩码防护 [68]。后续，Canright等人通过逻辑优化降低了掩码型S-Box的面积开销 [69, 70]。2006年，Giraud等人针对RSA公钥密码算法，通过安全模幂运算预防直观的信息泄露行为 [71]。同年，Mangard等人发现掩码方案的物理实现降低了算法可证明安全，毛刺现象使得密码中间值明文化并在某些时刻泄露出来 [72–74]。类似于安全多方计算，Nikova等人在2011年提出了门限掩码方案，能够抵抗毛刺现象对安全性的影响 [75, 76]。2013年，Maistri等人验证了布尔掩码和算术掩码抵抗电磁分析攻击的有效性 [77]。2014年，Masoumi等人运用随机化的有限域运算有效应对了一阶DEMA攻击 [78]。其后，研究者提出了大量的掩码优化方案，不断地降低开销、提高性能和增加安全性 [79–84]。同时，为了降低掩码实现的复杂度，Bayrak等人在算法层提出了自动实现流程，包括泄露分析、指令定位和代码转换等环节 [85]。2017年，Huss等人提出了安全驱动的逻辑综合流程，能够在硬件层自动加入掩码型元件 [86]。2020年，Kumar等人将掩码型列混淆模块与其他防护方案组合，提出了抗电磁分析攻击的轻量级密码硬件模块 [87, 88]。2022年，Intel公司设计了高吞吐量的可重构密码硬件引擎，基于掩码方案提供了抗电磁攻击的工作模式 [89]。

电磁安全增强技术得到了业界的重点关注，近三年来，国际固态电路会议(IEEE International Solid-State Circuits Conference，ISSCC) 已收录了4款具有抗电磁分析攻击能力的密码芯片。相比于国外，国内研究集中在抗功耗分析攻击方面，大部分方法没有经过电磁分析攻击的验证。在电磁安全增强方面，2011年，常小龙等人设计了抗电磁分析攻击的动态差分掩码防护逻辑，通过半定制流程

构造了掩码型S-Box电路 [90]。2018年，Wang Chenguang等人提出电磁均衡的概念，通过插入局部电容平坦化电源网络的电磁信息 [91]。2022年，曹宇文等人设计了随机预混淆逻辑单元，通过混淆逻辑状态达到隐藏电磁信息的目的 [92]。

综上所述，围绕着隐藏技术和掩码技术，安全增强的实现方式不断翻新，密码芯片的安全水平不断提升。然而，很多方法具有很高的功耗、性能或面积牺牲，部分硬件实现存在全定制或半定制的设计需求，限制了这些安全防护方法的实际应用。针对上述挑战，将溯源和增强结合是切实可行的技术思路，对于待防护的密码芯片，首先识别其中的信息泄露根源，然后针对性设计和实施安全增强策略，以较少的功耗、性能和面积开销提升侧信道抗性。

1.3 论文研究内容与主要创新点

1.3.1 论文研究内容

本论文针对电磁分析攻击的安全威胁，在总结现有安全测评和防护方法的基础上，开展了密码芯片硅前安全测评和增强技术研究。为了实现硅前安全测评，完善了芯片电磁仿真的理论依据，提出了版图级电磁仿真方法，改进了电流分析和电磁计算环节，在准确模拟电磁信息的同时，降低了整个过程的计算成本。针对高安全等级的芯片测评场景，将机器学习与芯片电磁仿真相结合，提出了基于生成对抗网络的测评优化方法，能够快速合成测评规定的海量数据，提升大规模数据量的测评效率。对于存在信息泄露的密码芯片，提出了安全溯源和靶向增强方法，可以识别敏感信息的泄露路径，自动地部署局部路径掩码方案，实现安全水平和电路开销的有效权衡。通过解决上述研究遇到的关键问题，形成了测评与增强相互融合的安全设计流程。后续章节的内容安排如下：

第二章重点介绍了典型密码算法的原理实现，分析了电磁信息泄露模型的构造方式，阐明了电磁分析攻击技术的具体流程，并讨论了抗电磁分析攻击的防护方法，为深入研究硅前安全测评和增强技术奠定了基础。

第三章首先建立了芯片电磁分析模型，探究了电流聚合效应和金属屏蔽效应，阐明了电磁信息的根本源头和主导因素，为芯片电磁仿真提供了理论支撑。基于此，提出了版图级电磁仿真方法，包括数据准备、电流分析和电磁计算环节，通过多种模型简化和仿真加速技术，实现了电磁信息的高效预测。最后，完成了两款密码芯片的流片制造，使用近场扫描系统开展实际测试，验证了版图级电磁仿真方法的有效性，以及应用到硅前安全测评的准确度。

第四章首先介绍了生成对抗网络的相关原理，分析了其加速芯片电磁仿真的优势。基于此，提出了测评优化方法的具体流程，由数据准备、模型训练和

风险量化组成，讨论了生成对抗网络的模型结构，以及各环节涉及的处理算法。最后，采用四种实验电路分析了优化方法的有益效果，相比于传统测评方法，该方法能快速合成磁场数据，提升了大规模数据量的安全测评效率。

第五章首先提出了泄露路径识别技术，采用动态关联度分析和静态安全性检验，构建了敏感信息的泄露路径，以达到安全溯源的目的。在此基础上，将布尔掩码和随机预充电组合，提出了局部路径掩码方案及其部署算法，实现了密码芯片的靶向增强。根据上述研究设计了增强型AES电路，通过仿真验证表明，该方法在提升安全性的同时，有效降低了功耗、性能和面积开销。

第六章总结了本论文工作以及研究成果，并展望了未来的研究工作。

1.3.2 主要创新点

本论文聚焦硅前安全测评与增强技术，旨在解决电磁分析攻击的安全威胁，进一步提升密码芯片的安全水平。为此，提出了芯片电磁仿真和安全测评优化方法，在设计阶段评估密码芯片的安全性。对于未通过测评的密码芯片，联合安全溯源与靶向增强方法，设计了兼顾安全与开销的防护方案。基于此，本论文的主要创新点如下：

(1) 建立了集成电路的芯片电气模型，考虑复杂的物理结构和电气行为，分析了逻辑单元和金属互连的重要作用，通过电流聚合效应和金属屏蔽效应的数学推导，不仅阐明了电磁信息的根本来源，还明确了顶层电源网格的主导地位，为芯片电磁仿真和安全测评优化提供了理论依据。

(2) 提出了版图级电磁仿真方法，采用器件模型近似、寄生网络约减和GPU并行计算，改进了电流分析和电磁计算环节，相比传统方法提升了32倍的时间效率，降低了硅前阶段开展安全测评的难度。设计了S-Box和AES芯片并完成了流片制造，验证了版图级电磁仿真方法的有效性，其中时域准确度高于74%，空间域准确度高达98%，安全测评准确度为93%。

(3) 提出了基于生成对抗网络的测评优化方法，设计了生成对抗网络的模型结构，采用模型训练和风险量化算法，提高了大规模测评数据的合成速度，非常适合高安全等级的芯片测评场景。参照ISO/IEC 17825-2016标准，对于安全等级3规定的1万条曲线，测评效率提升了9.22 ~ 9.62倍，对于安全等级4规定的10万条曲线，测评效率提升了73.48 ~ 86.05倍。

(4) 提出了密码芯片安全溯源和靶向增强方法。结合动态关联度分析和静态安全性检验，提出了泄露路径识别技术，可以准确定位敏感信息的泄露路径。组合布尔掩码和随机预充电的优点，设计了局部路径掩码方案，能够自动实现泄露路径的靶向增强。该方法将芯片安全水平提升了1066倍，在电路面积、功耗和性能方面，仅产生6.53%、4.51%和3.1%的额外开销。

第 2 章　安全测评及增强技术概述

本章主要介绍安全测评及增强技术的相关原理，包括典型密码算法、电磁信息泄露模型、电磁分析攻击技术和抗电磁分析攻击技术，作为后续章节需要用到的理论基础。

2.1　典型密码算法

密码算法是密码芯片承载的核心功能，包括对称密码算法、公钥密码算法和摘要算法。特别地，随着量子计算技术的快速发展，传统公钥密码算法将被后量子密码算法代替。本节以AES算法和Kyber算法为例，给出安全测评与增强的密码学背景，其中AES是对称密码算法，Kyber是后量子密码算法。

2.1.1　AES密码算法

AES算法是一种经典的对称密码算法，在密码学中也称为Rijndael算法。它的明文分组长度为128位，密钥长度可以为128位、192位和256位，分别称为AES-128、AES-192和AES-256。加密迭代轮数由密钥长度决定，128位的迭代轮数为10轮，192位的迭代轮数为12轮，256位的迭代轮数为14轮。本节以AES-128为例，介绍AES算法的工作原理和设计实现。其中，原始密钥经密钥扩展生成11个轮密钥，每个轮密钥的长度均为128位。16字节的明文和密钥首先进行轮密钥加操作，再进行10轮迭代的加密运算，前九轮依次进行字节替换、行移位、列混淆和轮密钥加操作，而第十轮的加密运算中不包括列混淆操作。图2-1显示了单轮加密运算的结构图。

16字节的输入$A_0, A_0, ..., A_{15}$按字节分别输入到并行的S-Box中。16字节的输出$B_0, B_0, ..., B_{15}$先在行移位层按字节进行置换，然后由列混淆变换$c(x)$进行混淆。最后将128位的子密钥$W[4i + j]$与中间结果进行异或计算。S-Box是唯一的非线性操作，使用字节B_i替换每个状态字节A_i，且不改变该字节在状态矩阵的位置。S-Box通常使用256×8的查找表实现，输入元素与输出元素满足双射关系，如图2-2所示。以状态矩阵的字节F6为例，把该字节的高4位作为行值，低4位作为列值，通过索引查找表确定替换后的字节42。本质上，S-Box是伽罗瓦域求逆和仿射变换构成的数学变换。在伽罗瓦域GF(2^8)中，每个输入元素A_i的逆元为其乘法逆，表示为$B_i' = (b_7', b_6', ..., b_0')$，且定义零元素被映射到自身。在仿射变换中，

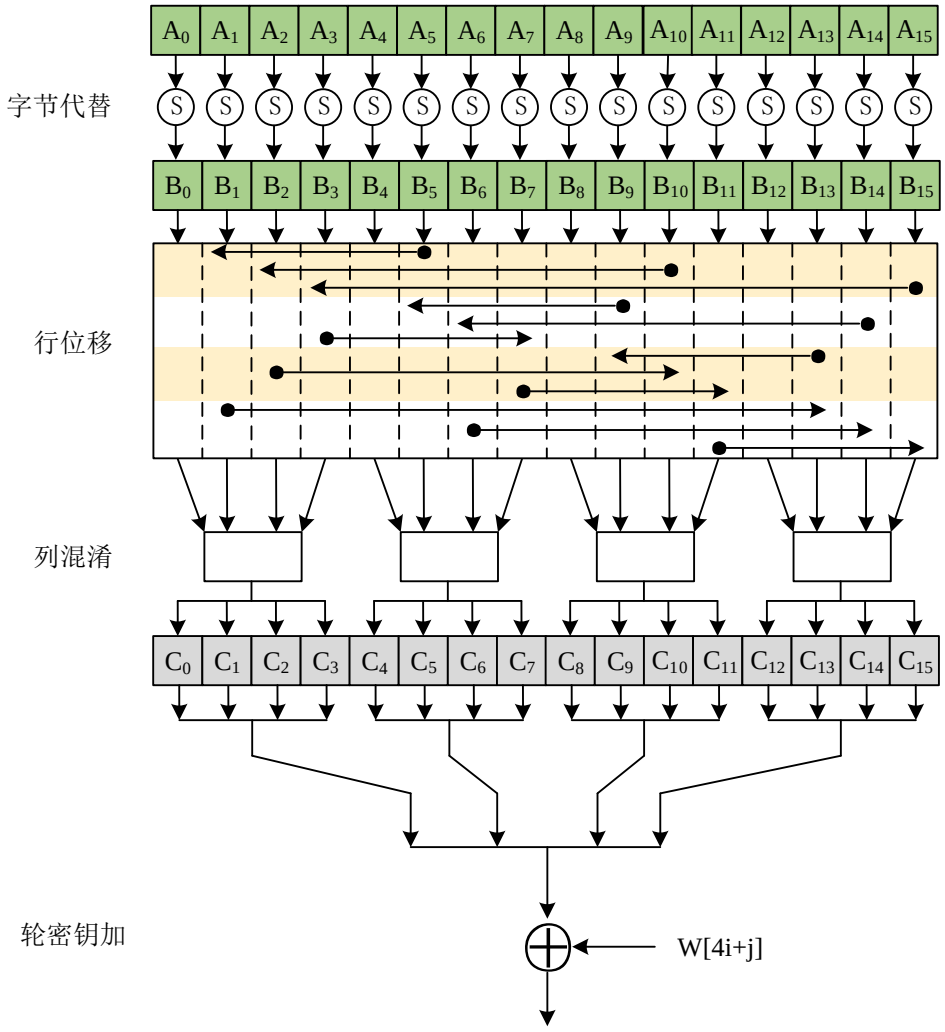


图 2-1　包含四种运算的轮加密

每个逆元字节首先与常量位矩阵相乘，然后再与常向量63相加，各比特运算如公式(2-1)所示，p_i代表常向量的第i位。

$$b_i = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus p_i \tag{2-1}$$

行移位和列混淆操作同属于AES算法的扩散层，将单个位的影响扩散到整个状态矩阵中。行移位将状态矩阵的第二行向右移动三个字节，将第三行向右移动两个字节，将第四行向右移动一个字节。列混淆是对状态矩阵的线性变换操作，将输入状态B的每一列与固定矩阵相乘，得到输出状态C的对应列向量，系数的乘法和加法都在域GF(2^8)中完成，如公式(2-2)所示。经过三轮行移位和列混淆操作后，状态矩阵的每个字节将依赖于所有16个明文字节。轮密钥加是每轮加密运算的最后一个操作，将16字节的状态矩阵和轮密钥按位异或组合起来。

字节替换查找表		低 4 位															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
高 4 位	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

图 2-2 S-Box的查找表实现

$$\begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{bmatrix} \tag{2-2}$$

密钥扩展操作用于生成每轮加密运算需要的轮密钥，其计算过程如图2-3所示。元素$K_0, K_1, ..., K_{15}$表示原始密钥对应的字节，轮密钥被存储在扩展密钥数组W中，表示为$W[0], W[1], ..., W[43]$共44个字节。其中，第一个轮密钥为原始密钥，其他轮密钥的各个字节由公式(2-3)和公式(2-4)计算。

$$W[4i] = W[4(i-1)] + g(W[4i-1]) \tag{2-3}$$

$$W[4i+j] = W[4i+j-1] + W[4(i-1)+j] \tag{2-4}$$

其中，$i = 1, 2, ..., 10$，$j = 1, 2, 3$。在非线性函数g中，输入字节首先按规律翻转位置，得到中间结果$U_0, U_1, ..., U_3$，其后所有字节通过四个S-Box操作，最左边的字节与轮常数RC相加，其值与扩展操作的轮次相关，如$RC[1] = 1$，$RC[i] = 2 \cdot RC[i-1]$。通过以上操作，增加了密钥扩展操作的非线性，并消除了整个密码算法的对称性。

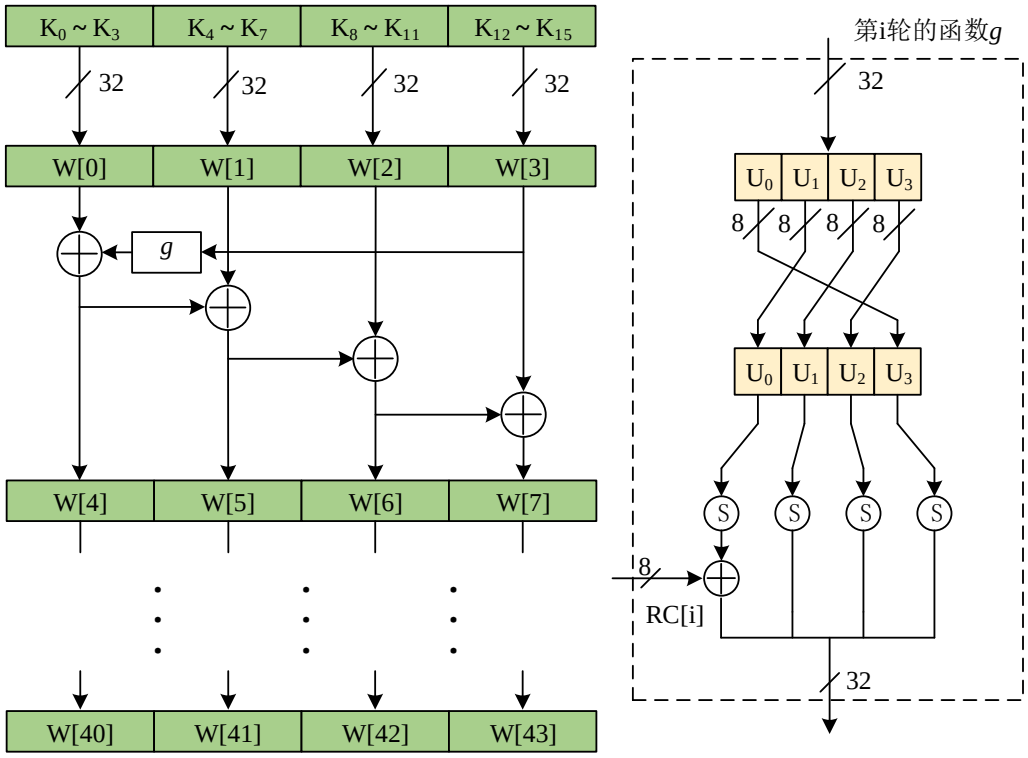


图 2-3　密钥扩展运算

2.1.2　Kyber密码算法

传统公钥密码算法的安全性依托于数学困难问题，例如整数分解问题和离散对数问题，它们的求解难度超越了经典计算机的能力。然而，随着量子计算技术的不断发展，在大规模稳定的量子计算机出现后，这些数学困难问题能够被量子算法轻松解决，现有的绝大多数公钥密码算法也将会被攻破。对于量子计算机带来的安全威胁，后量子密码 (Post Quantum Cryptography，PQC) 算法是有效的应对方案。美国国家标准技术研究所 (National Institute of Standards and Technology，NIST) 早在2012年开始了后量子密码的研究工作，并于2016年启动了全球范围的后量子密码标准征集工作，主要包括公钥加密、密钥封装机制 (Key Encapsulation Mechanism，KEM) 和数字签名，并将算法的安全性、速度与性能、成本和可共享性作为评估标准。经过三轮筛选，NIST于2022年7月公布了首批后量子密码标准算法，包括CRYSTALS-Kyber、CRYSTALS-Dilithium、FALCON和SPHINCS+。

Kyber是用于公钥加密和密钥封装的格密码，由密钥生成、加密和解密过程组成，其安全依赖于模误差学习 (Module Learning With Errors，MLWE) 问题，具有强大的安全性和出色的性能，软硬件实现的性能也位居同类型算法的前列。Kyber算法有三种参数集，对应Kyber512、Kyber768和Kyber1024，分

Algorithm 1 Kyber.CPAPKE.Dec(sk, c)

Input: Secret key $sk \in \mathcal{B}^{12\cdot k\cdot n/8}$

Input: Ciphertext $c \in \mathcal{B}^{d_u\cdot k\cdot n/8+d_v\cdot n/8}$

Output: Message $m \in \mathcal{B}^{32}$

1: $\mathbf{u} := \text{Decompress}_q(\text{Decode}_{d_u}(c), d_u)$

2: $v := \text{Decompress}_q(\text{Decode}_{d_v}(c + d_u \cdot k \cdot n/8), d_v)$

3: $\hat{\mathbf{s}} := \text{Decode}_{12}(sk)$

4: $m := \text{Encode}_1(\text{Compress}_q(v - \text{NTT}^{-1}(\hat{\mathbf{s}}^T \circ \text{NTT}(\mathbf{u}))), 1)$

5: ▷ $m := \text{Compress}_q(v - \mathbf{s}^T\mathbf{u}, 1)$

6: **return** m

别代表算法的三种安全等级。具体到Kyber的算法实现，Kyber.CPAPKE是具有选择明文攻击下不可区分性 (Indistinguishability under Chosen Plaintext Attack，IND-CPA) 的公钥加密方案，而Kyber.CCAKEM是具有选择密文攻击下不可区分性 (Indistinguishability under Chosen Ciphertext Attack，IND-CCA) 的密钥封装机制，Kyber.CPAPKE到Kyber.CCAKEM的构造通过Fujisaki-Okamoto变换实现。在Kyber.CPAPKE和Kyber.CCAKEM中，Kyber.CPAPKE.Dec收到密文后对其进行解密，具体过程如算法1所示。为简化符号，用$\mathcal{B}$表示整数字节的集合$\{0, 1, ..., 255\}$，用$\mathcal{B}^k$表示长度为k的字节数组。对于字节数组a，$a + k$表示从第k字节开始的字节数组。此外，$\mathbb{Z}_q$表示模为q的整数环，$\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n + 1)$表示多项式环，$n$为多项式的最高次项。$\mathcal{R}_q$的元素记为正体小写字母，多项式向量用粗体小写字母标注，表示成维度为k的列向量。在Kyber768参数集中，k、n、q、d_u和d_v分别设置为3、256、3329、10和4。

Algorithm 2 Decode$_\ell$: $\mathcal{B}^{32\ell} \to R_q$

Input: Byte array $B \in \mathcal{B}^{32\ell}$

Output: Polynomial $f \in R_q$

1: $(\beta_0, ..., \beta_{256\ell-1}) := \text{BytestoBits}(B)$

2: **for** i from 0 to 255 **do**

3: $\quad f_i := \sum_{j=0}^{\ell-1} \beta_{i\ell+j} 2^j$

4: **end for**

5: **return** $f_0 + f_1X + f_2X^2 + \cdots + f_{255}X^{255}$

具体来说，Kyber.CPAPKE.Dec的输入参数包括密文c和私钥sk。Kyber首先将字节数组反序列化为多项式向量，如算法2所示，Decode函数将32ℓ的字节数组B转化成$f_0+f_1X+f_2X^2+\cdots+f_{255}X^{255}$，系数$f_i$都在$\{0, 1, ..., 2^\ell-1\}$的范围内。其中，

BytestoBits函数用于转换数组格式，ℓ的字节数组会转化为8ℓ的位数组。此时，私钥sk被反序列化为多项式向量$\hat{\mathbf{s}}$，密文c还需解压为多项式向量$\mathbf{u}$和多项式v。为减小密文的数据尺寸，Compress函数和Decompress函数会丢弃对解密正确率影响较小的低位数据。如公式(2-5)所示，Compress函数将元素x压缩为$\{0,1,...,2^d-1\}$中的整数，其中$d < \lceil log_2(q) \rfloor$。Decompress函数对结果$\text{Compress}_q(x,d)$进行解压，得到满足公式(2-6)的元素$x'$。需要注意的是，元素$x'$为元素$x$的近似值，两者的关系如公式(2-7)所示。这样，密文c被转化为多项式向量$\mathbf{u}$和多项式v。

$$\text{Compress}_q(x,d) = \lceil 2^d/q \cdot x \rfloor \bmod^+ 2^d \tag{2-5}$$

$$x' = \text{Decompress}_q(x,d) = \lceil q/2^d \cdot x \rfloor \tag{2-6}$$

$$|x' - x \bmod^{\pm} q| \le B_q := \lceil \frac{q}{2^{d+1}} \rfloor \tag{2-7}$$

在Kyber.CPAPKE.Dec中，数论变换 (Number Theoretic Transform，NTT) 是定义在环$\mathbb{Z}_q$的线性正交变换，将多项式从系数表示变化为点集表示，可以快速实现$\mathbf{s}$和$\mathbf{u}$的多项式乘法。由于Kyber的素数模q具有256次原根，多项式环$\mathcal{R}_q$上$X^{256}+1$分解为128个平方多项式的乘积，如公式(2-8)所示。其中，$\{\zeta,\zeta^3,\zeta^5,...,\zeta^{255}\}$是所有256次原根的集合，$\text{br}_7(i)$表示7位整数$i$的位翻转值，其中$i = 0,1,...,127$。公式(2-9)描述了任意多项式$f$的NTT变换，该向量包含128个一次多项式元素，各项系数由公式(2-10)和公式(2-11)计算。

$$X^{256}+1 = \prod_{i=0}^{127}(X^2-\zeta^{2i+1}) = \prod_{i=0}^{127}(X^2-\zeta^{2\text{br}_7(i)+1}) \tag{2-8}$$

$$NTT(f) = \hat{f} = (\hat{f}_0 + \hat{f}_1 X, \hat{f}_2 + \hat{f}_3 X, ..., \hat{f}_{254} + \hat{f}_{255} X) \tag{2-9}$$

$$\hat{f}_{2i} = \sum_{j=0}^{127} f_{2j}\zeta^{(2\text{br}_7(i)+1)j} \tag{2-10}$$

$$\hat{f}_{2i+1} = \sum_{j=0}^{127} f_{2j+1}\zeta^{(2\text{br}_7(i)+1)j} \tag{2-11}$$

因此在Kyber的NTT变换中，将256次多项式拆分为2个128次多项式，并以两个多项式独立进行运算。然后对NTT域上的$\hat{\mathbf{s}}$和$\hat{\mathbf{u}}$向量，通过公式(2-12)进行逐点乘法 (Point-Wise Multiplication，PWM) 运算。此后，逆NTT函数将乘法结果转换回时域，通过Compress函数和Encode函数恢复二进制消息m。在这里，Encode函数是Decode函数的逆过程，作用于每个多项式并输出字节数组。

$$\hat{h}_{2i} + \hat{h}_{2i+1}X = (\hat{f}_{2i} + \hat{f}_{2i+1}X)(\hat{g}_{2i} + \hat{g}_{2i+1}X) \bmod X^2 - \zeta^{2\text{br}_7(i)+1} \tag{2-12}$$

针对Kyber的侧信道攻击主要分为两类，旨在恢复密钥配送的长期私钥和会话密钥，前者与Kyber.CPAPKE.Dec过程相关，涉及逆NTT运算、PWM运算和

模约减运算[93–95]，后者与加密过程的NTT运算、Encode函数和Decode函数有关[96]。然而，当前大部分工作集中在Kyber的软件实现，Kyber硬件实现的安全测评还有待完善。

2.2 电磁信息泄露模型

集成电路的电磁辐射与处理数据密切相关，处理不同的数据将产生不同的电磁信息泄露。与功耗分析攻击类似，电磁分析攻击通常采用汉明距离模型和汉明重量模型，以此建立密码中间值对应的信息泄露模型。

2.2.1 汉明距离模型

汉明距离模型最早用于模拟逻辑单元的能量消耗，该模型假定所有单元对能量消耗的贡献相同，逻辑单元的输出状态发生翻转时产生能量消耗，例如$0 \rightarrow 1$翻转和$1 \rightarrow 0$翻转，输出状态保持不变时无能量消耗。因此，可用汉明距离描述逻辑单元的状态翻转与电磁辐射的关系，统计特定时间段内状态翻转的总数目，如公式(2-13)所示。其中，v_0为逻辑单元的先前状态，v_1表示后来状态，$\mathrm{HD}(v_0, v_1)$表示v_0和v_1的汉明距离，即先后状态相异比特的个数，L表示状态翻转过程的电磁辐射能量。α表示电磁辐射的比例系数，$\mathcal{N}$为无关数据的翻转噪声和外部环境噪声。

$$L = \alpha \times \mathrm{HD}(v_0, v_1) + \mathcal{N} \tag{2-13}$$

在实际应用中，尽管攻击者很难获得完整的电路网表，但根据部分元件在特定时间段处理的连续数据，能够建立这些元件的信息泄露模型。对于密码算法的硬件实现，时序逻辑由时钟信号驱动，组合逻辑由输入电平控制，它们引起的电磁辐射均可由汉明距离模型刻画。以时序逻辑为例，在时钟边沿到来时发生数据采样，其状态翻转以时钟周期为时间单位。因此，通过计算连续周期内输出状态的汉明距离，攻击者可以仿真与处理数据相关的电磁辐射能量。

2.2.2 汉明重量模型

汉明重量模型相比汉明距离模型更为简单，适用于无法获得连续处理数据的攻击场景。该模型认为逻辑单元的能量消耗与当前状态直接相关，如公式(2-14)所示。其中，v_0为逻辑单元所处的状态，$\mathrm{HW}(v_0)$代表v_0的汉明重量，即该状态字符中1的个数，L对应此刻的电磁辐射能量，α和$\mathcal{N}$的含义与汉明距离模型中的一致。

$$L = \alpha \times \mathrm{HW}(v_0) + \mathcal{N} \tag{2-14}$$

在汉明重量模型中，电磁辐射能量与被置位的数据比特数目成正比，忽略了该数据的先前状态和后来状态，因此在准确度方面有所欠缺。考虑到$0 \rightarrow 1$翻转和$1 \rightarrow 0$翻转的能量消耗具有微小差异，汉明重量模型在一定程度反映了真实的电磁辐射，而且该模型不需要充分了解硬件实现细节，在实践中也得到了比较广泛的应用。

2.3 电磁分析攻击技术

电磁分析攻击是基于攻击的评估方法，通过侧信道攻击以恢复敏感信息，根据攻击结果成功与否，以及实施攻击的难易程度，判定密码芯片满足的安全水平。典型分析技术包括简单电磁分析、差分电磁分析和相关电磁分析等。本节主要介绍这些技术的工作原理和实施流程。

2.3.1 简单电磁分析

SEMA只需要少量电磁曲线即可恢复敏感信息，它假设攻击者了解密码算法的实现细节，且密码运算和电磁曲线之间有直接关系，能够通过观察曲线轮廓判断出敏感信息。SEMA适用于以下两种攻击场景，一种是公钥密码算法的密钥分析，如RSA算法和ECC算法，表现为以密钥取值为判断条件的分支指令。对于不能直接恢复密钥的场景，SEMA能够从电磁曲线上定位密码区间，辅助开展其他形式的攻击手段。

Algorithm 3 RSA的模幂算法

Input:

底数x，n位的指数y，模数N

Output:

模幂结果$z = x^y \bmod N$

$z = 1$

for $i = n;\ i \geq 1;\ i--$ **do**

    $z = z^2 \bmod N$

    if $y(i) == 1$ **then**

        $z = zx \bmod N$

    end if

end for

以RSA算法的模幂运算为例，对SEMA的原理进行简要分析。在RSA解密操作中，模幂运算的底数为密文，指数为私钥，攻击者恢复私钥即可破解RSA算

法。如算法3所示，根据指数y的位宽长度，模幂运算共循环n次，每次循环伊始执行模平方操作$z = z^2 \bmod N$，随后对指数y的第i位进行判定，若为1则执行模乘操作$z = zx \bmod N$，若为0则直接结束本次循环。因此，对于指数y的每一位数据，零值对应模平方操作，而非零值对应模平方和模乘两种操作。由于模平方操作和模乘操作的泄露差异，攻击者只需从电磁曲线区分上述操作，即可恢复指数y代表的私钥。

2.3.2 差分电磁分析

DEMA关注所有曲线在同一时刻的统计特性，无需了解密码算法的具体实现细节，是非常实用的电磁分析攻击手段。DEMA采用分而治之的攻击策略，将待攻击的密钥分成若干个密钥片段，逐一进行攻击和恢复。与SEMA相比，DEMA具有更强的统计分析能力，所以对密码芯片的威胁程度更高。在采集密码运算的电磁曲线之后，攻击者需根据密码中间值构造区分函数，结合猜测密钥和已知明文或密文计算区分函数值，依据该函数值将电磁曲线分为两个集合，从平均作差后的差分曲线中获取密钥。如图2-4所示，主要包括以下步骤：

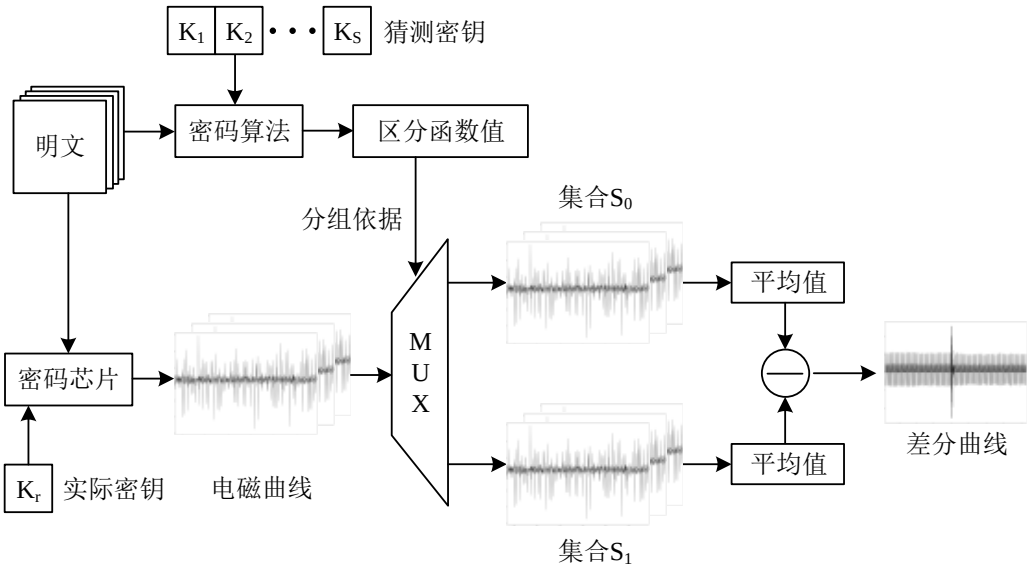


图 2-4 差分电磁分析的攻击流程

第一步，攻击者将随机明文C_i作为密码芯片的输入，测量运行过程产生的电磁曲线LC_i，其中$i = 1, 2, ..., N$表示当前明文的序数，N为输入明文的总数。

第二步，选择合适的密码中间值作为攻击点，例如AES算法的字节替换和Kyber算法的逐点乘法，在该处构建的区分函数具有分类器功能，将电磁曲线LC_i分为集合S_0和集合S_1，如公式(2-15)和公式(2-16)所示。其中C_i为第i个随机明文，K_s为猜测密钥，$D(C_i, K_s)$表示密码中间值的全部比特，HW代

表$D(C_i, K_s)$的汉明重量值。

$$S_0 = \left\{ LC_i | \mathrm{HW}(D(C_i, K_s)) \le \left\lceil \frac{n}{2} \right\rceil,\ 1 \le i \le N \right\} \tag{2-15}$$

$$S_1 = \left\{ LC_i | \mathrm{HW}(D(C_i, K_s)) \ge \left\lceil \frac{n}{2} \right\rceil,\ 1 \le i \le N \right\} \tag{2-16}$$

第三步，将集合S_0和集合S_1分别取算术平均值，作差得到猜测密钥的差分曲线$\Phi(K_s)$，如公式(2-17)所示，$|S_0|$和$|S_1|$代表集合S_0和集合S_1的元素个数。

$$\Phi(K_s) = \frac{1}{|S_0|} \sum_{LC_i \in S_0} LC_i - \frac{1}{|S_1|} \sum_{LC_i \in S_1} LC_i \tag{2-17}$$

第四步，逐个观察猜测密钥的差分曲线，若在密码中间值处产生明显的尖峰，代表区分函数值与真实处理数据一致，可以准确刻画电磁曲线的分布特征，此猜测密钥即为正确密钥。如果密码中间值附近没有出现明显尖峰，则表示该猜测密钥为错误密钥。

2.3.3 相关电磁分析

CEMA是更为通用的攻击方法，需要采集密码运算的实际电磁辐射，与此同时，构建密码中间值的假设电磁辐射，利用两种曲线的相关性筛选真实密钥。如图2-5所示，前几个步骤与DEMA类似，两者差异在于区分函数的构造方式，CEMA以皮尔逊相关性作为判别依据，下面具体介绍CEMA的实施流程。

第一步，选择合适的密码中间值作为攻击点，密码中间值是密钥和已知变量的函数。在大部分攻击场景中，已知变量为明文或者密文，本节按照明文描述整个流程。

第二步，将N个随机明文C_i输入到密码芯片，测量密码运算产生的电磁曲线。将第i个明文的电磁曲线记为$l_i = l_{i,1}, l_{i,2}, ..., l_{i,T}$，$T$表示采样点的数目，所有明文的测量结果构成$N \times T$阶矩阵$L$，即实际电磁辐射。

第三步，将所有猜测密钥表示为$k = k_1, k_2, ..., k_K$，K为猜测密钥的取值数量。针对已知的明文C_i和猜测密钥k_j，计算假设的密码中间值$v_{i,j} = f(C_i, k_j)$，对于所有的输入明文和猜测密钥，形成了$N \times K$阶的假设中间值矩阵。选择正确的信息泄露模型，如上节介绍的汉明距离模型，将该矩阵映射为假设电磁辐射V。

第四步，比较假设电磁辐射和实际电磁辐射的相关性，计算矩阵H每一列h_i与矩阵L各列l_j的皮尔逊相关性$r_{i,j}$，如公式(2-18)所示，形成$K \times T$阶的相关系数矩阵R，元素$r_{i,j}$的绝对值越大，表示h_i和l_j关联程度越大，反之亦然。其中，$i = 1, 2, ..., K$，$j = 1, 2, ..., T$，$\bar{h}_i$和$\bar{l}_j$分别为h_i和l_j的平均值。

$$r_{i,j} = \frac{\sum_1^N (h_i - \bar{h}_i)(l_j - \bar{l}_j)}{\sqrt{\sum_1^N (h_i - \bar{h}_i)^2} \sqrt{\sum_1^N (l_j - \bar{l}_j)^2}} \tag{2-18}$$

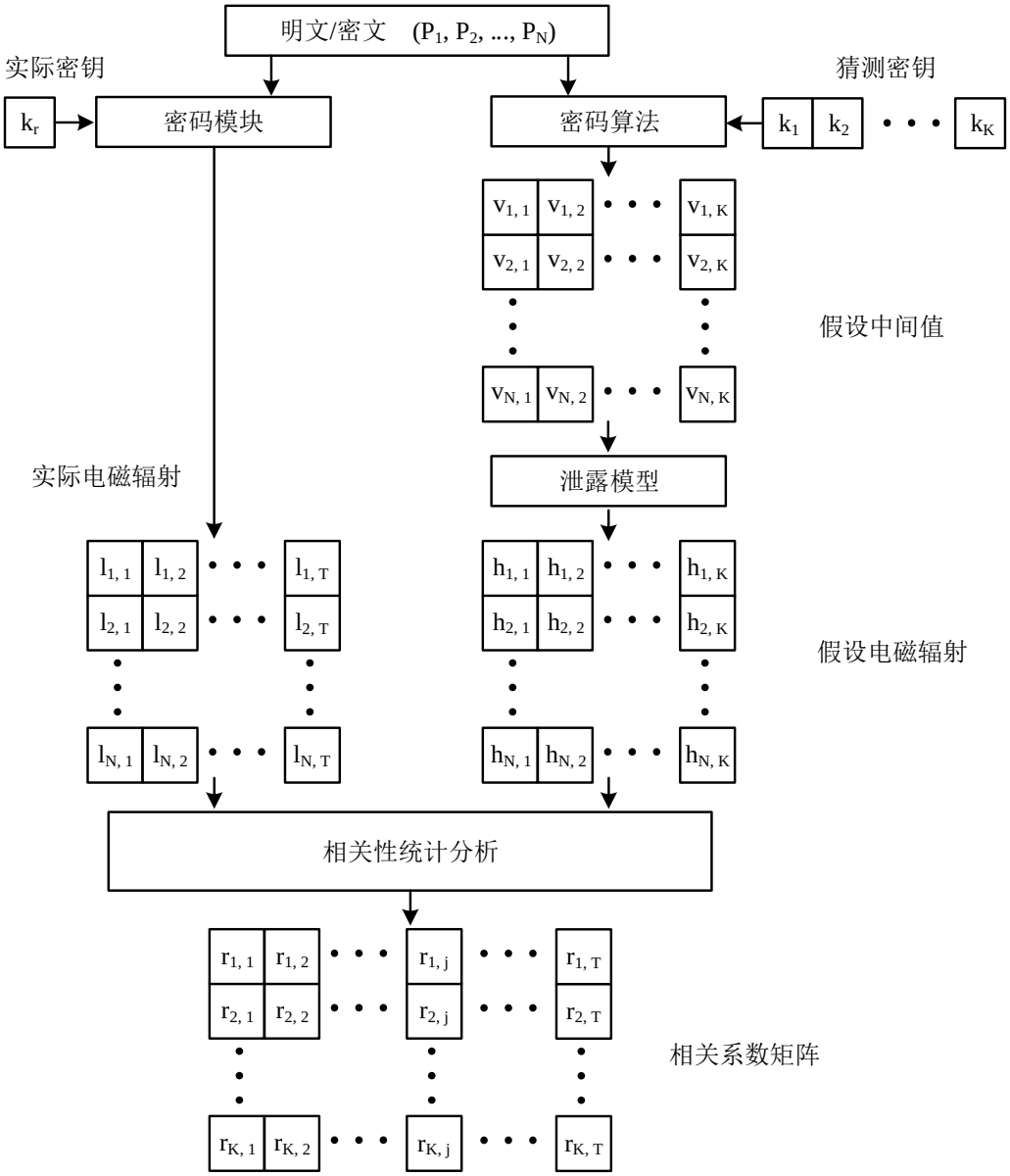


图 2-5 相关电磁分析的攻击流程

第五步，当猜测密钥为正确密钥时，在选定的密码中间值处，假设电磁辐射和实际电磁辐射有较大的相关性，而与其他中间值的实际电磁辐射相关性较小，所以相关性曲线会出现明显的尖峰。当密钥猜测错误时，由于相关性都比较小，相关性曲线不会出现明显的尖峰。假定猜测密钥k_s为正确密钥，将k_s的相关性峰值表示为ρ_c，其他猜测密钥的相关性峰值表示为ρ_w。两者的比值Ψ由公式(2-19)计算，Ψ越接近0泄露越不明显。随着曲线数目的增加，Ψ逐渐增加直到超过1，则表明k_s从猜测密钥中显现出来，攻击者能够恢复出正确的密钥。此时，破解密钥所需的最小曲线数量 (Measurement To Disclosure，MTD) 反映了攻击难

度，是评估信息泄露风险的重要指标。

$$\Psi = \frac{\rho_c}{\rho_w} = \frac{max\{r_{i,1}, r_{i,2}, ..., r_{i,T}\}|_{i=s}}{max\{r_{i,1}, r_{i,2}, ..., r_{i,T}\}|_{i\neq s}} \tag{2-19}$$

2.4 抗电磁分析攻击技术

电磁分析攻击之所以能够获取算法密钥，主要依赖于密码中间值和电磁信息的相关性。因此，对电磁分析攻击的防护手段，其目标在于降低或消除两者之间的相关性，如1.2.2节所述，主要分为隐藏技术和掩码技术。

2.4.1 隐藏技术

隐藏技术能够减弱电磁信息和密码中间值的相关性，这可以从时间和振幅两个维度实现，迫使攻击者采集更多的侧信道数据，提高了成功恢复密钥的难度。时间维度的隐藏技术会干扰密码电路的运行过程，使信息泄露时刻具有随机特性，典型技术包括随机延迟插入、时钟随机化和乱序操作等。Lu等人进行了随机延迟插入的硬件实现，在所有密码操作前添加了延迟逻辑 [97]。在延迟逻辑中，由一定数量的缓冲单元构成延时链，通过随机数确定延时链的输出位置，从而产生随机长度的延迟信号。然而，延迟逻辑使电路性能降低了39%，整体功耗增加了3.11倍。Bayrak等人提出了时钟随机化的硬件方案，采用随机产生的抖动时钟驱动时序逻辑，从而增加了信号时序的不确定性 [98]。根据参考时钟产生多个相移时钟，相邻时钟之间具有相同的时间延迟，使用多路复用器随机选择时钟，传递到时序逻辑的时钟输入端。然而，相移时钟会降低电路的运行速度，使时钟周期增加到参考时钟的1.64倍。

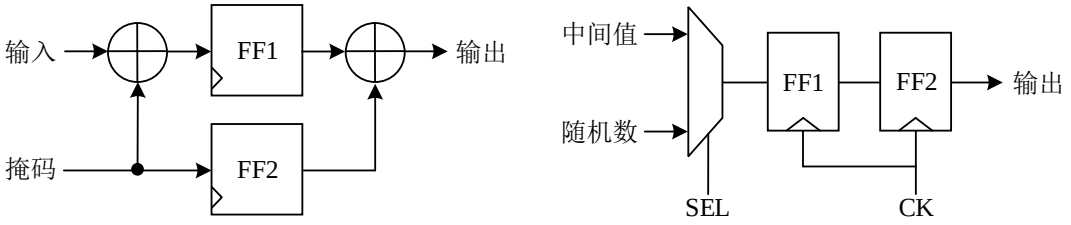
振幅维度的隐藏技术通过降低信噪比来隐藏敏感信息，典型的技术有噪声引擎、信号衰减和双轨预充电逻辑等。噪声引擎包括随机数生成器与噪声单元，在执行密码运算时并行产生随机噪声。噪声单元具有多种硬件实现方式，如有限状态机、负载电容和电流源，能够产生不同程度的电源噪声，但会引入较大的功耗开销。信号衰减通常由定制或半定制电路实现，旨在降低密码电路产生的能量消耗。一般而言，这种防护方式具有较高的安全性，但会带来较大的面积和功耗开销。例如，Das等人将密码电路封装到电流衰减模块，使用低压差线性稳压器减弱了供电端的能量波动，同时牺牲了23%和49%的面积和功耗 [58]。双轨预充电逻辑源于功耗平坦化的思想，使逻辑单元的能量消耗独立于处理数据，在每个时钟周期都产生相同的瞬态功耗。常见的硬件实现有敏感放大器逻辑 (Sense Amplifier Based Logic，SABL) 和行波动态差分逻辑 (Wave Dynamic Differential Logic，WDDL) [99, 100]。为使计算时间独立于处理数据，当所有的输入信

号置为互补值后，SABL单元才会进入求值阶段。由于这些特殊的设计要求，密码电路的SABL单元需要全部定制。其后，Tiri等人提出了较易实现的WDDL单元，它基于标准逻辑单元库构造，不需要特殊设计单元结构，很大程度上兼容了当前设计流程。但由于早期传播效应的影响，以及与门和或门的非对称性，WDDL单元不具备较好的能量均衡特性。除此之外，上述逻辑单元的面积消耗在常规单元的两倍以上，最高运行频率会降低到原来的一半，密码电路的整体功耗也将急剧增加。

2.4.2 掩码技术

掩码技术是常用的抗电磁分析攻击手段，通过掩码消除密码中间值和电磁信息的相关性。在掩码防护方案中，一般对明文或密钥进行掩码操作，其后的密码中间值都处于掩码状态，完成所有运算后再将掩码从中移除，获得正确的输出结果，这样保证了密码中间值不会被直接处理，从而产生与之独立的电磁信息。现有的掩码技术同样会降低运行效率，显著增加密码电路的面积和功耗。下面具体分析两种简单的掩码方案，包括布尔掩码和随机预充电。

布尔掩码是最早提出的掩码方案，实现效率较高，在业界已得到普遍应用。图2-6 (a)为逻辑掩码的实现方案，FF1为原始时序逻辑，FF2用于存储掩码值，密码中间值v与掩码m进行异或操作获得掩码型中间值v_m，即$v_m = v \oplus m$。该方案可推广到很多密码逻辑和函数，它们具有$f(x * y) = f(x) * f(y)$的特性，均为异或操作的线性运算。给定掩码型中间值v_m和掩码m，可以唯一确定中间值v的值。因此，布尔掩码是(v_m, m)构成的秘密共享方案，由于m是均匀分布的随机信号，攻击者很难同时获得v_m和m的具体值，也就无法恢复关于v的实际信息。



(a) 布尔掩码　　(b) 随机预充电

图 2-6　掩码实现方案

随机预充电是一种简单的隐式掩码方案，如图2-6 (b)所示，该方案并非直接对中间值进行掩码操作，而是向时序逻辑和组合逻辑传送随机数，目的是随机化密码中间值的侧信道行为。在典型实现方案中，数据选择器使用控制信号SEL选择输出数据，即密码中间值或随机数，FF1为原始时序逻辑，FF2为复制时序逻辑，两者均被时钟信号CK所驱动，其输出连接电路的组合逻辑。假定

在当前时钟周期内，FF1和FF2分别存储中间值和随机数，组合逻辑的输出结果会被随机数覆盖。在下一个时钟周期开始时，数据选择器将随机数保存到FF1，FF1存储的中间值被转移到FF2，此时组合逻辑将继续执行密码运算，并输出正确的密码结果。所以，在密码电路工作过程中，两种时序逻辑的功能不断转变，所有组合逻辑和时序逻辑均在一个时钟周期内处理随机数，在下一个时钟周期处理密码中间值。由于攻击者无法预测中间值和随机数间的状态翻转，起到了扰乱密码电路侧信道行为的作用。

2.5 本章小结

本章介绍了两种密码算法的原理实现，其中AES是对称加密算法，Kyber属于后量子密码算法，用于公钥加密和密钥封装。其后，以汉明距离和汉明重量为例，分析了电磁信息泄露模型的构造方法。在此基础上，说明了电磁分析攻击技术的具体流程，包括简单电磁分析、差分电磁分析和相关电磁分析。最后，讨论了抗电磁分析攻击的方法措施，重点分析了当前防护方法存在的问题，为深入研究安全测评和增强技术奠定了基础。

第 3 章　集成电路版图级电磁仿真方法研究

芯片电磁仿真是开展硅前安全测评的关键步骤，核心问题是如何在可接受的成本下准确模拟电磁信息。为此，本章基于最接近实际芯片的版图数据，开展了集成电路版图级电磁仿真方法研究。首先构建了物理版图的芯片电气模型，分析了电流聚合效应和金属屏蔽效应，探究了电磁信息的根本源头和主导因素。基于上述理论依据，提出了版图级电磁仿真方法，称之为EMSim，采用多种模型简化和仿真加速技术，优化了电流分析和电磁计算环节，实现了电磁信息高效而准确的预测。最终以S-Box和AES芯片为实验对象，比较了仿真结果和实测数据的匹配程度，从仿真精度、测评准确度和计算成本方面，验证了版图级电磁仿真的有效性，能够很好地应用到硅前阶段的安全测评。

3.1　芯片电气模型

3.1.1　电磁产生机理

电磁仿真方法旨在从设计阶段预测集成电路的电磁行为。为实现此目的，最直接的方法是使用商业的三维电磁仿真软件，如Ansys HFSS。对于电子设备的三维模型，Ansys HFSS进行自适应地网格剖分，通过麦克斯韦方程组求解电磁场。考虑到芯片内部数以万计的晶体管和互连线，Ansys HFSS等商业软件还无法应用于集成电路的瞬态电磁仿真。当前主流的方法是借助集成电路的设计与验证工具，基于行为模型或电气模型实现芯片层次的电磁信息仿真。基于行为模型的仿真方法直接使用RTL代码或门级网表，并没有考虑集成电路的物理信息，因此仿真精度较低难以匹配真实的电磁信息。物理版图通常用在基于电气模型的仿真方法，其作为芯片设计阶段的最终输出数据，不仅包含逻辑单元和互连线，还覆盖了所有的物理信息，如电路制造工艺、单元布局位置、金属布线尺寸和各类寄生参数等。所以，以物理版图为基础构建芯片电气模型，获得的仿真结果最接近芯片实际的测量数据。

如图3-1所示，基于互补金属氧化物半导体 (Complementary Metal Oxide Semiconductor，CMOS) 的集成电路可表征为逻辑单元集合和金属互连网络这两个互相依赖的电气系统。逻辑单元集合由生长在硅衬底的晶体管构成，包括标准单元、模块单元和输入输出单元，提供组合逻辑和时序逻辑功能。金属互

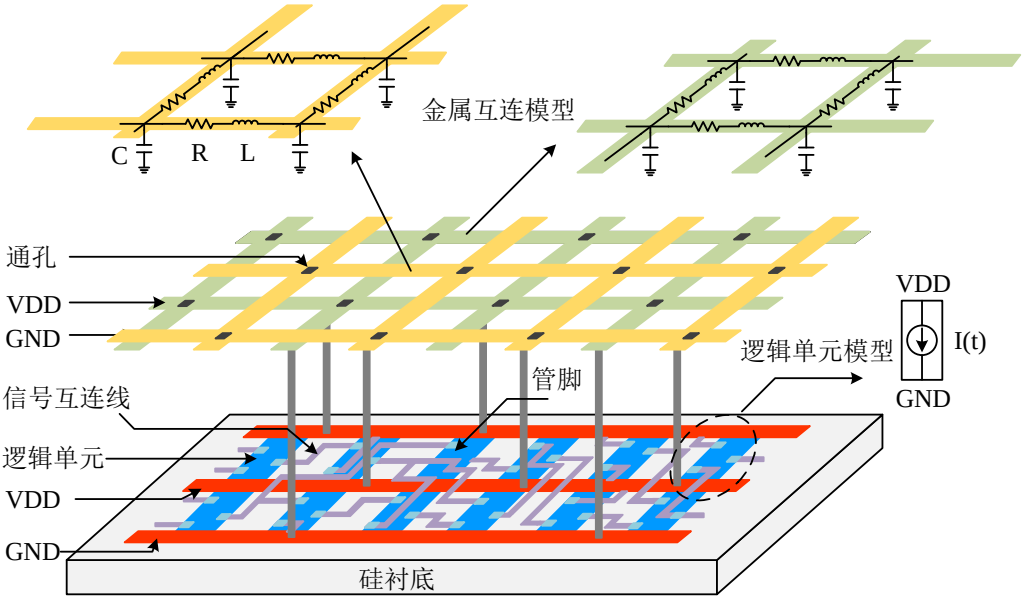


图 3-1　集成电路的物理结构

连网络由信号互连线和片上电源网络构成，分别负责逻辑信号传输和核内电源供应。具体而言，信号互连线桥接不同逻辑单元的输入和输出管脚，驱动级联单元的逻辑运算和状态转换。片上电源网络连接所有逻辑单元的电源和接地管脚，传递来自片外电源网络 (PCB电路板、封装和供电I/O单元) 的供应电压。在片上电源网络中，由电源环线和电源条线构成纵横交错的电源网格，以此为桥梁将供电I/O单元和电源轨相连，电源轨连接逻辑单元的电源和接地管脚，实现了电源网格-电源轨-逻辑单元的片内供电。由于电路阻抗的存在，任何来自逻辑单元集合的激励，都会在金属互连网络产生流动的瞬态电流。携带电流的金属线将成为小型环状天线或短单极天线，向外界环境辐射电磁波。

3.1.2　电流聚合效应

人们普遍认为，高幅度电流存在于片上电源网络的顶部金属层内，从而形成了电磁辐射的主要来源。这一说法得到了部分实验佐证，被大多数版图级电磁仿真方法采用 [46, 58]。然而，目前还没有充足的理论证明支持该论断的正确性。在这种情况下，本节通过构建芯片电气模型探究了电磁辐射的根本来源。如图3-2所示，VDD和GND表示核内电源网格的电源和接地端口，通过金属线与芯片供电I/O单元连接。VDD/Hj和GND/Hj, $j = 1, 2, ..., m$表示分布在电源网格顶层金属层的电源和接地节点，而VDD/Li和GND/Li, $i = 1, 2, ..., n$表示位于底层电源轨线的电源和接地节点。以正向电压供应为例，来自外部供电I/O单元的电压，从VDD端口开始，经过VDD/Hj和VDD/Li节点，最终传递给逻辑单元。为了方便分析，本节将复杂的逻辑电路表示为反相器的单元集合。每个反相器由互补对

偶的PMOS晶体管和NMOS晶体管构成，等效电阻分别为R_{pi}和R_{ni}。它的输出负载包括信号互连线和扇出电路，等效为电阻R_i和电容C_i的组合。当输入管脚发生1 → 0的状态翻转时，开关$\bar{G}_i$闭合，而开关 G_i断开，形成了VDD/Li节点对负载电容C_i的充电回路。当输入管脚发生0 → 1的状态翻转时，开关$\bar{G}_i$断开，而开关 G_i闭合，构成了负载电容C_i对GND/Li节点的放电回路。与反相器类似，其他逻辑单元在状态翻转时也具有上述充放电现象。

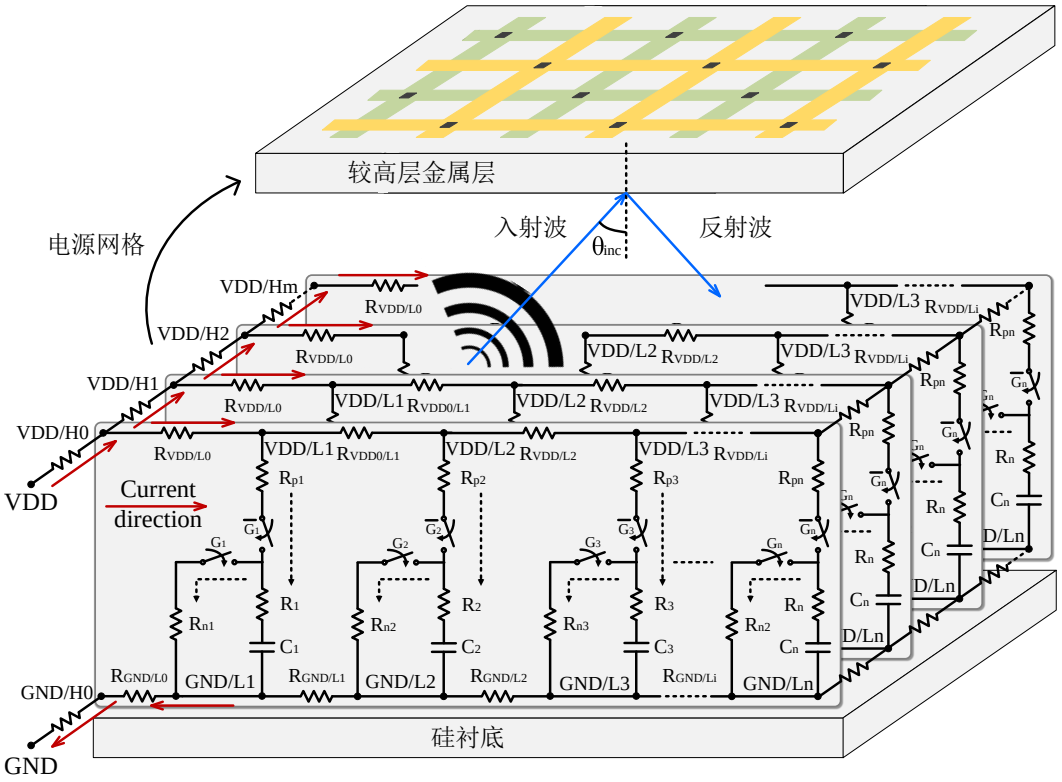


图 3-2　集成电路的电气模型

对于充电回路，由基尔霍夫电路定律求解任意电源节点的瞬态电流，如公式(3-1)所示。而对于放电回路，通过公式(3-2)可推导出任意接地节点的瞬态电流。其中，I_{short}代表电源节点和接地节点同时导通产生的短路电流，I_{leak}代表逻辑单元的静态电流，包括亚阈值电流、PN结反偏电流、栅极漏电流和沟道隧穿电流等。

$$\begin{aligned} I_{VDD} &= \sum_{j=1}^{m} I_{VDD/Hj} = \sum_{j=1}^{m}\sum_{i=1}^{n} I_{VDD/Li} \\ &= \sum_{j=1}^{m}\sum_{i=1}^{n}\left[\frac{V_{VDD/Li} - V_{GND/Li}}{R_{pi} + R_i + 1/jwC_i} + I_{short} + I_{leak}\right] \end{aligned} \tag{3-1}$$

$$I_{GND}=\sum_{j=1}^{m}I_{GND/Hj}=\sum_{j=1}^{m}\sum_{i=1}^{n}I_{GND/Li}$$
$$=\sum_{j=1}^{m}\sum_{i=1}^{n}[\frac{V_{VDD/Li}-V_{GND/Li}}{R_{ni}+R_i+1/jwC_i}+I_{short}+I_{leak}] \tag{3-2}$$

顶层金属通常具有较大的物理尺寸和较小的寄生电阻，可以在满足电压降预算的条件下通过尽可能大的电流。在电源规划阶段，设计者会选择顶层金属层设计电源网格，以满足整个芯片的供电需求。电源轨线需要与逻辑单元硬连接，一般选择较低金属层进行电源布线。结合公式(3-1)和公式(3-2)，逻辑单元的瞬态电流会经过电源轨线的VDD/Li和GND/Li节点，逐级汇聚到顶层电源网格的VDD/Hj和GND/Hj节点，即发生电流聚合效应。因此，在电源网格的顶层金属层内，金属线携带着较大幅度的瞬态电流。

3.1.3 金属屏蔽效应

在芯片设计过程中，为满足金属密度的要求，空白区域会填充无实际连线功能的金属块。这些填充金属和顶层电源网格将组成电磁屏蔽，衰减来自低层金属层的电磁辐射。如图3-3所示，来自低层金属的电磁波入射到高层金属表面时，由于层间介质和金属层的阻抗不匹配，入射波将在金属下边界发生反射。透射入金属的电磁波继续传播时，由于传导电流的存在，电磁能量会转化成焦耳热。当衰减后的电磁波传播到金属上边界时，同样会发生界面反射，并在金属内部发生多重反射。经过金属材料的反射、吸收和多重反射，上边界透射波的磁场强度将大幅度降低。

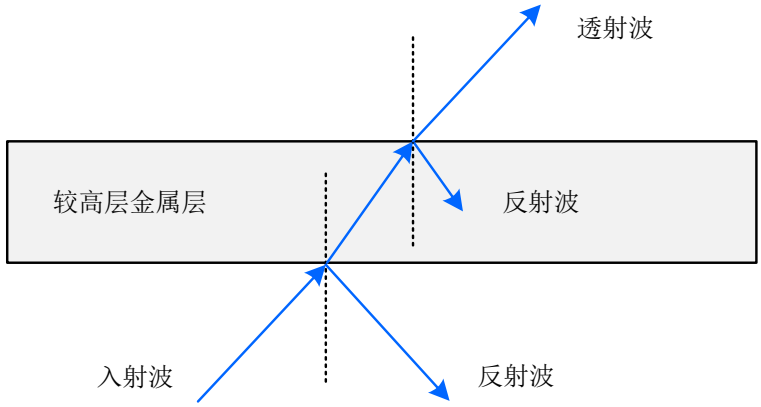


图 3-3 金属屏蔽效能机理

根据谢昆诺夫屏蔽公式，高层金属对底层电磁波的能量衰减由屏蔽效能(Shielding Effectiveness，SE) 表示，如公式(3-3)所示，包括反射损耗*R*、吸收损

耗A和多重反射修正损耗B[101]。H_b和H_a分别表示金属屏蔽前后的磁场强度。

$$\mathrm{SE} = 20lg(\frac{H_b}{H_a}) = R + A + B \tag{3-3}$$

当频率为f的电磁波穿过厚度为t的金属线时，由于金属是良导体，其吸收损耗A表示为公式(3-4)。

$$A = 8.98\alpha t \approx 131.43t\sqrt{f\sigma_r\mu_r} \tag{3-4}$$

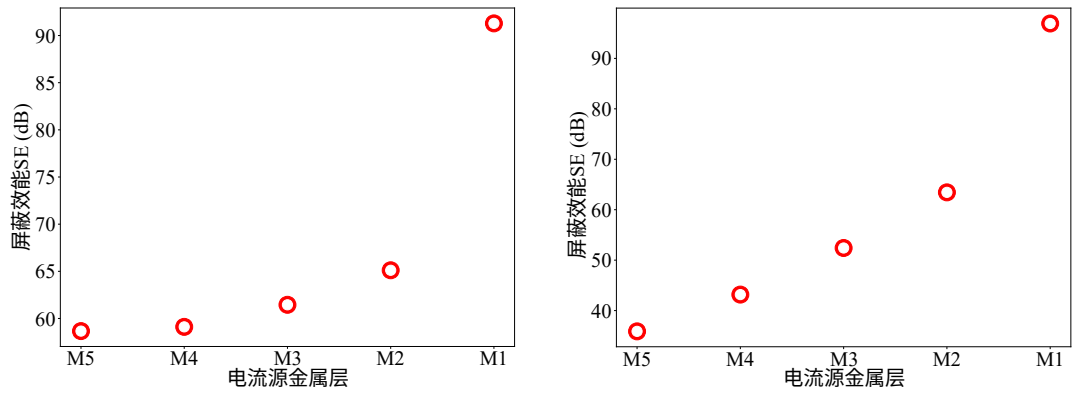
其中金属的衰减常数$\alpha \approx 15.13\sqrt{\pi f\sigma_r\mu_r}$，$\mu_r$表示相对真空的磁导率，真空磁导率$\mu_0$为$4\pi \times 10^{-7}\mathrm{N/A^2}$，$\sigma_r$表示相对铜的电导率，铜的电导率为$5.8 \times 10^7\mathrm{S/m}$。同时，芯片内部电磁波的波阻抗表示为$Z_w$，对于本征阻抗为$Z_w$的金属层，反射损耗$R$可表示为公式(3-5)。

$$R = 20lg\left|\frac{(Z_w + Z_m)^2}{4Z_wZ_m}\right| \tag{3-5}$$

相应地，多重反射修正损耗B可由公式(3-6)求解，γ为传播常数。当吸收损耗较高时，可忽略多重反射修正损耗。

$$B = 20lg|1 - (\frac{Z_m - Z_w}{Z_m + Z_w})^2e^{-2\gamma t}| \tag{3-6}$$

公式(3-3)到公式(3-6)描述了单层金属的屏蔽效能，为了量化芯片多层金属的屏蔽效能，本节根据SMIC 180nm CMOS工艺，构建了金属互连网络的三维模型，其中M1到M5金属层的厚度均为0.53μm，层间距为0.85μm，而M6金属层的厚度为0.99μm，与M5金属层的间距为1μm，借助Ansys HFSS得到了电磁场的屏蔽效能。如图3-4所示，低层电场的衰减幅度在58.66dB和91.29dB之间，低层磁场的衰减幅度在35.88dB到96.92dB的范围。因此，在芯片内部传播过程中，由于较高层金属构成的电磁屏蔽，较低金属层的电磁辐射损耗了绝大部分能量。



(a) 电场　　(b) 磁场

图 3-4　片上金属层对电磁场的屏蔽效能

通过上述理论分析，本节得出了有关芯片电磁信息的三条论断。首先，逻辑单元集合的翻转活动是信息来源，金属互连网络的金属线是辐射载体，以电

磁波的形式将敏感信息传到外界环境。其次，由于电流聚合效应的存在，顶层金属层的电源网格流动着较大幅度的瞬态电流。同时，受金属屏蔽效应的影响，来自较低金属层的电磁波很难传播到芯片外界。这些论断阐明了电磁信息的根本来源和主导因素，使得本章能够合理地优化版图级电磁仿真。

3.2 版图级电磁仿真方法

在上节理论分析的基础上，本节提出了版图级电磁仿真方法，该方法被称为EMSim，如图3-5所示，主要包括数据准备、电流分析和电磁计算环节。基于版图数据库，通过多级电路分析获得物理版图的电流分布。再根据电磁场理论，将瞬态电流转化为空间任意观测点的磁场数据。

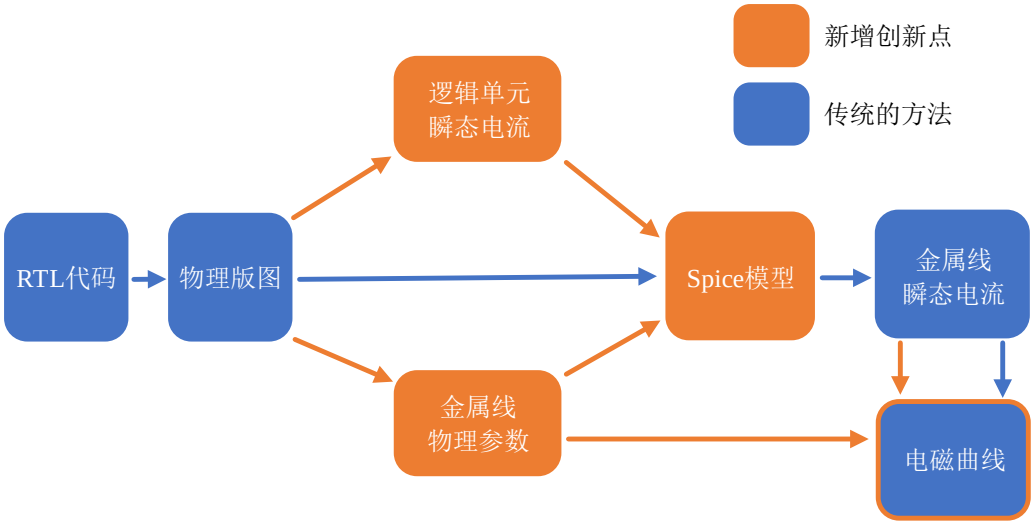


图 3-5 版图级电磁仿真流程

3.2.1 数据准备环节

创建版图数据库是EMSim的首要环节，交由RTL到GDS的芯片设计流程完成。如图3-6所示，芯片的RTL代码是Verilog/VHDL硬件语言描述的行为级模型，逻辑综合根据指定工艺库将其转化为门级网表，结合逻辑单元库和单元时序库，通过物理实现产生GDSII文件形式的物理版图。芯片设计的物理实现通常被称为布局布线，具体包括布图规划、电源规划、布局、时钟树综合和布线等阶段。布图规划是布局布线的最初步骤，规划了芯片尺寸、I/O单元放置以及模块或宏模块的放置。电源规划为芯片供电构造均匀的片上电源网络，实现平均分布电流、减小电压降和避免电迁移的目的。布局完成标准单元和模块的摆放，并根据面积、拥塞和时序约束进行迭代优化。时钟树综合旨在构建时钟网络，将时钟信

号稳定地传递到各个时序逻辑单元，力求达到时钟树约束文件提供的期望参数。布线通过全局布线、详细布线和布线修正，将分布在芯片核内的标准单元、模块和I/O单元进行逻辑互连。在物理实现阶段，寄生参数提取、静态时序分析和物理验证贯穿整个环节，为优化功耗、性能和面积提供目标结果反馈。

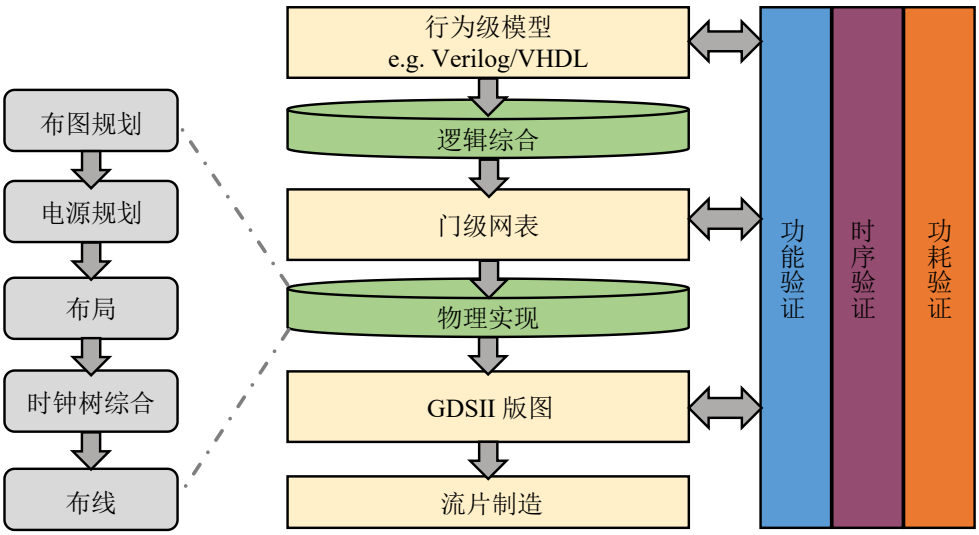


图 3-6　RTL到GDS的芯片设计流程

表 3-1　版图数据库的文件描述

文件名称	数据格式	功能作用
版图后设计网表	Verilog HDL	描述物理实现后的电路功能
标准版图数据	GDSII	描述版图的几何图形、拓扑关系、结构和层次信息
设计交换格式	DEF	描述电路布局布线后单元及互连线的具体物理信息
标准时序约束	SDC	约束电路的时序、功耗和面积等设计要求
标准延时格式	SDF	描述布局布线后单元及互连线的延时数据
标准寄生交换格式	SPEF	描述布局布线后电路的电阻、电容及电感等寄生参数

表3-1描述了版图数据库包含的各类型文件，作为后续电流分析和电磁计算的输入数据。其中，版图后设计网表描述物理实现后的电路功能，设计交换格式文件描述了布局布线后逻辑单元及互连线的具体物理信息，标准版图数据为最终交付流片的文件，附有版图的几何图形、拓扑关系、结构和层次信息。标准时序约束文件约束了电路的时序、功耗和面积等设计要求。标准延时格式文件描述了布局布线后单元和互连线的延时数据，标准寄生交换格式文件包括了布局布线后电路的电阻、电容和电感等寄生参数。

3.2.2 电流分析环节

在EMSim的电流分析环节，根据器件模型近似和寄生网络约减，将逻辑单元的翻转活动等效为瞬态电流源激励，将片上电源网络和信号互连线等效为寄生网络模型，进而将上述模型融合为整个芯片的仿真模型，通过Spice仿真获得物理版图上的瞬态电流分布。

3.2.2.1 单元级电流源

传统的电磁仿真方法采用深亚微米器件模型，通过晶体管级的Spice仿真获取指定时间范围的瞬态电流。以金属氧化物半导体场效应晶体管 (Metal-Oxide-Semiconductor Field-Effect Transistor，MOSFET) 为例，在深亚微米器件模型中，逻辑单元的物理行为用数学方程和模型参数来描述，例如业界通用的BSIM (Berkeley Short-channel IGFET Model) 模型。BSIM模型增加了几百个模型参数，用来匹配实际的器件特性，刻画了短沟道效应、窄沟道效应、亚阈值特性等二级效应，以及特征尺寸缩小产生的诸多效应。例如，当晶体管进入饱和区时，随着漏源电压的不断增加，实际的反型沟道长度逐渐减少，在伏安特性中表现为漏极电流的曲线上翘。尽管提升了器件模型精度，数量庞大的模型参数也降低了仿真效率，随着电路尺寸和方程规模的增加，电路仿真的时间成本和资源消耗急剧增加，已成为限制芯片电磁仿真的关键因素。由于充电回路和放电回路的存在，逻辑单元的翻转活动会产生电源电流，通过电流聚合效应影响顶层电源网格的瞬态电流。因此，在电流分析环节，逻辑单元可等效为单元电源电流，并作为电路方程求解的激励源。如图3-1所示，本节将逻辑单元建模成电流源激励，电流方向从电源管脚指向接地管脚，电流大小由单元级功耗分析预先确定。这种思想被称为器件模型近似，采用单元级电流源取代深亚微米器件模型，将非线性数学方程求解转化为分段线性的电流查找表。同时，采用事件驱动仿真创建电流查找表，有效权衡仿真精度和计算成本的关系。

图3-7为单元级电流源的构建流程，分为动态门级仿真和单元功耗分析两个步骤。在芯片设计过程中，动态门级仿真致力于验证时序和功能的正确性，检查电路网表的完备性。EMSim通过仿真激励文件控制该步骤的执行，旨在获得逻辑单元的翻转活动，为后续单元功耗分析提供数据支撑。仿真所需的其他输入文件有版图后设计网表、SDF文件和标准单元模型文件。以Synopsys VCS工具为例，仿真过程将SDF文件反标到版图后设计网表，在特定测试激励条件下，记录单元翻转活动并输出值变转储 (Value Change Dump，VCD) 文件。VCD文件包含头信息、变量定义和值变化信息，保存了电路中选定信号的状态变化。对于指定时间范围的电磁仿真，EMSim仅记录给定时间段的单元翻转活

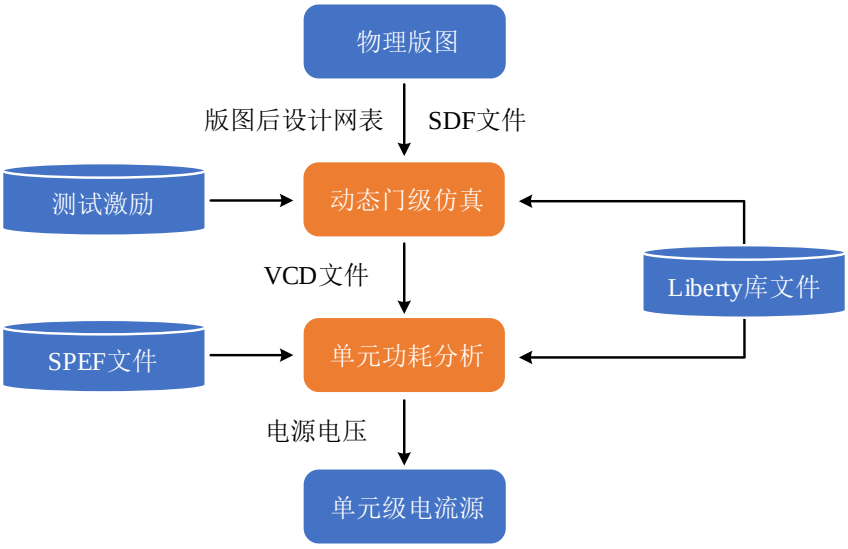


图 3-7 单元级电流源构建流程

动，这是通过$dumpfile、$dumpvars、$dumpall、$dumpon和$dumpoff等命令实现的。$dumpfile定义了输出VCD文件的名称，$dumpvars指定了待记录到VCD文件的所有信号，$dumpall记录了当前时间点选定信号的值，$dumpoff表示中断选定信号值的记录活动，$dumpon重新恢复记录选定信号的值。默认模式下，所有逻辑单元的翻转活动都将被记录，以此获得最为准确的电磁信息。同时，EMSim也允许指定动态门级仿真所包含的逻辑单元，当排除敏感数据无关的逻辑单元时，可以模拟更加精通的攻击场景，为安全测评提供灵活的使用模式。

EMSim通过工具命令语言 (Tool Command Language，TCL) 脚本执行单元功耗分析。以Synopsys PrimeTime PX工具为例，选择瞬态仿真模式获得每个逻辑单元的实时电流值。首先导入设计数据和工艺库信息，包括版图后设计网表、Liberty库文件、SDC文件、SPEF文件和VCD文件。Liberty库文件由工艺厂提供，采用非线性功耗模型 (Non-Linear Power Model，NLPM) 或复合电流源模型 (Composite Current Source Model，CCS) 建立，用于描述逻辑单元的时序和功耗信息[102, 103]。设计者也可以根据实际测量或仿真模拟的数据构建专用Liberty库文件[104]。其后，将VCD文件记录的翻转活动标定到版图后电路网表，同时将SPEF文件的寄生参数注释到各单元及其线网。时序分析会针对每次信号翻转活动，计算并存储逻辑单元的输入翻转时间和输出负载。最终，单元功耗分析利用事件驱动的仿真架构，仅在逻辑单元的输出状态变化时计算其电源电流。以输入翻转时间和输出负载信息为索引，通过访问Liberty库文件的功耗查找表获得当前时刻的功耗值。EMSim允许指定单元功耗分析的起止时间和波形精度，分别由-read_vcd -time命令和-set_power_analysis_options -waveform_interval命令决定。这样，每个逻辑单元的瞬态电流由瞬态功耗除以电源电压来获得，在后续Spice仿

真中充当分段线性电流源。

3.2.2.2 寄生网络模型

金属互连网络的建模在芯片电磁仿真中至关重要。在给定电压源和电流激励的条件下，金属线的阻抗特性是影响电流行为的主要因素。所以，如图3-1所示，由通孔分割的金属线被等效为电阻R、电容C和电感L的阻抗模型。由此，可以将金属互连网络视作寄生网络模型，在物理实现和签发核实过程，借助寄生参数提取获得上述模型中电阻、电容和电感的具体值。由3.1节的理论分析可知，只关注来自顶层电源网格的电磁辐射，是对版图级电磁仿真过程的合理简化。所以，在电流分析环节，关键问题是如何获取顶层电源网格的瞬态电流。

传统仿真方法利用晶体管级Spice仿真获取瞬态电流，该过程采用深亚微米器件模型，其输入状态和输出负载需要由信号互连线来提供。然而，信号互连线会导致庞大的寄生网络，为节点方程求解带来巨大的计算量，且容易产生仿真收敛性问题。为达到精度和速度的平衡，EMSim预先确定逻辑单元的瞬态电流，建立等效的电流源激励，以此替代复杂的晶体管级器件模型，无需在Spice仿真过程求解该模型的输入和输出参数。因此，本节提出了寄生网络约减，从寄生网络模型中排除信号互连线，在保证电路收敛的同时节省矩阵求解的时间。对于单元级电流源的理论分析和技术实现，已在上一节进行了详细描述，本节重点讨论寄生网络约减的实现流程。

```
/* ---Hcell示例---*/

JKFFRX2* JKFFRX2
NAND3XL* NAND3XL
NAND2X2* NAND2X2
NOR2BX1* NOR2BX1
NOR3BX1* NOR3BX1
NOR3BX1* NOR3BX1
XNOR2X1* XNOR2X1
NAND3X2* NAND3X2
DFFHQX1* DFFHQX1
OAI21XL* OAI21XL

/* ---Hcell示例---*/
```

(a) Hcell文件

```
/* ---Xcell示例---*/

JKFFRX2* JKFFRX2 -I
NAND3XL* NAND3XL -I
NAND2X2* NAND2X2 -I
NOR2BX1* NOR2BX1 -I
NOR3BX1* NOR3BX1 -I
NOR3BX1* NOR3BX1 -I
XNOR2X1* XNOR2X1 -I
NAND3X2* NAND3X2 -I
DFFHQX1* DFFHQX1 -I
OAI21XL* OAI21XL -I

/* ---Xcell示例---*/
```

(b) Xcell文件

```
/* ---规则文件示例---*/

LVS BOX JKFFRX2 JKFFRX2
LVS BOX NAND3XL NAND3XL
LVS BOX NAND2X2 NAND2X2
LVS BOX NOR2BX1 NOR2BX1
LVS BOX NOR3BX1 NOR3BX1
LVS BOX NOR2BX4 NOR2BX4
LVS BOX XNOR2X1 XNOR2X1
LVS BOX NAND3X2 NAND3X2
LVS BOX DFFHQX1 DFFHQX1
LVS BOX OAI21XL OAI21XL

/* ---规则文件示例---*/
```

(c) 规则文件

图 3-8 Hcell、Xcell及规则文件的代码示例

具体来说，在通过电气规则检查 (Layout Versus Schematic，LVS) 后，采用寄生参数提取获得物理版图的寄生参数。以寄生参数提取工具Calibre xRC为例，门级提取方式将单个逻辑单元视为理想器件，只提取到单元边界外的寄生参数，仍保留单元的内部层次结构，如较低层级的嵌套单元、晶体管与互连线。为此通过遍历DEF文件内容，EMSim提取了所有类型的逻辑单元。首

先创建Hcell和Xcell文件，Hcell文件指定用于门级提取的单元列表，Xcell文件定义视作理想器件的单元列表，其内部不再经历寄生参数提取。图3-8 (a)列出了Hcell文件的代码示例，第一列为单元的版图名称，第二列为对应的原理图名称。Xcell文件具有相同的单元列表，不同的是，代码第三列的标识符用于指定理想器件，如图3-8 (b)所示。同时，在规则文件中添加LVS BOX命令语句，以黑盒形式处理上述单元，如图3-8 (c)所示。最终，Calibre xRC输出详细标准寄生格式 (Detailed Standard Parasitic Format，DSPF) 的寄生参数文件，记录了寄生网络模型中电阻、电容和电感的物理信息，包括数值，位置、宽度、长度、金属层和厚度等。其后，从DSPF文件中提取片上电源网络模型，作为Spice仿真模型的组成部分。

3.2.2.3 Spice仿真模型

EMSim处理单元级电流源和寄生网络模型，构建用于电流分析的Spice仿真模型，具体流程如算法4所示。单元级电流源*Current*对应的单元名称*CellDef*继承自DEF文件，按照实例化的电路层级表示，如top-module/sub-module/cell-instance。而寄生网络模型中采用子电路语句描述逻辑单元，其名称*CellDspf*的标识符必须以X为前缀。为了将单元级电流源插入到寄生网络模型的内部节点，需要执行步骤3到6统一两种单元集合的排列方式。具体来说，Order函数遍历物理版图的单元坐标(x, y)，从下到上、从左到右对单元集合重新排序。步骤11到21定义了Order函数执行过程，*argsort*函数返回对数组升序排序的索引元组，*unique*函数返回数组中非重复元素组成的元组，*count_nonzero*函数用来统计数组中非零元素的数目。而对于数组切片操作，在进入循环前将*end*参数初始化为0，每次循环伊始将值传递给*start*参数。由于相对位置的唯一性，重新排序后的单元集合具有一一对应的映射关系。步骤6到8遍历集合内的逻辑单元，将瞬态电流编码为PWL(t_1 val_1 t_2 val_2 ... t_n val_n)的分段线性格式，依据映射关系连接到寄生网络模型的内部节点，从而确保正确的电源传递关系。在步骤9中，Probe函数检索寄生网络模型的金属层信息，筛选出顶层电源网格内的金属线，表述为.PROBE TRAN $i(*)$语句并添加到Spice仿真模型。同时，如有片外电源网络模型可执行步骤10实现模型拼接。这样，EMSim融合了寄生网络模型、单元级电流源和独立电压源，构成了描述拓扑结构和电气行为的Spice仿真模型，通过仿真获得顶层电源网格的瞬态电流分布。以HSpice工具为例，借助改进节点分析、基尔霍夫电流和电压定律，Spice仿真模型将被重构为具有不同初始条件的微分代数方程系统 [105]。如公式(3-7)所示，$\boldsymbol{v} = \boldsymbol{v}(t)$表示节点电压和分支电流的向量，$\boldsymbol{u} = \boldsymbol{u}(t)$表示电压源及其他输入向量。电荷、电流和时间分别用$q$，$i$，$t$表示。HSpice使用直接线性求解器求解该方程系统，并输出选定金属线集合的瞬

Algorithm 4 Spice仿真模型的构建算法

Input:

$CellDef, Current, (x,y)_{def}$ ▷ DEF文件的单元名称、单元电流和单元坐标

$CellDspf, (x,y)_{dspf}$ ▷ DSPF文件的单元名称和单元坐标

Output: $SpiceModel$ ▷ 用于电流分析的Spice模型

$CellDef \leftarrow \text{Order}(x,y)_{def}$

$CellDspf \leftarrow \text{Order}(x,y)_{dspf}$

$Current \leftarrow (CellDef \leftrightarrow CellDspf)$

for each $CellDef$ **do**

    $SpiceModel \leftarrow \text{PWL}(CellDef, Current)$

end for

$SpiceModel \leftarrow \text{Probe}(SpiceModel)$

$SpiceModel \leftarrow Off\ chip\ Parasitics$

function ORDER(x,y)

    $vertical = argsort(y)$

    $x, y = x, y[vertical]$

    $classy = unique(y)$

    for each $classy$ **do**

        $end = start + count\_nonzero(y == classy)$

        $tmp\_x = x[start : end]$

        $horizontal = argsort(tmp\_x)$

        $x[start : end] = tmp\_x[horizontal]$

    end for

end function

态电流。需要注意的是，直接线性求解器的时间复杂度与电路规模具有超线性关系，改进的求解器如FastSPICE引擎可以进一步加快仿真过程。

$$\frac{dq(\boldsymbol{v},t)}{dt} = i(\boldsymbol{v},\boldsymbol{u},t) \tag{3-7}$$

3.2.3 电磁计算环节

对于某观测点特定时刻的磁感应强度$B_{t,p}$，本节采用毕奥-萨伐尔定律进行磁场计算，如公式(3-8)所示。图3-9为电磁计算的解释模型，描述了上述公式的求解细节。在直角坐标平面，x_i表示第i条金属线在x轴向子区域的数量，y_i表示y轴向子区域的数量。相应地，l_i和w_i分别为第i条金属线子区域的长度和宽

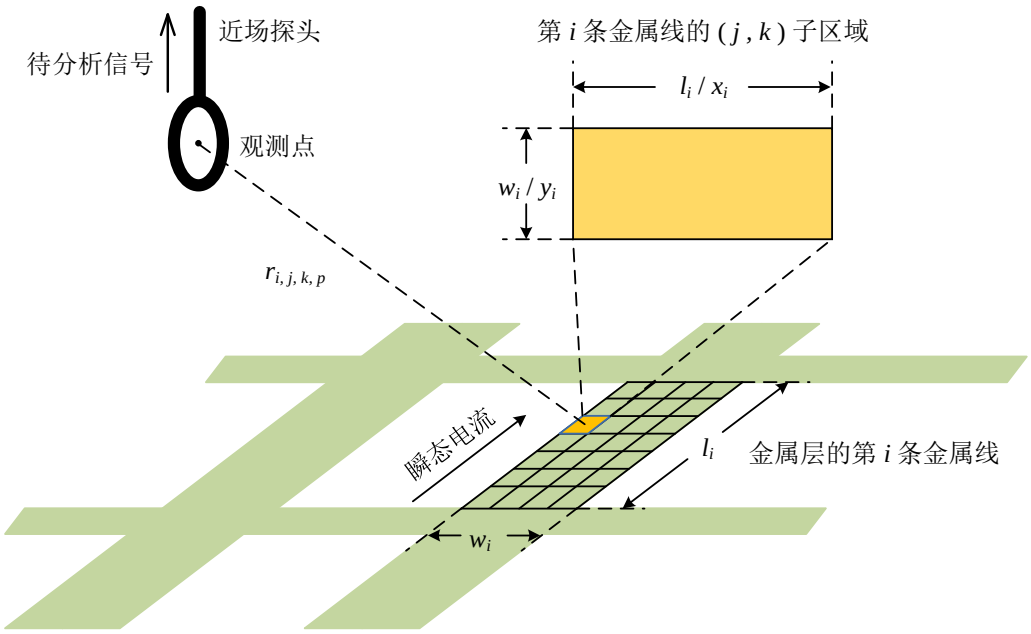


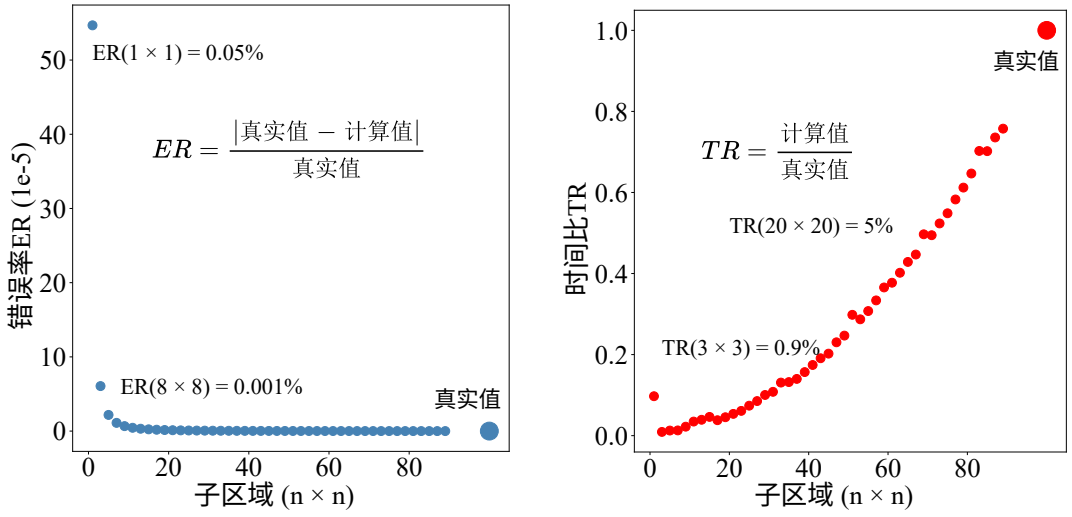
图 3-9 电磁计算的解释模型

度。$r_{i,j,k,p}$为子区域的中心点到观测点的空间距离，其方向由单位向量$\hat{r}_{i,j,k,p}$表示。$J_{i,t}$表示第i条金属线在t时刻的电流密度，μ_0为真空磁导率。在电磁计算环节，金属线总数由顶层金属层内的电源网格决定，而非考虑整个芯片的金属互连网络。此时，金属线的物理尺寸小于波长的1/10，所以将其视为面电流均匀分布的电小尺寸天线。这使得EMSim可通过离散法求解公式(3-8)的近似值，即将每条金属线划分为一定数量$(x_i \times y_i)$的等面积矩形平面。首先计算各子区域的面积与金属线内电流的乘积，然后利用空间距离$r_{i,j,k,p}$计算子区域对观测点的磁场贡献量。根据场叠加理论将所有子区域的贡献矢量相加，得到观测点的近似磁感应强度。需要注意的是，将金属线进行区域划分和离散求解，是模拟金属线面积分的求解过程。因此，子区域数量越多，近似计算值就越接近真实值。

$$B_{t,p} = \frac{\mu_0}{4\pi} \sum_{i \in wires} \sum_{j \in x_i} \sum_{k \in y_i} \frac{J_{i,t} \times \hat{r}_{i,j,k,p}}{r^2_{i,j,k,p}} l_i w_i \tag{3-8}$$

以一条金属线 ($l = 10\mu$m, $w = 5\mu$m) 为例，保持电流值和观测点不变，将金属线划分不同数量的子区域，采用离散法求解观测点的磁场强度。以面积分求解的磁场强度作为真实值，离散法求解的磁场强度为计算值，分析不同子区域数量对应的精度损失和时间效率。用错误率 (Error Rate，ER) 来表示离散求解过程的精度损失，即计算值的误差占真实值的百分比。使用时间比 (Time Rate，TR) 来比较两种求解过程的时间效率，即离散求解与真实求解的时间开销比值。如图3-10所示，随着子区域数量的增加，错误率迅速下降，并且从(8×8)开始低于0.001%。而时间比则随着子区域数量逐渐增加，从(20×20)开

始超过了5%。由此可见，在保证求解精度的同时，子区域数量应尽可能降低计算成本。EMSim提供了相应的参数选项，允许用户自主确定子区域的数量。



(a) 错误率　　(b) 时间比

图 3-10　不同子区域划分的错误率和时间比

由于每个子区域到观测点的空间距离为固定值，在仿真给定时间点的磁场时只需要计算$J_{i,t} \times \hat{r_{i,t}}$的值。其结果可被扩展为叉乘矩阵，与距离矩阵相乘即可得到$B_{t,p}$。该过程的磁场算子Field如算法5所示，输入为特定时间点的电流密度，输出各个轴向的磁场强度。在CPU平台上，矩阵求解可以通过Numpy库的多维数组实现。同时，得益于大量且高效的内核，GPU平台支持多维数组的并行计算，从而加速了电磁计算过程。Numpy库不支持GPU平台上的数值计算，为此本节采用适配GPU平台的CuPy库。它使用NVIDIA的CUDA平台与相关依赖库，包括cuBLAS、cuDNN、cuRAND、cuSOLVER、cuSPARSE和NCCL，充分利用了GPU的并行计算架构[106, 107]。Numpy库和CuPy库具有相似的语法风格，两者在EMSim工具中相互兼容，能够在CPU和GPU平台间切换矩阵求解模式。

在实际测量中，芯片的磁场会被近场探头接收，磁通量变化在探头线圈处感应出电压信号，如公式(3-9)所示。所以，公式(3-8)的结果被转化成近场探头的电压信号。在公式(3-10)中，磁场的导数dB/dt是对时间点的离散取值。

$$V_{probe} = -\int_{S_{probe}} \frac{dB}{dt} \cdot ds \tag{3-9}$$

$$x'(n) = \frac{x(n+1) - x(n-1)}{2} \tag{3-10}$$

$$V_{amp} = 10^{\frac{g}{20}} \cdot V_{probe} \tag{3-11}$$

探头接收到的电压信号通常较弱，前置放大器会对信号进行放大处理。假设放大器的增益为gdB，放大后的电压信号V_{amp}由公式(3-11)计算。在传输到示

Algorithm 5 磁场算子

function FIELD(t)
    $J_x = J(t) \times \hat{x}$
    $J_y = J(t) \times \hat{y}$
    $J_z = J(t) \times \hat{z}$
    $temp = l \cdot w \ / \ (4 \cdot \pi \cdot r^3)$
    $H_x = (J_y \cdot r_z - J_z \cdot r_y) \cdot temp$
    $H_y = (J_z \cdot r_x - J_x \cdot r_z) \cdot temp$
    $H_z = (J_y \cdot r_x - J_x \cdot r_y) \cdot temp$
return H_x, H_y, H_z
end function

波器的前端电路时，由于设备带宽的限制，前端电路具有低通滤波器的作用，将滤除电压信号中特定频率的谐波。

3.3 与传统方法的对比验证

本节从仿真精度、测评准确度和计算成本方面，全面比较EMSim与传统方法的效果，仿真精度的对比涵盖时域和空间域特征。在本节中，传统方法被称为ConvEM，其中电流分析采用晶体管级Spice仿真，电磁计算则采用CPU平台实现矩阵求解 [48]。

3.3.1 评价指标

对于电磁仿真方法质量的评估，关键是分析仿真结果与实际结果的匹配度。早期的仿真质量评估通常选用视觉比较法，通过主观地肉眼观察判断仿真结果的优劣 [44, 47, 108, 109]。为了更客观地评估仿真方法，本论文采用多种指标定量分析仿真结果的各个方面，不仅包括电磁辐射的固有精度，如时域特性和空间特征，还有其应用到侧信道安全评估的准确度。

3.3.1.1 固有精度指标

在时域上，给定观测点的电磁辐射表现为一维时变信号。对于一维信号的相似性比较，常用的度量指标有欧氏距离、马氏距离、决定系数和互相关系数等。其中互相关是两个信号相对于采样点的函数，用于度量仿真信号与参考信号间的相似性。公式(3-12)给出了互相关系数的计算式，$Cov(X, Y)$为信号X和Y的协方差，$Var(X)$和$Var(Y)$为自身的方差。本节采用归一化互相关作为相似性度量

指标，按照特定规律将信号分割为信号子集，分别计算每对子信号的互相关系数后取平均值，如公式(3-13)所示。将仿真信号x和参考信号y归一化到$[-1,1]$范围内，$\|x\|$和$\|y\|$是具有T采样点的归一化信号。在每个输入激励下，计算归一化信号$\|x\|$和$\|y\|$之间的互相关系数。对N个输入激励的互相关系数矩阵进行平均操作，获得代表时域准确度的NCC指标。

$$\rho(X,Y)=\frac{Cov(X,Y)}{\sqrt{Var(X)Var(Y)}} \tag{3-12}$$

$$\mathrm{NCC}=\frac{1}{N}\sum_{i=1}^{N}\frac{\sum_{t=1}^{T}(\|x\|_t^i-\|\bar{x}\|^i)(\|y\|_t^i-\|\bar{y}\|^i)}{\sqrt{\sum_{t=1}^{T}(\|x\|_t-\|\bar{x}\|^i)^2}\sqrt{\sum_{t=1}^{T}(\|y\|_t^i-\|\bar{y}\|^i)^2}} \tag{3-13}$$

空间分布是电磁辐射另一个重要特征，以二维信号的形式呈现，可以视作图像进行相似度分析。本论文采用结构相似性 (Structural Similarity，SSIM) 指标，从亮度、对比度和结构三个方面比较仿真样本x和参考样本y，具体计算见公式(3-14)、公式(3-15)和公式(3-16)。其中，(μ_x,μ_y)、(σ_x,σ_x)分别为x和y的平均值和标准差，σ_{xy}为x和y的协方差，C_1、C_2和C_3均为常数，避免除零引起的不稳定。结构相似性指标定义为$l(x,y)^\alpha$、$c(x,y)^\alpha$和$s(x,y)^\gamma$的乘积，取$\alpha=\beta=\gamma=1$以及$C_3=C_2/2$，得到比较空间域准确度的SSIM指标。

$$l(x,y)=\frac{2\mu_x\mu_y+C_1}{\mu_x^2+\mu_y^2+C_1} \tag{3-14}$$

$$c(x,y)=\frac{2\sigma_x\sigma_y+C_2}{\sigma_x^2+\sigma_y^2+C_2} \tag{3-15}$$

$$s(x,y)=\frac{\sigma_{xy}+C_3}{\sigma_x\sigma_y+C_3} \tag{3-16}$$

$$\mathrm{SSIM}=\frac{(2\mu_X\mu_Y+C_1)(2\sigma_{XY}+C_2)}{(\mu_X^2+\mu_Y^2+C_1)(\sigma_X^2+\sigma_Y^2+C_1)} \tag{3-17}$$

3.3.1.2 应用精度指标

考虑电磁仿真的实际应用，除了固有精度之外，还需验证安全测评结果的有效性。在硅前电磁安全测评中，通过芯片电磁仿真获得电磁辐射，结合安全评估方法量化安全性。安全评估方法包括基于攻击的评估方法和基于信息泄露的评估方法，后者诸如TVLA技术具有误报的缺陷，在某些情况下，尽管TVLA结果显示设计具有泄漏风险，但实际攻击无法成功获取敏感信息。因此，本论文采用基于攻击的评估方法，使用CEMA评估信息泄露风险，以皮尔逊相关系数和MTD为安全指标，分析EMSim仿真的测评准确度。

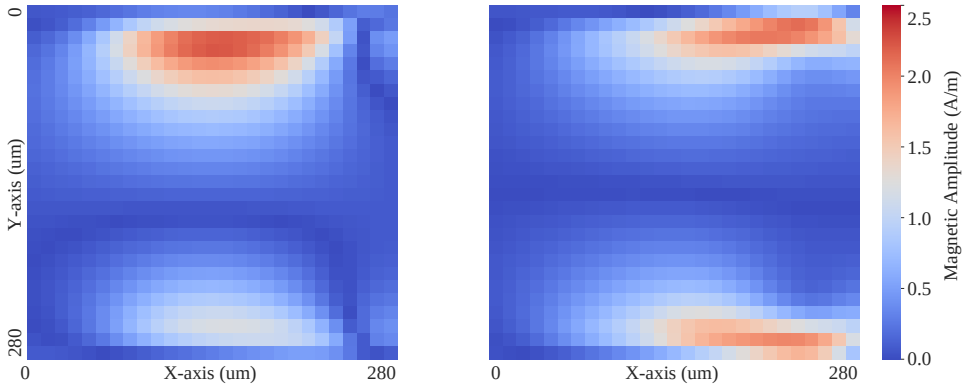
3.3.2 实验电路设计

本节以32位S-Box电路作为实验电路，该电路由四个8位S-Box模块组成，每个模块均以查找表形式实现。S-Box模块将乘法求逆与仿射变换相结合，提供了抵抗代数密码分析的非线性特征。选用SMIC 180nm CMOS工艺，对32位S-Box电路进行逻辑综合和物理实现，最终生成GDSII格式的物理版图。该版图面积为280.36μm×280.24μm，由900个逻辑单元和31546条金属线构成。按照典型的设计实践，将电源网格放置于M5和M6金属层内，将电源轨线放置在M1金属层内，信号互连线则置于所有金属层内。在物理版图中，电源VDD和接地VSS端口分布在左侧中间处，连接呈矩形排布的电源环线，为底层电源轨和逻辑单元供应1.8V电压。将时钟频率设置为20MHz，在工作过程中，明文和密钥首先进行异或操作，其后作为输入数据传送到S-Box模块。对应100个随机测试激励，EMSim通过器件模型近似预先构建了单元级电流源。然后借助寄生网络约减的思想，排除寄生网络模型中的信号互连线，将用于电流分析的金属线数目减少到16070，仿真得到了每条金属线的瞬态电流。在30μm高度处将芯片平面划分为28×28的网格矩阵，每个格点的边长约为10μm。在电磁计算环节，EMSim只关注顶两层电源网格的瞬态电流，分别对应754条金属线，将这些金属线划分成100 (10×10) 个子区域，通过多维矩阵求解获得了每个格点的磁场数据。

3.3.3 实验结果分析

图3-11 (a)和图3-11 (b)分别是两种方法得到的磁场分布图，此时S-Box电路的运行时间点$t = 26$ns。显示色条用于量化磁场强度的幅度，蓝色和红色分别代表最低幅度和最高幅度。由图可知，ConvEM和EMSim的结果具有相似的空间特征，磁场强度热点分布在物理版图的上侧和下侧，并近似圆形地向四周扩散，SSIM指标表明两者的相似程度约为95%。进一步地，图3-12展示了P_0点 $(x = 175\mu\text{m}, y = 15\mu\text{m})$ 的归一化时域波形，上方子图为ConvEM仿真的时域曲线，下侧子图为EMSim仿真的时域曲线，两者随时间点具有近似的变化趋势，波形峰值0.69均出现在1109ns处，NCC指标表明两者在时域上具有82%的相似性。

当应用到硅前安全测评时，本节使用两种仿真方法得到的磁场曲线，执行CEMA攻击来恢复S-Box电路的敏感信息。考虑工艺偏差的影响，在ConvEM和EMSim仿真结果中加入相同的高斯噪声，遍历芯片表面的网格矩阵量化信息泄露风险。取正确密钥的最大相关系数作为信息泄露的度量，代表着电磁曲线与敏感信息的依赖程度，图3-13 (a)和图3-13 (b)展示了随空间位置变化的信息泄露分布。右侧的显示色条用于量化信息泄露的程度，越接近顶部色条的颜色代表越大的相关性峰值，该位置具有较大的信息泄露风险。



(a) ConvEM仿真结果　　(b) EMSim仿真结果

图 3-11　S-Box电路的磁场分布图 (SSIM = 0.95)

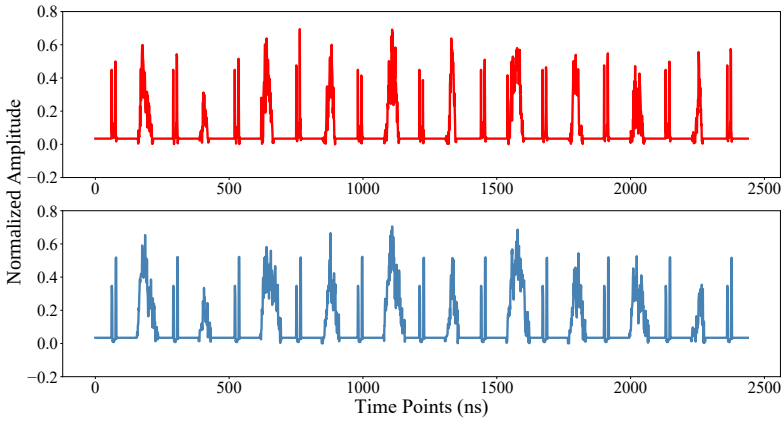
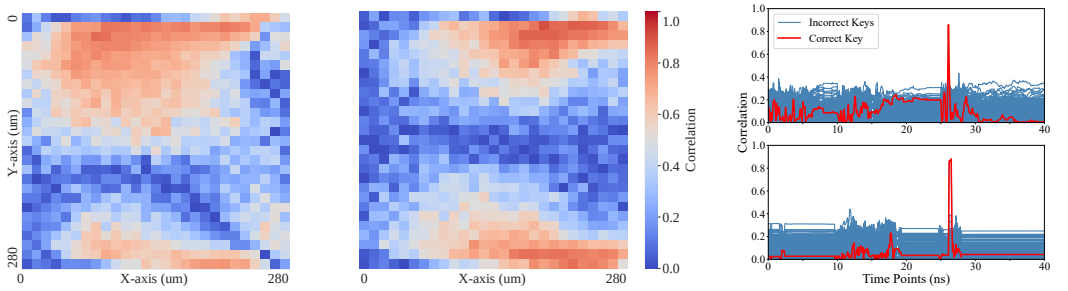


图 3-12　ConvEM和EMSim仿真的时域曲线 (NCC = 0.82)

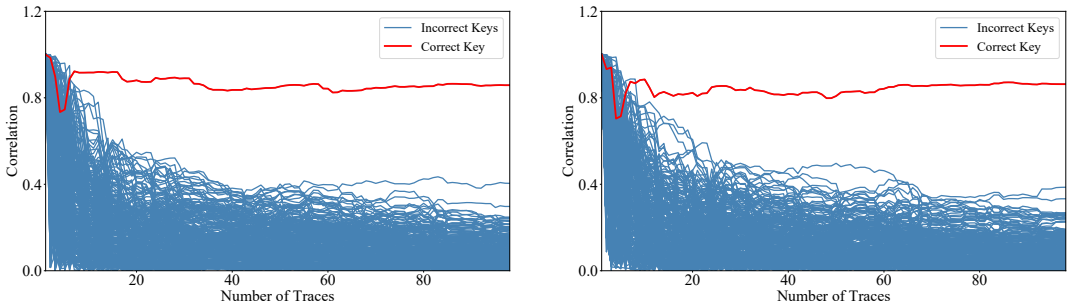
ConvEM和EMSim预测的信息泄露具有相似的空间分布，从物理版图的左上侧和左下侧逐渐向右侧扩散，空间准确度指标SSIM为0.86。对于芯片表面的信息泄露热点，猜测密钥对应的相关性曲线是时间点的函数，如图3-13 (c)所示。可以看出，ConvEM和EMSim具有相似的预测结果，正确密钥的相关性曲线在26ns处出现峰值，且皮尔逊相关系数约为0.82。随着测试曲线数目的增加，所有猜测密钥的相关性峰值将逐渐下降。相对于其他猜测密钥，正确密钥的相关性峰值下降比较缓慢，从而在诸多错误密钥中显现出来，如图3-14所示。其中，红色曲线对应正确的猜测密钥，蓝色曲线对应错误的猜测密钥。由图3-14 (a)可知ConvEM预测的MTD ≈ 7，由图3-14 (b)可知EMSim预测的MTD ≈ 8，即两种方法具有接近的安全测评结果。

在计算成本方面，ConvEM仿真单个时间点的总时间为2.25s，其中2.017s用于电流分析环节，0.233s用于电磁计算环节。而EMSim仿真需要的总时间为0.069s，其中0.065s用于电流分析，0.003s用于电磁计算，各自实现了31倍和78倍的效率提升。在仿真所需的时间成本上，相对于ConvEM仿真方法，



(a) ConvEM仿真结果　(b) EMSim仿真结果　(c) 随时间变化的相关性曲线

图 3-13　S-Box电路的信息泄露分布图 (SSIM = 0.86)



(a) ConvEM仿真结果　(b) EMSim仿真结果

图 3-14　随曲线数目变化的相关性曲线

EMSim工具提升了32倍的时间效率。两种方法的电流分析都运行在Intel X5690 (3.47GHz) 平台上，EMSim在NVIDIA V100 GPU平台执行电磁计算，而ConvEM的电磁计算运行在Intel 9700k (4.6GHz) 平台。

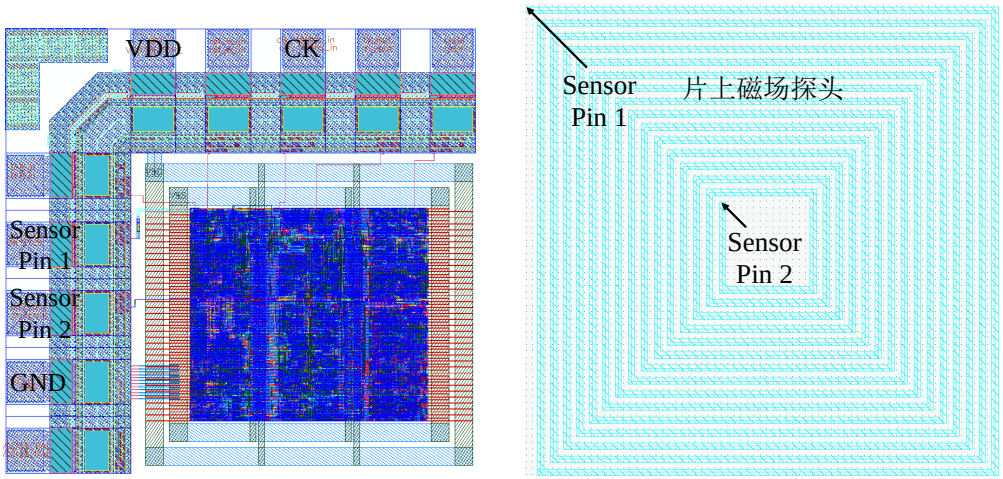
3.4　基于S-Box芯片的实测验证

本节设计了S-Box芯片并进行流片测试，比较EMSim仿真结果与实际测量数据，从仿真精度和测评准确度证明了EMSim的有效性。

3.4.1　S-Box芯片设计

S-Box芯片的主模块是3.3.2节的32位S-Box电路，负责执行字节替换的并行运算。接口电路采用通用异步收发传输器 (Universal Asynchronous Receiver/Transmitter，UART) 接口，其中uart_fifo为串口接收模块，uart_fifo_out为串口发送模块，而data_select为串口配置模块，设置串口通信的数据帧格式和波特率。在工作过程中，明文和密钥首先进行异或操作，其后作为输入数据传送到S-Box模块。选用SMIC 180nm CMOS工艺进行逻辑综合和布局布线，生成GDSII格式的物理版图，如图3-15 (a)所示。芯片面积为790μm × 750μm，由1960个逻辑

单元和91985条金属线构成。时钟频率和供电电压分别设置为1.5MHz和1.8V。时钟CK端口位于芯片版图的正上方，电源VDD和接地VSS端口位于芯片版图的左上脚和左下角，连接由电源环形和两对电源条线组成的电源网格。为了模拟局部电磁分析，本节利用顶层金属资源设计了片上磁场探头，其线圈由中心开始向四周延伸并覆盖到整个电路。如图3-15 (b)所示，Sensor Pin 1和Sensor Pin 2为片上磁场探头的信号接收端口。由于磁场探头置于芯片内部，且磁通量是所有同心线圈的磁通量累加值，因此具有较高的测量信噪比。



(a) 芯片版图　　(b) 片上磁场探头

图 3-15　S-Box芯片版图和片上磁场探头

为了测试S-Box芯片的实际数据，本节设计了测试电路板的原理图，并完成了PCB实物制造，主要包括芯片模块、电源模块、时钟模块、串口模块以及接口模块，如图3-16所示。芯片模块采用板上芯片封装 (Chips on Board，COB) 技术，用黑胶把芯片和键合引线包封起来，避免芯片直接暴露在空气中。电源模块外接7.2V的直流电压，使用AMS1117-3.3稳压芯片输出3.3V电压，使用AMS1117-1.8稳压芯片输出1.8V电压，为芯片I/O单元及其他模块传输稳定电源。时钟模块采用四脚有源晶振，其中四脚连接3.3V电压，三脚输出1.5MHz振荡信号，作为S-Box芯片的时钟信号。串口模块用于S-Box芯片与上位机的数据通信，向芯片发送输入数据并回传输出数据。接口模块提供芯片的复位信号和使能信号，以及片上磁场探头的输出接口，用于采集芯片内部实时变化的磁场信号。

3.4.2　实验结果分析

在实际测量期间，示波器的采样率设置为2.5GSa/s，以平均模式收集片上磁场探头的电压信号。每次输入相同的1000条测试激励，重复进行8次电压信号的采集过程，利用静态对齐技术进行时域曲线对齐，采用平均降噪技术滤除外部

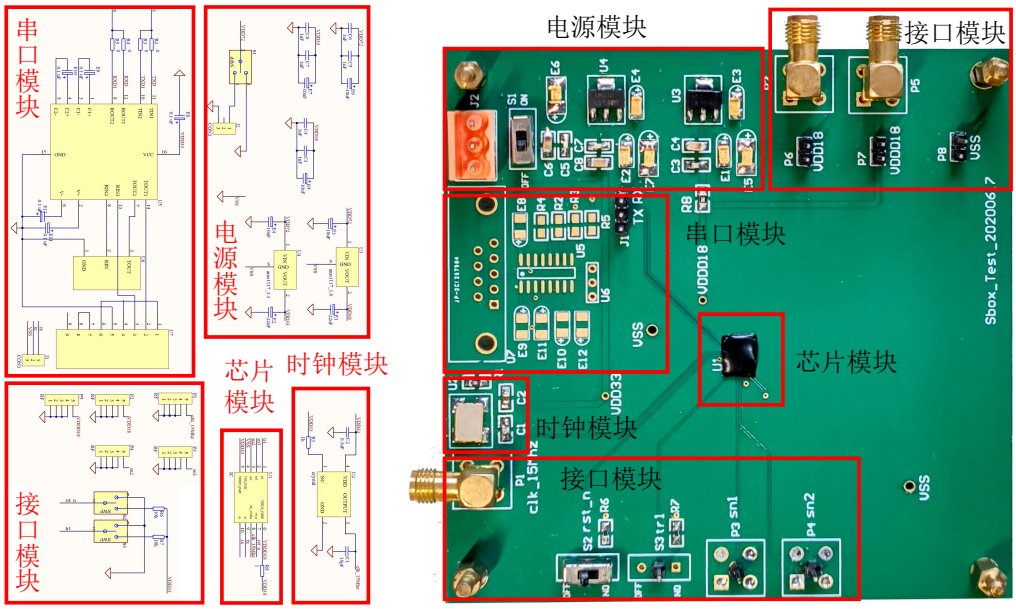


图 3-16　S-Box芯片的测试电路板

环境噪声。在电磁仿真期间，得益于器件模型近似和寄生网络约减，EMSim将电流分析所需的金属线降低到56171，得到S-Box芯片金属层的瞬态电流分布。将芯片表面划分为28 × 26的网格矩阵，选取最上两层电源网格的668条金属线，采用离散法计算所有同心线圈的感应电动势，通过累加上述结果获得片上磁场探头的电压信号。每个时间点的仿真总计需要1.192s，其中1.161s用于电流分析环节，0.031s用于电磁计算环节。图3-17展示了两种方法得到的电压信号，上方子图为实际测量数据，下方子图为EMSim仿真结果，其中横轴为时间点而纵轴代表信号幅度。由图可知，电压信号峰值出现在相同的时间区间，在该时间段内，状态寄存器更新S-Box模块的输出数据。在仿真精度方面，代表时域准确度的NCC指标为0.74，表明实测数据和仿真结果具有74%的相似度。

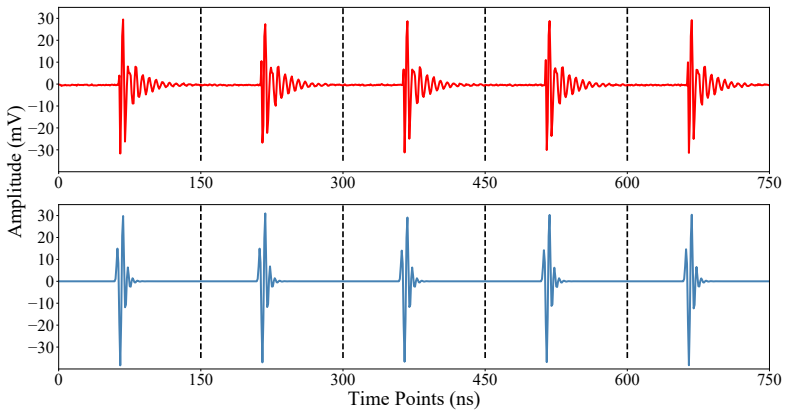


图 3-17　实际测量和EMSim仿真的磁场曲线

为验证安全测评的准确度，分别对实测数据和仿真结果执行CEMA攻击，泄露模型为S-Box输出结果的汉明距离。图3-18展示了猜测密钥随时间变化的相关性曲线，上方子图代表实际测量数据，下方子图代表EMSim仿真结果。对于实测数据和仿真结果，正确密钥的相关性为峰值0.21和0.23，位于横轴上[9, 14]的时间范围，且均大于其他错误密钥的相关系数。与3.3.3节的测评结果相比，片上磁场探头覆盖了信息泄露较低的位置，因此降低了正确密钥的相关性峰值。图3-19为猜测密钥随曲线数目变化的相关性曲线，攻击者使用185条实测曲线可恢复正确密钥，而仿真结果预测攻击者需要162条曲线达成目的。因此，从安全测评的角度来看，EMSim仿真和实际测量具有一致的测评结果。

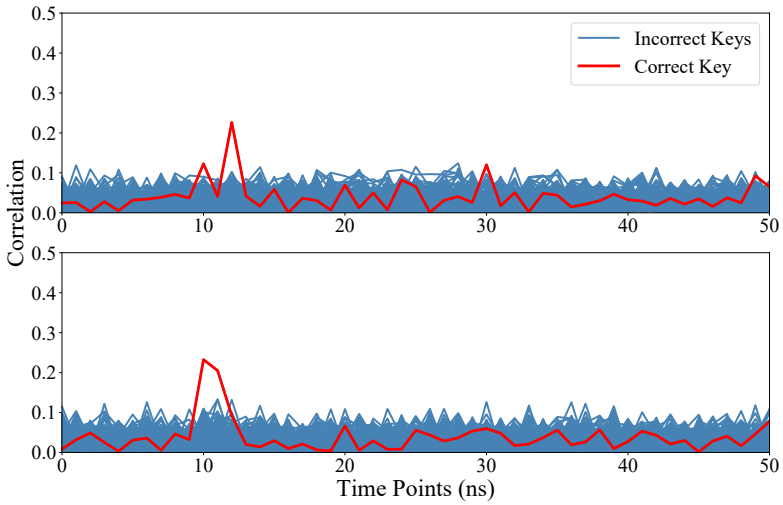
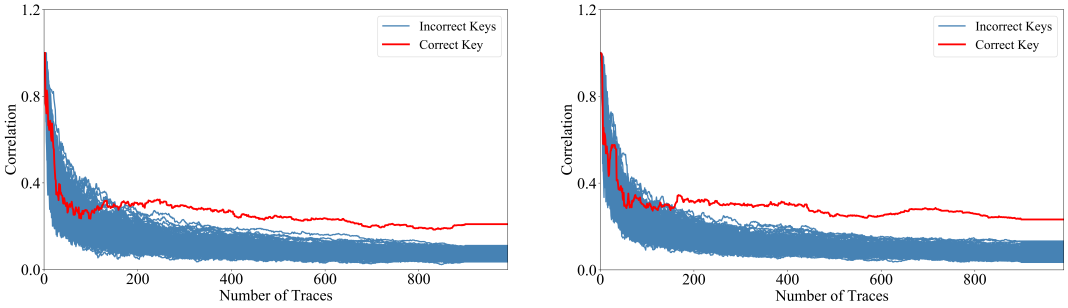


图 3-18　随时间变化的相关性曲线



(a) 实测数据　　(b) 仿真结果

图 3-19　随曲线数目变化的相关性曲线

3.5 基于AES芯片的实测验证

进一步地，本节设计了AES芯片并进行流片制造，通过比较实际数据和仿真结果的相似度，包括仿真精度和测评准确度，验证了EMSim仿真结果的有效性，也证明了EMSim在较大规模电路的适用性。

3.5.1 AES芯片设计

AES芯片用于实现128位AES算法的加密功能，主模块aes_core的原理图如图3-20所示，AES电路首先执行密钥扩展操作，然后进行十轮次的加密操作。其中，前九轮加密依次执行字节替换、行移位、列混淆和轮密钥加操作，而最后一轮不执行列混淆操作。每一轮加密运算中，字节替换操作占用四个时钟周期，其他操作占用后续一个时钟周期，使用状态寄存器存储密码中间值和密文输出。另外，reg_in模块用于接收明文和密钥，而reg_out模块用于发送密文。选用SMIC 180nm CMOS工艺进行逻辑综合和物理实现，将电源网格放置于M5和M6金属层，将电源轨线放置在M1金属层内，信号互连线分布在所有金属层，形成了最终投产制造的物理版图。图3-21为AES芯片的裸片图，左上方是两对电源和接地端口，连接电源环线和三对平行排布的电源条线。考虑I/O单元面积的情况下，芯片面积为1.6mm × 1.3mm，由14559个逻辑单元和733662个金属线构成，时钟频率和供电电压设置为25MHz和1.8V。

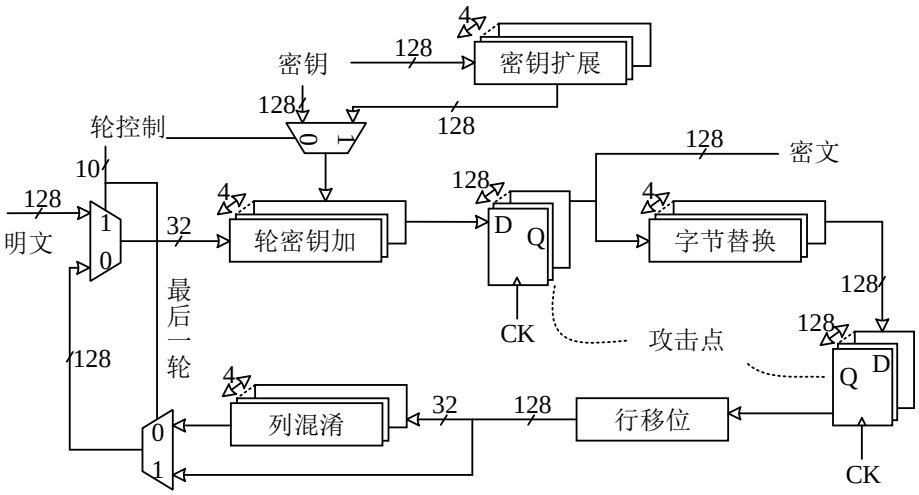


图 3-20 AES芯片的原理图

为了测试AES芯片的功能，本节设计了相应的测试电路板，由电源模块、芯片模块和接口模块组成。电源模块外接7.2V的直流电压，采用AMS1117-3.3和AMS1117-1.8电源转换芯片输出3.3V和1.8V，为I/O单元和芯片内核传输直流稳定电源。在芯片模块中，AES芯片采用双列直插式陶瓷封装，由于输

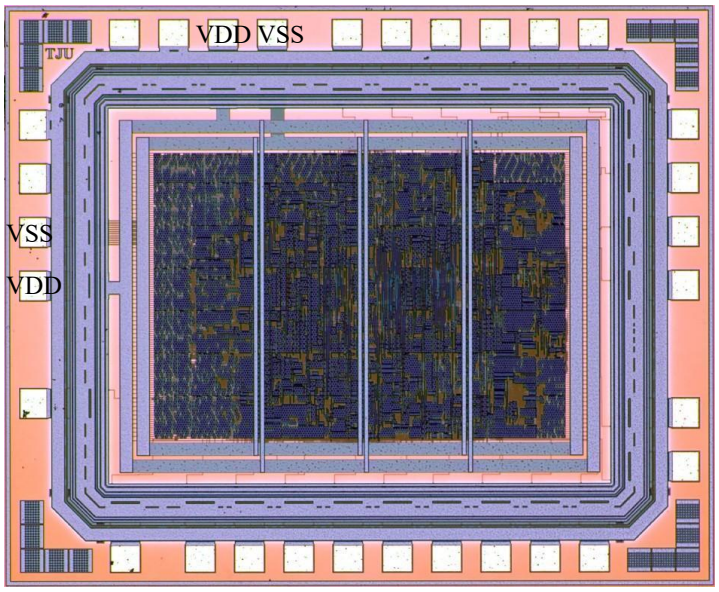


图 3-21　AES芯片的裸片图

入输出接口单元较多，使用48P芯片锁紧座放置封装后芯片。接口模块提供时钟信号、复位信号和使能信号，还提供了芯片输入和输出信号的接口。此外，使用AX7035 FPGA开发板设计时钟和串口模块，该开发板板载了ARTIX-7系列的FPGA芯片，并提供了50MHz有源晶振给FPGA作为系统时钟。在时钟模块中，混合模式时钟管理器 (Mixed-Mode Clock Manager，MMCM) 将分频时钟分配给AES芯片的时钟输入端。串口模块采用UART通信协议，负责AES芯片和上位机的数据通信，向芯片发送输入数据并回传输出数据。为了保证信号传输质量，FPGA开发板和测试电路板采用硬连接方式，如图3-22所示。当密钥设定为128′h0123_4567_89ab_cdef_0123_4567_89ab_cdef，输入明文128′hfecc_5206_ba78_64db_0e62_240b_b1e8_613d时，经过10轮加密运算后，输出密文为128′h82c9_37f6_ef5e_ccbb_db13_ac23_345b_abe6，输出密文与预期结果一致，证明了AES芯片功能的正确性。

3.5.2　实验环境配置

为了采集AES芯片的电磁信号，本节搭建了图3-23所示的近场扫描系统，由三轴位移台、显微镜摄像头、近场微探头、示波器、屏蔽箱和上位机组成。该系统选用Langer ICR HH250-75近场微探头，分辨率为150μm，集成增益为30dB的前置放大器。在测量过程中，显微镜摄像头用于芯片表面成像，并将图像显示在上位机上，据此可建立近场扫描的参考坐标系。将近场微探头放置在芯片表面，由三轴位移台控制其与参考原点的空间距离，步进精度为10μm，在上位机的控制下完成区域电磁扫描。收集到的磁场信号通过Tektronix MSO4054示波器

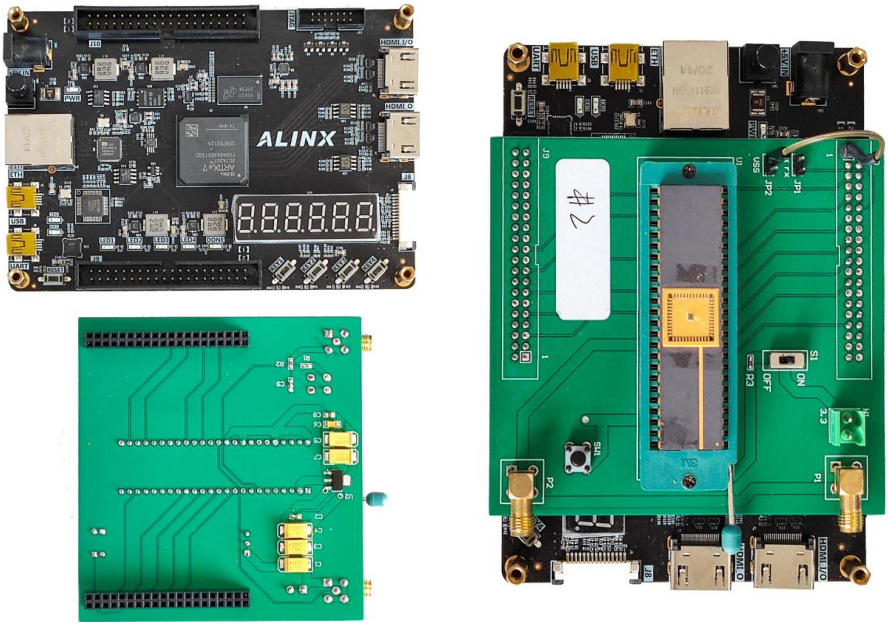


图 3-22　AES芯片的测试电路板

传输到上位机以进行后续处理。由此可见，上位机具有底层硬件控制、测试进程管理、数据存储、处理和显示等功能。此外，电磁测试设备放置在屏蔽箱中，以降低外部环境的噪声干扰。

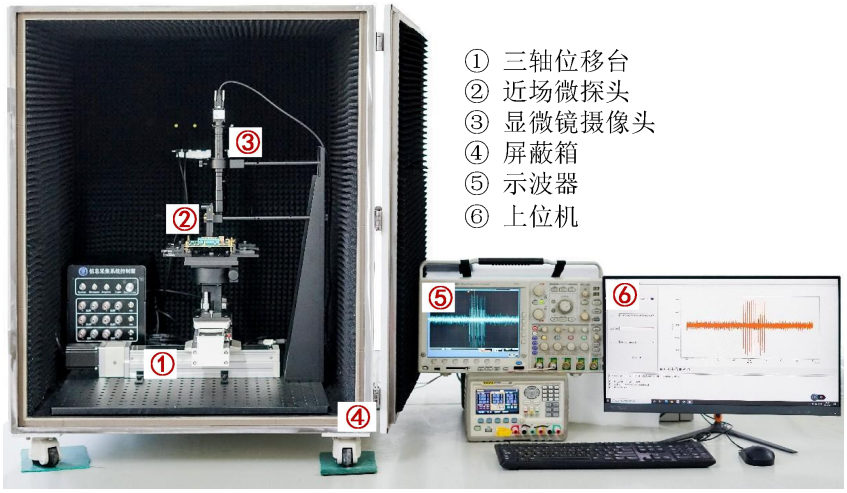


图 3-23　近场扫描系统的整体架构

根据近场扫描系统的基本功能，设计了AES芯片的电磁采集流程，具体步骤如下所示：

第一步，初始化系统的参数设置，指定各硬件设备的数据接口、输入数据的文件路径以及电磁曲线的保存路径。同时将示波器的采样率和带宽设为2.5GSa/s和500MHz，存储深度设为100K采样点。

第二步，开启显微镜摄像头捕获芯片图像，选取芯片版图的左下角作为参考原点，建立了近场扫描的参考坐标系，表示为22×12的网格矩阵，此时三轴位移平台的步进距离为50μm。

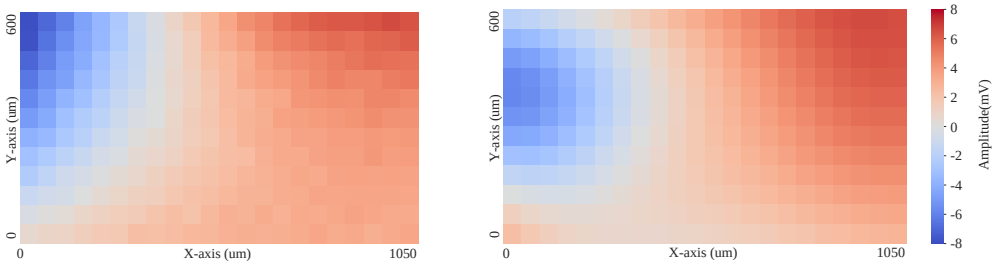
第三步，上位机向AES芯片发送明文和密钥数据，同时接收芯片回传的密文数据，检查该数据是否与预期结果一致。在验证加密的正确性后，触发示波器采集当前位置的电磁信号，上传到上位机并保存在指定位置。

第四步，遍历网格矩阵的每个位置，重复上述功能验证和近场扫描过程，共采集了26400条电磁曲线。为尽可能降低环境噪声，取32次重复测量的平均值作为最终数据，用于后续的侧信道安全评估。

3.5.3 实验结果分析

为了仿真芯片表面的电磁场，EMSim构建了14559个逻辑单元的电流源激励，排除了寄生网络模型的信号互连线，在用于电流分析的Spice仿真模型中，金属线数目从733662减少到365529，仿真得到了每条金属线的瞬态电流。选择顶两层电源网格中1424条金属线，将这些金属线划分成100个子区域，采用离散法计算22×12网格矩阵的磁场数据。每个时间点的仿真成本总计3.860s，其中3.451s用于电流分析，0.409s用于电磁计算。根据实际测量数据和EMSim仿真结果，构造了时间点 ($t = 1356.4$ns) 的磁场分布图，如图3-24所示。在该时间点所在的时钟周期，状态矩阵的前四个字节进行字节替换操作。在空间分布特性方面，实测数据和仿真结果具有98%的相似度。具体来说，沿负轴向和正轴向的最高幅度分别出现在左上角和右上角，当近场微探头从左向右移动时，电磁信号的幅值会先沿负轴向减小，然后沿正轴向逐渐增大。因此，图3-24 (a)和图3-24 (b)均出现信号幅值的正负边界，在磁场分布图上具有相似的变化趋势。另外，本节选择网格矩阵的两个格点，对于AES芯片加密期间的所有操作，比较了仿真结果与探头接收信号的时域特性。图3-25为格点P_1 ($x = 25\mu\mathrm{m}, y = 475\mu\mathrm{m}$) 的曲线对比图，上方子图为实际测量数据，下方子图为EMSim仿真结果，两者幅度均分布在-10mV到10mV之间，相似度指标NCC为0.85。图3-26为格点P_2 ($x = 475\mu\mathrm{m}, y = 225\mu\mathrm{m}$) 的曲线对比图，实测数据和仿真结果均在$[-5\mathrm{mV}, 5\mathrm{mV}]$的幅度范围内，相似度指标NCC为0.74。上述结果表明，EMSim能够很好地仿真近场探头的接收数据。

当应用到侧信道安全测评时，本节使用实际测量和EMSim仿真数据，通过CEMA攻击恢复AES芯片的敏感信息。考虑到工艺偏差的影响，在仿真结果中加入高斯分布的随机噪声，选择字节替换的状态寄存器为攻击点，计算寄存器数据的汉明距离模型，遍历芯片表面的网格矩阵量化信息泄露风险。取正确密钥的相关性峰值度量信息泄露风险，图3-27 (a)和图3-27 (b)展示了随空间位置



(a) 实测数据　　(b) 仿真结果

图 3-24　AES芯片的磁场分布图

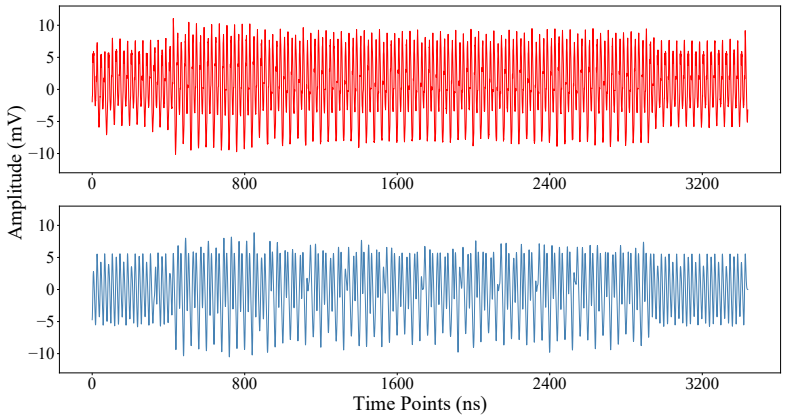


图 3-25　P_1格点处实际测量和EMSim仿真的磁场曲线

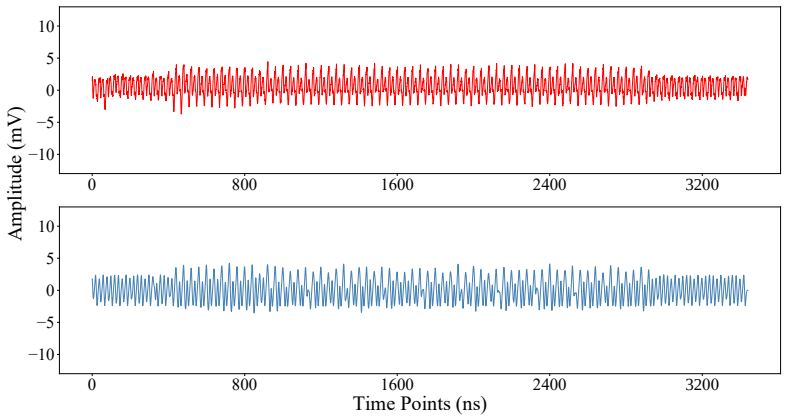
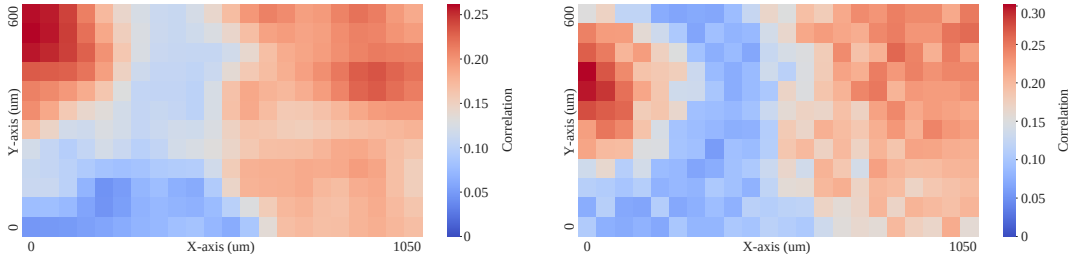


图 3-26　P_2格点处实际测量和EMSim仿真的磁场曲线

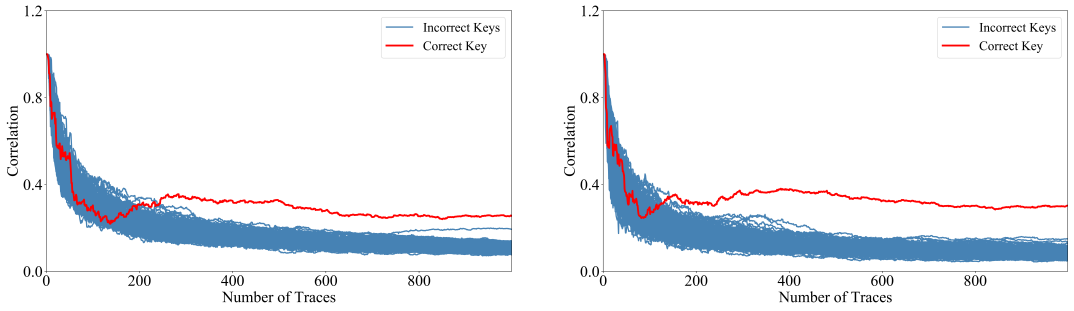
变化的信息泄露分布图，左上角和右上角具有较高的信息泄露风险，空间准确度指标SSIM为0.93，表明两种信息泄露分布具有相似的空间特性。其后，分析实测数据在P_1和P_2格点的泄露情况，图3-28 (a)和图3-29 (a)将猜测密钥的相关性表示为曲线数目的函数。格点P_1处正确密钥的最大相关性系数为0.25，攻击者使用244条实测曲线可恢复正确密钥。而在格点P_2处，攻击者在1000条电磁曲线后无法揭示正确密钥，相关性峰值0.13淹没在其他的错误密钥中。相应地，图3-

28 (b)和图3-29 (b)展示了仿真结果在两个格点的泄露情况。格点P_1处正确密钥的最大相关性系数为0.30，攻击者使用150条仿真曲线可恢复正确密钥。而在格点P_2处，攻击者在1000条电磁曲线后无法揭示正确密钥，其最大相关性系数仅为0.13。从这些比较结果可知，基于EMSim仿真的硅前测评具有接近硅后测评的准确度。



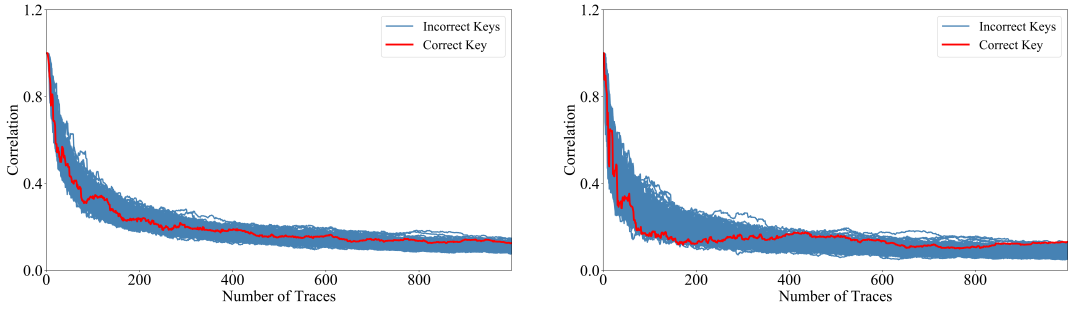
(a) 实测数据　　(b) 仿真结果

图 3-27　AES芯片的信息泄露分布图



(a) 实测数据　　(b) 仿真结果

图 3-28　P_1格点处随曲线数目变化的相关性曲线



(a) 实测数据　　(b) 仿真结果

图 3-29　P_2格点处随曲线数目变化的相关性曲线

3.6 本章小结

为实现硅前阶段的安全测评，本章开展了版图级电磁仿真方法研究，由版图数据获取集成电路的电磁信息。首先建立了集成电路的电气模型，分析了电磁辐射的产生和传播机理，包括电流聚合效应和金属屏蔽效应，明确了电磁信息的根本来源和主导因素。其次，介绍了版图级电磁仿真方法，采用器件模型近似、寄生网络约减和GPU并行计算，改进了电流分析和电磁计算环节，降低了芯片复杂性对计算成本的影响。相对于ConvEM仿真方法，EMSim方法提升了32倍的时间效率。最后，基于SMIC 180nm工艺设计了S-Box和AES电路，完成了两款芯片的流片制造和封装测试，搭建了近场扫描系统进行测试验证，结果表明仿真结果与实际数据相一致，具有高于74%的时域准确度，以及高达98%的空间准确度，能够准确地开展硅前安全测评，对信息泄露风险的预测准确度为93%。

第 4 章　基于生成对抗网络的测评优化方法研究

在大规模数据量的测评场景中，往往需要数千乃至上百万条曲线，才足以评估密码芯片的信息泄露风险。因此，这种场景对测评效率有着更高要求。为此，本章在版图级电磁仿真方法的基础上，借助生成对抗网络优化传统测评方法，通过生成器和判别器的对抗训练，准确地学习物理版图的磁场分布，快速地生成测评需要的大规模数据。具体来说，首先介绍了生成对抗网络的相关原理，阐明其应用于安全测评的可行性。在这之后，重点讨论了测评优化方法的整体流程，包括数据准备、模型训练和风险量化环节，以及各环节的数据处理、模型结构和实现算法。最后采用四种密码电路开展了硅前测评，对比传统测评方法，验证了测评优化方法的准确度，分析了不同规模数据量的效率提升值。

4.1　测评优化思想

在传统测评方法中，全部测评数据均由电磁仿真方法获得 [48, 49, 51]，包括上一章提出的EMSim。受限于复杂物理方程的求解过程，大规模数据量的仿真效率难以提升。近年来，机器学习在芯片设计领域的应用，如热分析和电压降分析，为上述问题提供了新的解决思路。在本章中，首次将机器学习和安全测评相结合，芯片电磁仿真被转换为图像翻译问题，基于EMSim提供的少量样本数据，由生成对抗网络加速大规模数据的获取，从而提升安全测评的应用效率。

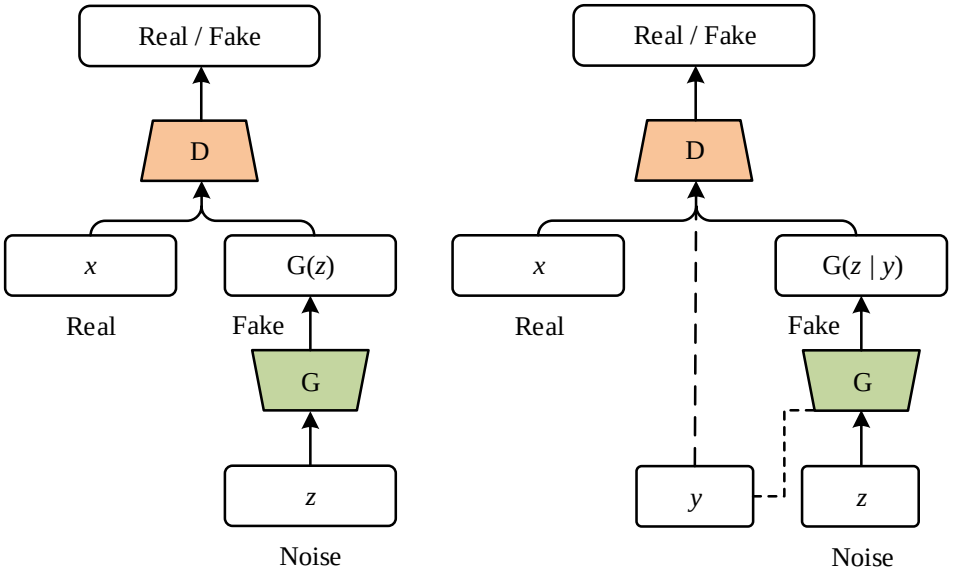
4.1.1　生成对抗网络

生成对抗网络 (Generative Adversarial Networks，GAN) 是基于深度学习的生成式模型 [110]。模型结构如图4-1 (a)所示，通过判别器和生成器这两个网络的对抗和博弈，准确地学习和模拟复杂的数据分布，广泛应用在图像生成、图像翻译、图像修复和视频预测等计算机视觉领域。具体来说，生成器G从给定噪声z中产生合成数据$G(z)$，判别器D区分真实数据x和合成数据$G(z)$。前者试图产生更接近真实的数据，后者则试图更准确地分辨真假数据。两者在相互对抗中得到优化，在优化后继续进行对抗，使得生成器G的合成数据愈加准确，不断逼近真实的数据分布。假设P_{data}代表真实数据分布，P_z代表给定噪声x的先验分布，

它的损失函数如公式(4-1)所示。

$$\min_{G}\max_{D} V(D,G) = E_{x\sim P_{data}(x)}[\log D(x)] + E_{z\sim P_z(z)}[\log(1 - D(G(z)))] \tag{4-1}$$

其中，$\log D(x)$表示判别器对真实数据的判断，而$\log(1-D(G(z)))$表示判别器对合成数据的判断，在极大极小博弈中优化生成器和判别器，最终达到纳什均衡点，使得生成器以很高的准确度拟合真实数据。



(a) GAN　　(b) CGAN

图 4-1　生成对抗网络的模型结构

为了使生成对抗网络满足有条件的数据生成，在模型训练中引入条件信息y，形成了条件生成对抗网络 (Conditional Generative Adversarial Networks，CGAN)，如图4-1 (b)所示。生成器G拼接随机噪声z和条件信息y，以此为输入，输出合成数据$G(z \mid y)$。在条件信息y的约束下，判别器D区分真实数据x和合成数据$G(z \mid y)$，损失函数如公式(4-2)所示。其中，$\log D(x \mid y)$表示判别器对真实数据对(x, y)的判断，而$\log(1 - D(G(z \mid y)))$表示对合成数据对$(G(z \mid y), y)$的判断。

$$\min_{G}\max_{D} V(D,G) = E_{x\sim P_{data}(x)}[\log D(x \mid y)] + E_{z\sim P_z(z)}[\log(1 - D(G(z \mid y)))] \tag{4-2}$$

4.1.2　芯片电磁仿真

近些年，研究人员也将生成对抗网络应用到芯片设计领域，用于预测、评估和优化传统设计流程的各项子任务。Lu等人使用CGAN进行时钟树综合的结果预测，以触发器、时钟网络和试验布线为输入，输出时钟树功耗、线长和最大偏差等指标[111]。Alawieh等人将布局方案和信号连接作为输入图像，通过CGAN进行布线拥堵预测[112]。Chhabria等人提取功耗分布和电源密度的潜在特征，采用

编码器-解码器进行热分析和电压降预测 [113]。Zhou等人以行列电阻、电流分布和老化时间为输入特征，借助CGAN预测了电迁移引起的电压降 [114]。得益于生成对抗网络的强大性能，上述方法取代了一系列偏微分方程的求解过程，大幅提升了各项子任务的实现效率，并取得了接近传统仿真工具的预测结果。

与热分析和电压降分析类似，芯片电磁仿真也需要求解复杂的数学物理方程组，输入由逻辑单元和金属互连构成的物理版图，输出随时间和空间变化的电磁信息，两者都具有二维图像的表征形式。因此，基于EMSim提供的输入-输出样本对，芯片电磁仿真可转换为图像翻译问题，由生成对抗网络加速大批量的数据预测。图像翻译本质上是空间转换问题，假设X和Y分别代表原始空间和目标空间，x和y分别为符合两种空间特征的图像，图像翻译的目的是训练空间转换函数f，将原始空间的图像x转换到目标空间Y，并使得转换后的图像$f(x)$具备空间Y的特征。如果原始空间和目标空间的图像构成双射，则属于配对的图像翻译问题，Pix2Pix是解决该问题的经典模型。

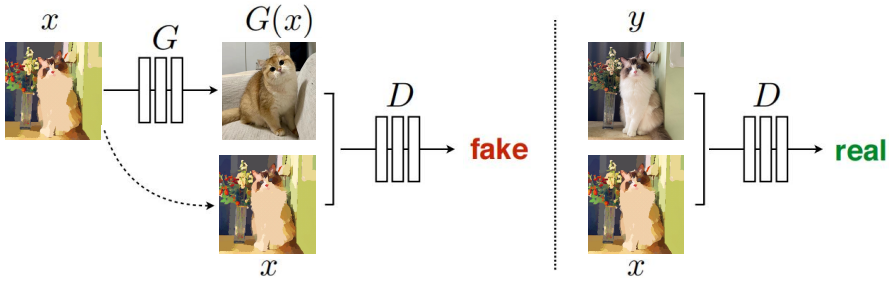


图 4-2　Pix2Pix的模型结构 [115]

Pix2Pix模型提供了统一的图像翻译框架，其整体结构以CGAN模型为基础，不同的是生成器的输入没有噪声信息 [115]。如图4-2所示，生成器G以条件信息x为输入并输出合成数据$G(x)$，在条件信息y的约束下，判别器D区分真实数据y和合成数据$G(x)$。Pix2Pix模型采用U-net结构作为生成器，由一系列卷积层、池化层、反卷积层构成。其中编码器利用最大池化层进行下采样，提取原始图像的高层特征并捕捉上下文信息，而解码器利用上采样恢复低层特征信息。编码器和解码器之间采用跳跃连接，在上采样时加入底层的特征信息，达到了输入输出之间信息共享的效果，避免了下采样过程中重要信息丢失的问题。

4.2　测评优化方法

本节介绍基于生成对抗网络的测评优化方法，包括数据准备、模型训练和风险量化三个环节。在数据准备环节，以单元电流和电源网格为输入，以空间磁场为输出，提取模型训练所需的少量输入输出样本对，根据测评量需求构建

风险量化的输入样本。在模型训练环节，通过生成器和判别器的对抗训练，进行生成对抗网络的模型优化，不断提升生成器的预测能力，使得合成数据接近真实磁场分布。在风险量化环节，使用训练好的生成器合成磁场数据，结合安全评估方法量化芯片安全性。

4.2.1 数据准备环节

对于集成电路而言，逻辑单元的瞬态电流充当激励源，金属互连网络的金属线是辐射载体，将内部信息以电磁波传递给外界环境。考虑到电流聚合效应和金属屏蔽效应，空间磁场的主导因素包括两方面：逻辑单元的瞬态电流和顶层电源网格的阻抗特性，两者均来自于物理版图的数据库。本节将前者表示为随时间变化的单元电流分布，将后者表示为电源网格分布，将空间磁场表示为随时间变化的磁场分布。以尺寸为$w \times h$的密码芯片为例，将其划分为$m \times n$的网格矩阵，每个格点均是边长为l的正方形，即$m = w/l$和$n = h/l$。

为了描述随时间变化的单元电流激励，提取每个逻辑单元的位置坐标和瞬态电流I_i，其中$i = 1, 2, ..., n$，N为该芯片的逻辑单元总数。图4-3为构建单元电流分布的示意图，蓝色矩形为边长l的矩阵网格，灰色矩形代表携带瞬态电流的逻辑单元。假定格点内电流均匀分布，每个格点的等效电流等于内部所有逻辑单元的电流总和，当某个逻辑单元覆盖多个格点时，则认为它只对最左边的格点有贡献。因此，左边格点的等效电流为$I_1 + I_4 + I_6$，中间格点的等效电流为$I_2 + I_3 + I_5 + I_7$，而右边格点的等效电流为I_8。遍历所有逻辑单元的位置坐标，将瞬态电流添加到对应的格点，能够得到$m \times n \times t$的单元电流分布，t为时间序列的长度。

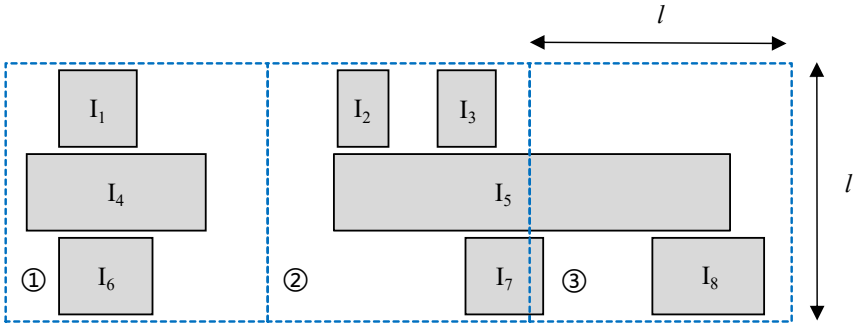


图 4-3 单元电流分布的示意图

为了刻画顶层电源网格的阻抗特性，需提取供电端口以及各金属线的位置坐标。由于物理版图具有规则的电源布线，电源环形和电源条线遵循水平和垂直方向排布，单个供电路径的等效电阻可用曼哈顿距离表示，如公式(4-3)所示。其中(x_1, y_1)为金属线所处格点的中心坐标，而(x_2, y_2)表示供电端口的中心坐标。

对于网格矩阵的某个格点，若格点内存在金属布线，其等效阻抗d_e为当前格点到N个供电端口的距离函数，如公式(4-4)所示，常数项C用来避免分母为零的异常情况。遍历所有格点形成了$m \times n \times 1$的电源网格分布，描述了物理版图的阻抗特性，并直观显示了电源网格密度。

$$d = |x_1 - x_2| + |y_1 - y_2| \tag{4-3}$$

$$d_e^{-1} = d_1 + d_2 + ... + d_N + C \tag{4-4}$$

对于指定高度和时间范围的磁场分布数据，可由EMSim依据3.2节的仿真流程获得，该数据用作模型训练的输出样本。本节采用离差标准化方法，将上述数据归一化到[0, 1]的范围，再输入到生成器和判别器，消除数据量纲和数量级影响，提升模型的收敛速度和精度。归一化的转换函数如公式(4-5)所示，其中$max(x)$和$min(x)$分别是样本数据的极大和极小值。

$$x' = \frac{x - min(x)}{max(x) - min(x)} \tag{4-5}$$

4.2.2 模型训练环节

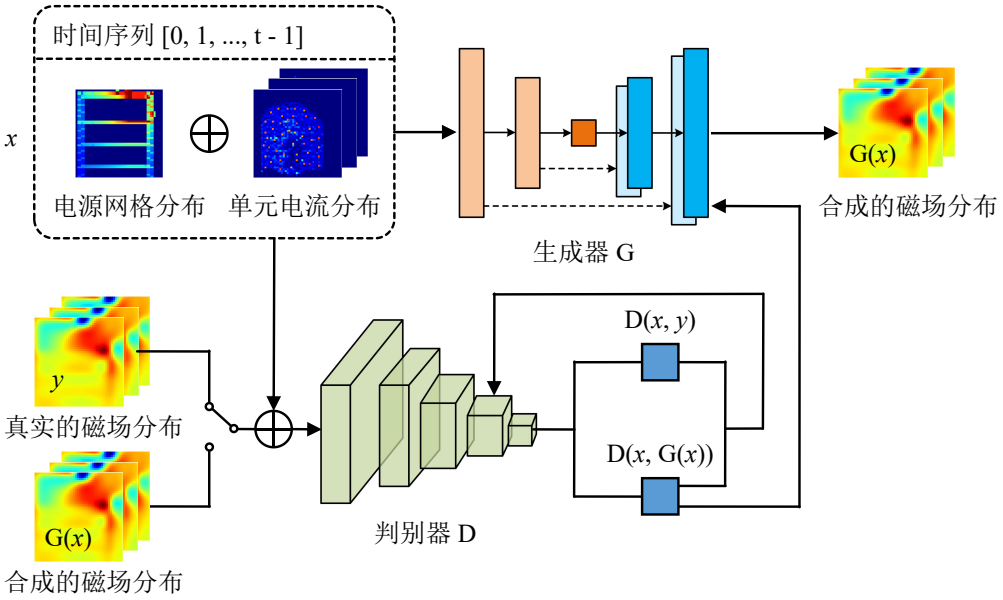


图 4-4 生成对抗网络的模型结构

根据EMSim提供的输入输出样本对，芯片电磁仿真被转换为图像翻译问题。为了求解该问题，本节设计了图4-4所示的生成对抗网络模型。生成器G的输入x包括图像数据和时间数据两部分，图像数据为单元电流分布和电源网格分布的拼接，时间数据为时间序列$\tau = 0, 1, ..., t - 1$，其中t为时间采样点的数目。对于上述输入，生成器通过编码器的下采样提取图像特征，与全连接层

提取的时间特征相融合，再由解码器进行上采样恢复时变图像信息，即合成的磁场分布$G(x)$。无论是合成的磁场分布$G(x)$还是真实的磁场分布y，连同生成器G的输入x一起，都被交替式地输入到判别器D，判别器将输出判定结果为$D(G(x), x)$或$D(y, x)$。在循环迭代的对抗训练中，判别器的反馈结果促使生成器进行优化，同时不断增强自身的判别能力，当生成器和判别器达到平衡状态，合成磁场分布和真实磁场分布趋于相同。在风险量化阶段，对于规定数据量的输入x，训练好的生成器可以快速合成磁场分布$G(x)$。下面考虑$m = 48$、$n = 48$和$t = 20$的情况，具体介绍生成器结构、判别器结构以及模型训练算法。

4.2.2.1 生成器结构

在生成器的输入数据中，既有描述单元电流和电源网格的二维图像，也有表示时间的一维序列。本节采用图4-5所示的生成器结构，使用编码器捕获二维图像的高层特征，采用全连接层融合时间特征和空间特征，由解码器恢复瞬态磁场分布的低层表征，在编码器和解码器之间添加跳跃连接，保留输入信息对输出信息的细节贡献。

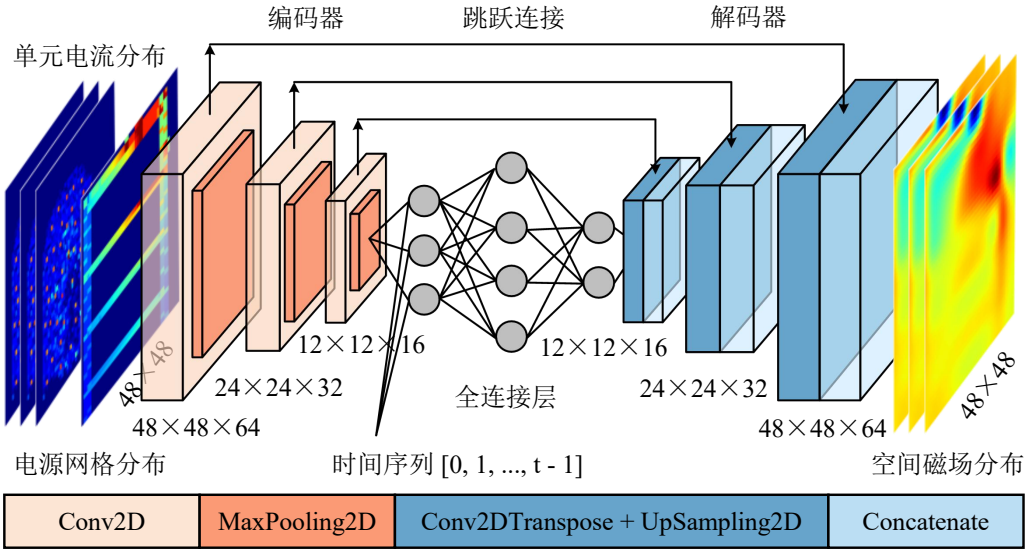


图 4-5 生成器结构

本节设计了由相邻卷积层和最大池化层构成的编码器，其结构如表4-1所示。表格从上到下列出了各个网络层结构，其中卷积层采用Conv2D结构，最大池化层采用MaxPolling2D结构。输入通道为到达该层的输入特征数量，而输出通道代表经过该层后得到的输出特征大小。除此之外，表格还列出卷积层和池化层采用的核尺寸，以及卷积层后使用的激活函数。卷积层在滑动窗口上进行卷积运算，提取到二维图像的局部特征，选择修正线性单元 (Rectified Linear Unit，ReLU) 作为激活函数处理卷积结果。最大池化层选取滑动窗口上的最大值，将

卷积层提取的特征维度缩减到原来的一半。如图4-5所示，经过多次图像卷积和最大池化运算，编码器完成下采样操作，根据输入图像推断出磁场分布的全局信息。

表 4-1 编码器的结构参数

结构	输入通道	输出通道	核尺寸	激活函数
Conv2D	2	64	3×3	ReLU
MaxPolling2D	-	-	2×2	-
Conv2D	64	32	3×3	ReLU
MaxPolling2D	-	-	2×2	-
Conv2D	32	16	5×5	ReLU
MaxPolling2D	-	-	2×2	-

在预测瞬时变化的磁场数据时，输入的单元电流和电源网格逐帧传入网络，对应生成一帧一帧的空间电磁。为此本节设计了全连接层结构，将编码器提取的图像特征扁平化后，与输入的一维时间特征进一步融合。之后由解码器恢复下采样期间丢失的位置信息，其结构由反卷积层和上采样层实现，分别采用Conv2DTranspose结构和UpSampling2D结构，详细参数如表4-2所示。上采样层在功能上与池化层相反，通过行列方向的数据插值来增加矩阵维度。由于生成器的输出结果与输入数据高度相关，在编码器和解码器之间添加跳跃连接，允许输入特征直接穿梭到更接近输出的网络层，将全局信息、时间信息和位置信息相结合，有利于更准确地描述空间磁场分布，同时避免梯度消失和梯度退化现象的发生。

表 4-2 解码器的结构参数

结构	输入通道	输出通道	核尺寸	激活函数
Conv2DTranspose	16	16	7×7	ReLU
UpSampling2D	-	-	2×2	-
Conv2DTranspose	32	32	7×7	ReLU
UpSampling2D	-	-	2×2	-
Conv2DTranspose	64	64	3×3	ReLU
UpSampling2D	-	-	2×2	-
Conv2DTranspose	128	1	3×3	ReLU

4.2.2.2 判别器结构

判别器具有图像分类的作用，它以单元电流分布、电源网格分布和时间序列为条件，判断输入的磁场分布是否真实。本节采用类似编码器的结构提取输入特征，利用全连接层进一步融合时间信息，通过PatchGAN结构实现图像分类器的功能。PatchGAN将输入图像转化为感受野矩阵，每个元素对应特定图像区域的真假概率，最终将矩阵均值作为判别器的输出结果。这样判别器能够充分考虑图像的局部细节，从而拥有较强的判别能力，其反馈结果有助于生成器的优化，使其准确预测输入数据的空间磁场。

4.2.2.3 训练算法流程

Algorithm 6 模型训练算法

Input:

数据集的输入输出样本对

初始化生成器G和判别器D参数

Output: 训练好的生成器G和判别器D

while 模型没有收敛 **do**

  for k次迭代 **do**

    从数据集中采样m个输入图像和时间样本$\{x_1, ..., x_m\}$

    从数据集中采样m个真实的磁场分布样本$\{y_1, ..., y_m\}$

    使用梯度上升法更新判别器参数：

    $\nabla_{\theta_D} \frac{1}{m} \sum_{i=1}^{m} [logD(x_i, y_i) + log(1 - D(x_i, G(x_i)))]$

  end for

  从数据集采样m个输入图像和时间样本$\{x_1, ..., x_m\}$

  使用梯度下降法更新生成器参数：

  $\nabla_{\theta_G} \frac{1}{m} \sum_{i=1}^{m} log(1 - D(x_i, G(x_i)))$

end while

模型训练过程如算法6所示，生成器G和判别器D进行对抗式训练。本节采用Adam优化方法训练模型，学习率遵循指数衰减规律，随着迭代次数的增加逐步减小学习率，使模型在训练后期更加稳定。在每次迭代训练中，采用回归损失作为被优化的目标函数。其中，判别器采用均方误差 (Mean Squared Error，MSE) 作为损失函数，得到预测值$\hat{y}$和真实值y间距离的平方和，计算过程如公式(4-6)所示。生成器采用平均绝对误差 (Mean Absolute Error，MAE) 作为损失函数，得到预测值$\hat{y}$和真实值y的绝对差值之和，计算过程如公式(4-7)所示。同时，使用准

确率为判别器效果的评估指标，实时记录判别结果正确与否的频率。在每次迭代结束后，采用MSE、MAE和平均绝对百分比误差 (Mean Absolute Percentage Error，MAPE) 对当前模型进行性能评估。其中，MAPE用于计算真实值与预测值的误差百分比，如公式(4-8)所示，目的是避免数据范围大小的影响。

$$\mathrm{MSE} = \frac{1}{m}\sum_{i=1}^{m}(\hat{y} - y)^2 \tag{4-6}$$

$$\mathrm{MAE} = \frac{1}{m}\sum_{i=1}^{m}|\hat{y} - y| \tag{4-7}$$

$$\mathrm{MAPE} = \frac{100\%}{m}\sum_{i=1}^{m}\left|\frac{\hat{y} - y}{y}\right| \tag{4-8}$$

4.2.3 风险量化环节

如算法7所示，根据测试集的输入样本，使用训练好的生成器合成磁场数据，结合安全评估方法统计信息泄露风险。具体来说，根据安全测评的数据规模，从测试集范围内选择n个输入样本$X = \{x_1, ..., x_n\}$，包括单元电流、电源网格和时间序列，生成器合成与输入样本对应的磁场分布$Y = \{y_1, ..., y_n\}$。采用离差标准化处理磁场分布样本，将合成磁场数据归一化到[0, 1]的范围，这方便添加指定水平的高斯噪声，从而模拟芯片安全测评的真实环境。对于网格矩阵的所有格点，选择CEMA攻击进行局部电磁分析，计算正确密钥与泄露模型的最大相关性，得到随位置变化的信息泄露风险，辅助进行密码芯片的安全性判定。

Algorithm 7 风险量化算法

Input:

数据集的输入样本

训练好的生成器

Output: 密码芯片的信息泄露风险

从数据集采样n个输入图像和时间样本$X = \{x_1, ..., x_n\}$

使用生成器合成n个磁场分布样本$Y = \{y_1, ..., y_n\}$

采用离差标准化方法处理磁场分布样本

for k个矩阵格点 **do**

    根据信息泄露模型开展电磁分析攻击

    计算猜测密钥对应的皮尔逊相关性系数

end for

判定密码芯片是否存在信息泄露风险

4.3 多种密码电路的效果验证

本节根据AES和Kyber算法分别设计了DUT-1和DUT-2电路，对照传统测评方法，分析了测评优化方法的有效性。

4.3.1 实验电路设计

DUT-1用于实现AES算法的加密功能，输入的明文和密钥长度为128位，采用与3.5.1节相同的电路结构。DUT-2用于实现Kyber算法的解密功能，输入的私钥和密文长度为24位。DUT-2使用移位寄存器实现Encode和Decode函数，采用两组蝶形运算模块实现Compress、Decompress、NTT、逆NTT和PWM等函数。蝶形运算模块具有两个输入对和输出对，通过控制信号sel调节上述函数的运行顺序，部分结构如图4-6所示。其中，tw_l和tw_h信号来自私钥$\hat{\mathbf{s}}$，in_2和in_3来自多项式向量$\hat{\mathbf{u}}$，逐点乘法由两个乘法器并行计算，随后对乘积$prod_0$和$prod_1$进行模约减。选用SMIC 180nm CMOS工艺进行逻辑综合和物理实现，得到两种密码模块的物理版图。在不考虑I/O单元面积的情况下，DUT-1版图面积为1140mm × 840mm，包含14559个逻辑单元和733662个金属线，其中1424条金属线属于顶层电源布线。DUT-2版图面积为1160mm × 1160mm，包含14598个逻辑单元和858474个金属线，其中587条金属线属于顶层电源布线。除此之外，两种密码模块的时钟频率设置为25MHz，其供电电压均为1.8V。

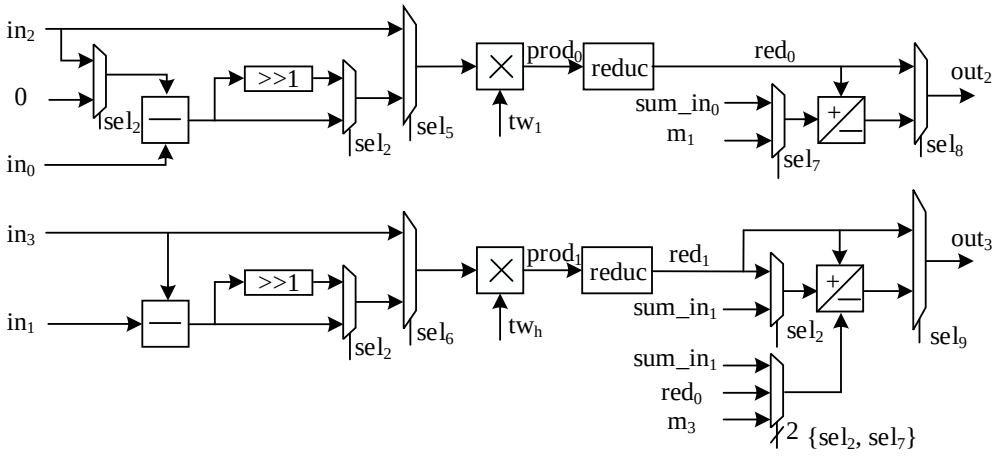
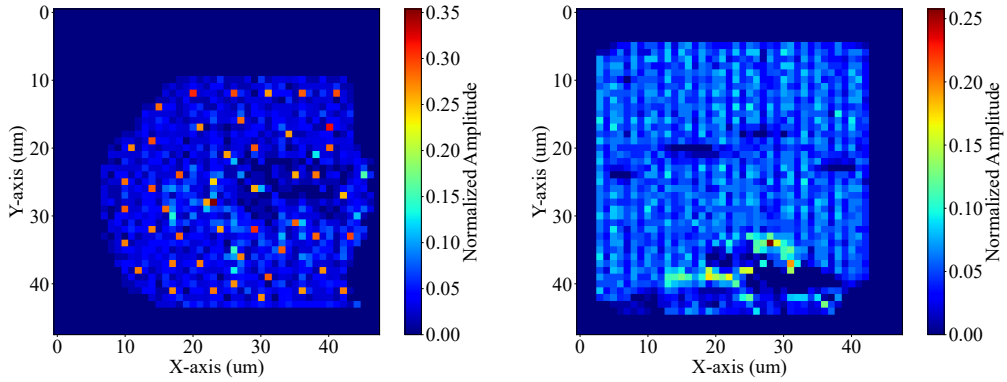


图 4-6 蝶形运算模块的部分结构 [116]

4.3.2 数据集和实验设置

为了实现测评优化方法，首先创建模型训练的数据集。根据1000组随机测试用例，使用EMSim仿真距芯片100μm的磁场平面，包含20个连续的时间采

样点，表示为48 × 48 × 20的输出样本。相应地，从版图数据库中提取输入样本，得到48 × 48 × 20的单元电流和48 × 48 × 1的电源网格，如图4-7和图4-8所示。通过以上操作，构建了1000组输入输出样本对，其中900组数据用作训练集，100组数据用作验证集。模型训练中的Epoch设置为100，Batch Size为64，采用Adam优化方法训练生成器和判别器，学习率遵循指数衰减规律，初始学习率为0.0005，衰减系数为0.98，经1000次迭代完成一次学习率衰减。具体流程如算法6所示，最终得到收敛状态的生成器和判别器。对DUT-1的生成器和判别器而言，在验证集的损失函数值为5.689×10^{-4}和0.2740。对DUT-2的生成器和判别器而言，在验证集的损失函数值为2.505×10^{-4}和0.3495。在这之后，根据另外的1000组随机激励，从版图数据库中提取单元电流和电源网格，作为风险量化的输入样本。按照算法7描述的流程，磁场数据由训练好的生成器合成，实现对DUT-1和DUT-2的信息泄露评估。在传统测评方法中，根据风险量化使用的测试用例，借助EMSim仿真指定高度的磁场数据，其他步骤与测评优化方法保持一致。这样，真实数据和合成数据共同组成了测试集，用于分析测评优化方法的准确性。

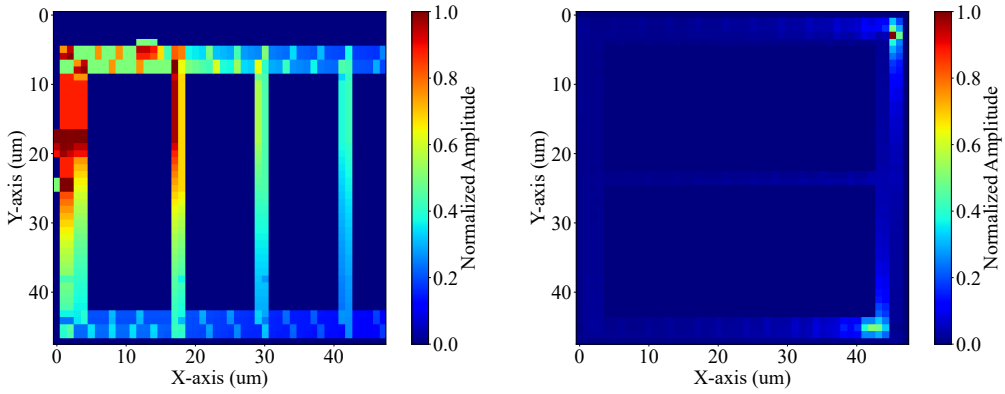


(a) DUT-1　　(b) DUT-2

图 4-7　不同电路的单元电流分布

4.3.3　实验结果分析

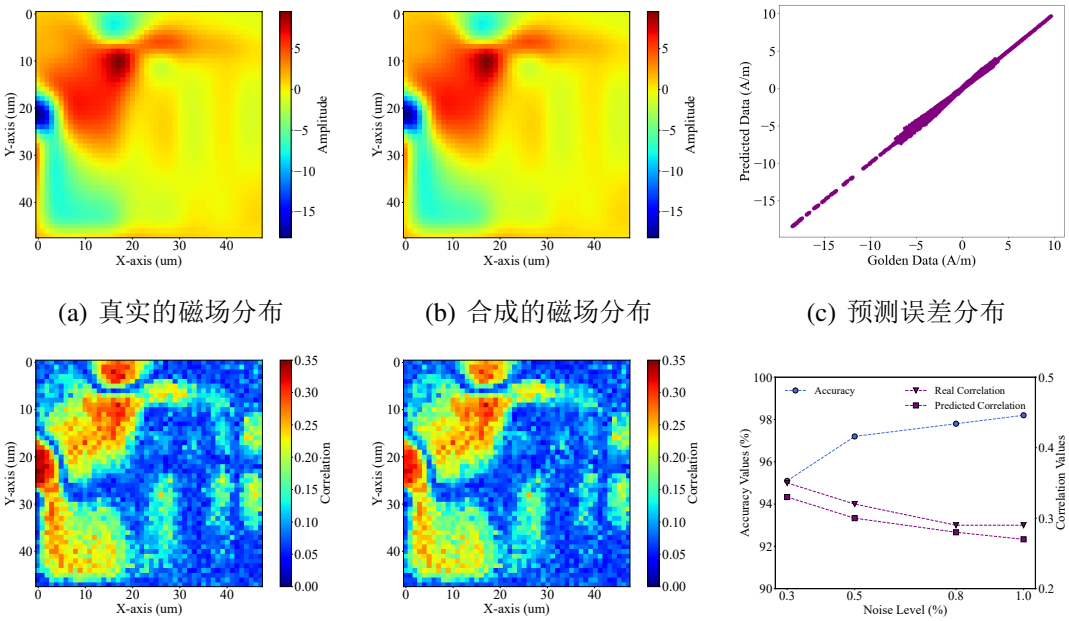
图4-9显示了DUT-1的空间磁场分布和信息泄露分布情况。在空间磁场分布方面，图4-9 (a)为EMSim仿真得到的参考样本，图4-9 (b)为生成器预测的磁场数据。对测试集的所有样本统计了SSIM平均值，可知预测磁场具有99.6%的空间准确度。对于网格矩阵所有格点的瞬态曲线，对照参考样本统计了NCC平均值，表明预测磁场具有99.2%的时域准确度。与此同时，图4-9 (c)分析了生成器的误差情况，其中横轴代表参考样本，纵轴代表预测数据，误差分布越接近线性关系 ($y = x$)，预测结果就越逼近参考样本。总体来说，磁场数据的极值差



(a) DUT-1　　(b) DUT-2

图 4-8　不同电路的电源网格分布

为28.43A/m，生成器的平均误差为0.019A/m，具有0.027A/m的标准差。在信息泄露分布方面，将字节替换操作的状态寄存器作为攻击点，利用汉明距离建立信息泄露模型，分别在0.3%、0.5%、0.8%和1%的噪声环境下，通过电磁分析度量了DUT-1的信息泄露风险，即正确密钥对应的相关性峰值。图4-9 (d)为真实的信息泄露分布，图4-9 (e)为生成器预测的信息泄露分布。SSIM指标的统计值表明两者具有95.1%的相似度，信息泄露热点位于相同的局部区域，该处的泄露风险值分别为0.35和0.33。进一步地，图4-9 (f)展示了其他噪声环境的测评误差，信息泄露分布的相似度高于97.2%，在信息泄露热点的差异值低于0.02。从而证明了测评优化方法的准确性。

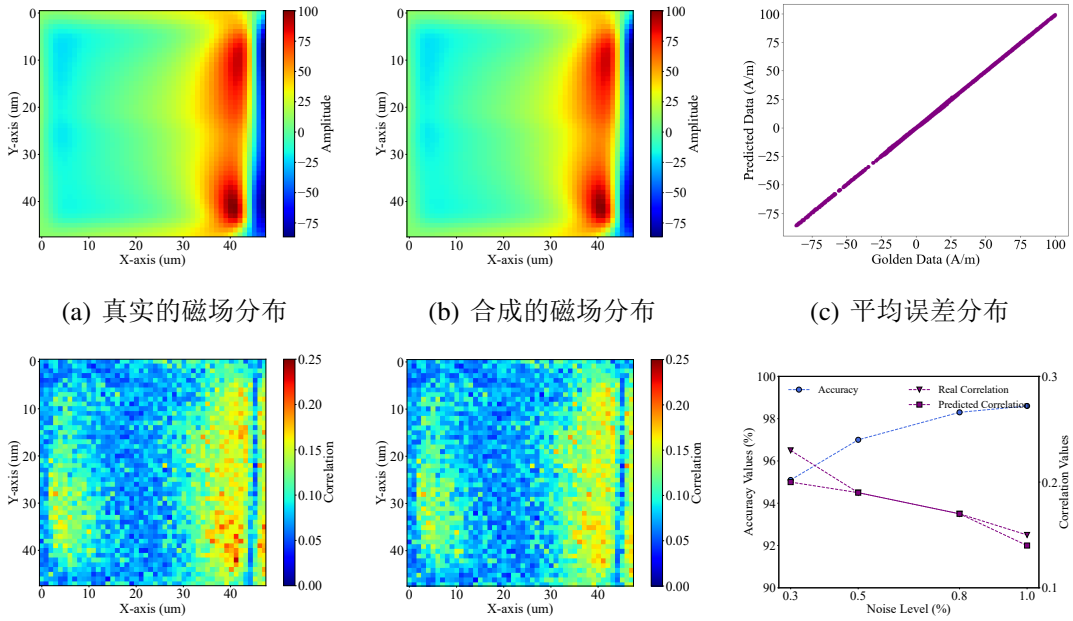


(a) 真实的磁场分布　　(b) 合成的磁场分布　　(c) 预测误差分布

(d) 真实的测评结果　　(e) 合成的测评结果　　(f) 测评误差分布

图 4-9　DUT-1的空间磁场和信息泄露图

图4-10显示了DUT-2的空间磁场分布和信息泄露分布情况。在空间磁场分布方面，图4-10 (a)为EMSim仿真得到的参考样本，图4-10 (b)为生成器的预测结果，磁场数据的极值差为186.69A/m。计算SSIM指标和NCC指标可知，预测结果的空间准确度为99.3%，其时域准确度达99.5%。图4-10 (c)展示了生成器的误差情况，参考样本和预测数据呈线性分布，平均误差为0.048A/m，具有0.076A/m的离散程度。在信息泄露分布方面，选择逐点乘法的输出结果为攻击点，计算汉明距离值作为信息泄露模型，通过电磁分析量化了DUT-2的信息泄露风险。噪声水平0.3%的测评结果如图4-10 (d)和图4-10 (e)所示，两种信息泄露分布具有95.2%的相似度，信息泄露热点都位于左右两侧，右侧泄露风险的极大值为0.23和0.20。与此同时，图4-10 (f)为其他噪声环境的测评误差，信息泄露分布的相似度高于97.0%，在信息泄露热点的差异值低于0.01，从而证明了测评优化的准确性。



(a) 真实的磁场分布　(b) 合成的磁场分布　(c) 平均误差分布

(d) 真实的测评结果　(e) 合成的测评结果　(f) 测评误差分布

图 4-10　DUT-2的空间磁场和信息泄露图

除此之外，本节还分析了不同规模数据集的影响，在模型训练的1000组数据集中，随机保留250组、500组和750组数据样本，而保持其他实验设置不变，重复测评优化方法的上述环节。表4-3给出了DUT-1电路的验证结果，实验结果表明，随着数据集规模的增加，生成器在验证集的损失函数值逐渐降低，随之减少的还有合成数据的误差均值。由于生成器性能的增强，预测磁场的固有精度和测评准确度也不断提高。数据集规模为500组时，训练后的测评准确度为91.6%，其后增速逐渐放缓。

表 4-3　数据集规模的影响分析

数据集规模	损失函数	误差均值	时域准确度	空间准确度	测评准确度
250	0.0017	0.052	0.958	0.992	0.886
500	0.0010	0.030	0.983	0.995	0.916
750	6.64×10^{-4}	0.022	0.991	0.996	0.947
1000	5.69×10^{-4}	0.019	0.992	0.996	0.951

4.4　对防护方案的测评结果

对于采用防护方案的密码芯片，例如掩码防护方案和物理防护策略，本节将分析测评优化方法的评估结果，展示其辅助安全漏洞检查的有益效果。

4.4.1　掩码防护方案

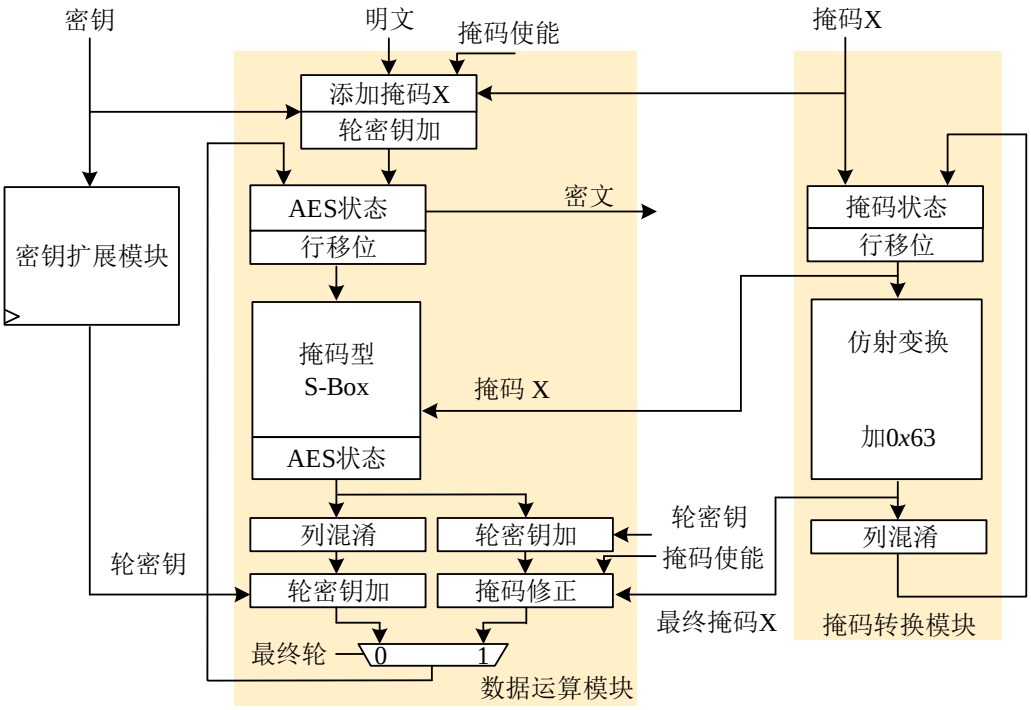


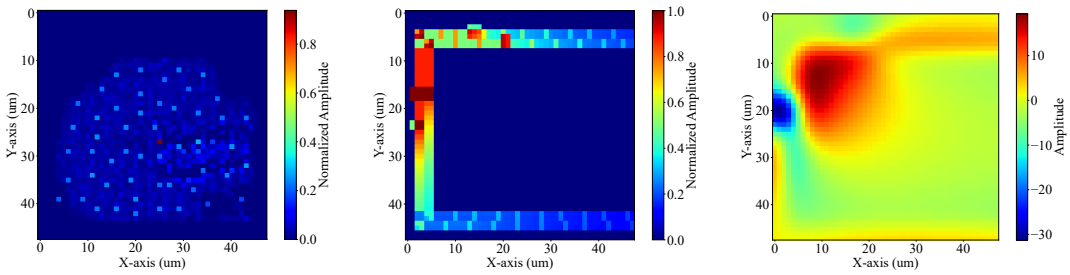
图 4-11　掩码型AES电路原理图

本节采用Oswald等人提出的经典掩码方案，设计掩码型电路AES-MA抵抗一阶侧信道攻击 [68]。如图4-11所示，AES-MA主要由密钥扩展模块、数据操作模块和掩码转换模块构成。密钥扩展模块计算每轮加密所需的轮密钥，数据操作模块实现AES算法的字节替换、行移位、列混淆和轮密钥加等操作。对于线性运算部分，掩码转换模块完成上一轮掩码的消除、下一轮掩码的添加以及最后

一轮的掩码修正。AES-MA电路具有32位的数据路径，存在4个掩码型S-Box模块，字节替换后的数据由状态寄存器存储。本节选用SMIC 180nm CMOS工艺库，在完成逻辑综合和物理实现后，AES-MA电路由10360个底层逻辑单元构成。电源网格位于M5和M6金属层内，包含878条电源环形和电源条线，电源轨线位于M1金属层内，将电源信号传递给底层逻辑单元。

4.4.1.1 数据集和实验设置

首先创建模型训练的数据集。使用EMSim仿真100μm高度的芯片磁场，选取首轮字节替换的时间段，将其表示成$48 \times 48 \times 20$的磁场输出样本。与此同时，从版图数据库中提取输入样本，得到$48 \times 48 \times 20$的单元电流和$48 \times 48 \times 1$的电源网格。通过以上操作，构建了1000组输入输出样本对，其中900组数据用作训练集，100组数据用作验证集。模型训练中的Epoch设置为100，Batch Size为64，采用Adam优化方法训练生成器和判别器，学习率遵循指数衰减规律，初始学习率为0.0005，衰减系数为0.98，经1000迭代后完成一次学习率衰减。具体流程如算法6所示，最终得到收敛状态的最优生成器和判别器，在验证集的损失函数值分别为5.018×10^{-4}和0.3132。其次，根据1万组随机明文激励，准备风险量化环节的输入样本，使用训练好的生成器合成磁场数据，图4-12 (a)和图4-12 (b)为单元电流分布和电源网格分布，而图4-12 (c)为合成的磁场分布。



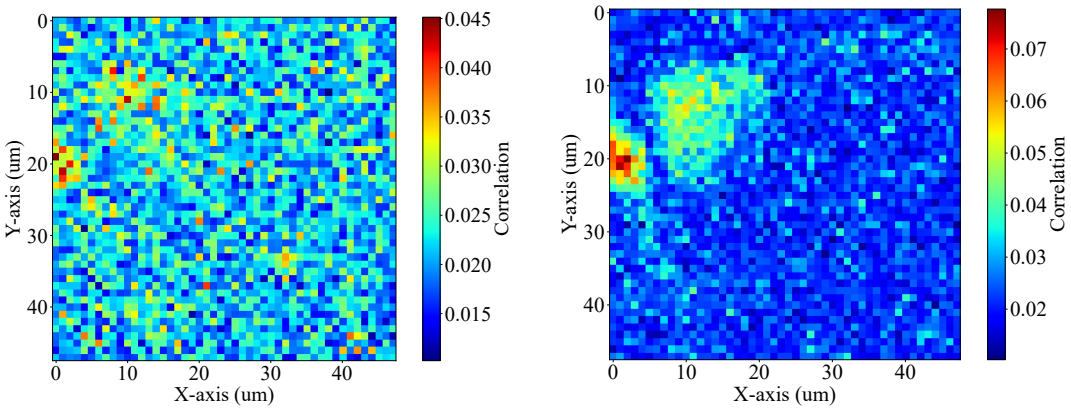
(a) 单元电流分布　(b) 电源网格分布　(c) 合成的磁场分布

图 4-12　AES-MA电路的预测结果

4.4.1.2 实验结果分析

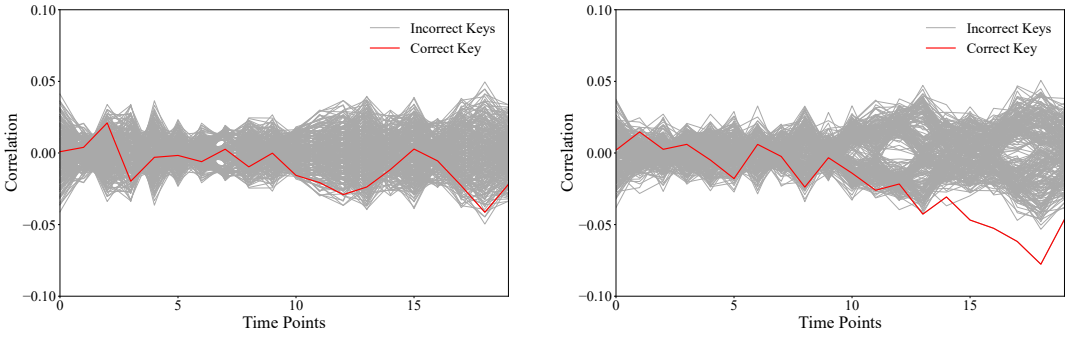
本节借助局部电磁分析开展硅前安全测评，分别采用汉明重量模型和翻转计数模型，研究经典掩码方案的一阶安全性，并分析它潜在的安全漏洞。作为比较，首先验证AES-MA抵抗传统攻击的能力，以掩码型S-Box模块的状态寄存器为目标，构建汉明重量矩阵作为信息泄露模型，遍历网格矩阵的所有格点开展电磁分析，得到图4-13 (a)所示的信息泄露分布图。在信息泄露热点处，猜测密钥对应的相关系数如图4-14 (a)所示，掩码X切断了寄存器状态与电磁信息的相

关性，导致正确密钥被隐藏在众多错误密钥中。其后，以掩码型S-Box模块内部逻辑门为目标，构建翻转计数矩阵作为泄露模型，来研究毛刺现象对AES-MA电路安全性的影响。对于不同的数据输入，翻转计数模型统计掩码型S-Box内部逻辑信号的平均翻转次数。对掩码型电路进行局部电磁分析，得到图4-13 (b)所示的信息泄露分布图。同样地，分析信息泄露热点处所有密钥的相关性曲线，如图4-14 (b)所示，正确密钥的相关性峰值远远大于其他错误密钥，即攻击者可以在1万条曲线内恢复主密钥。



(a) 汉明权重模型　　(b) 翻转计数模型

图 4-13　两种攻击场景的信息泄露图



(a) 汉明权重模型　　(b) 翻转计数模型

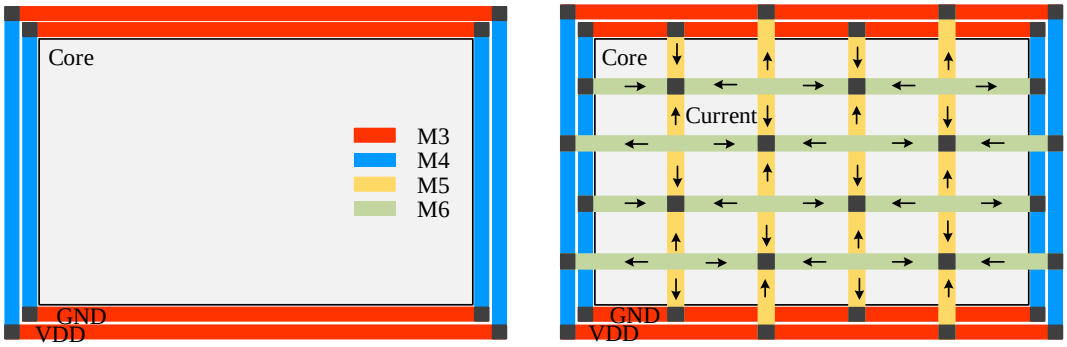
图 4-14　随曲线数目变化的相关性曲线

毛刺现象的安全性影响最早由Mangard等人发现，该漏洞使得密码中间值在某些时刻明文化 [72–74]。由上述实验结果可知，本节使用测评优化方法得到了相同结论。作为掩码型S-Box模块的非线性单元，掩码乘法器由普通乘法器和异或门组成，用于合并处理掩码和掩码型数据。通常来说，异或门的输出信号会根据输入信号的变化而改变。但是当输入信号出现毛刺时，其信号翻转将被异或门吸收，阻断了翻转信号的进一步传播。对于掩码型S-Box来说，不同数据输入

具有不同的路径延时，其内部异或门将吸收不同数目的信号翻转，从而导致不同特征的电磁信息，这也是该方案存在安全漏洞的本质原因。因此，测评优化方法能够正确评估防护方案，并且辅助设计人员诊断潜在的安全漏洞。

4.4.2 物理防护策略

电源网格的布局优化可以减弱敏感信息泄露，如电源网格扭转和电源网格屏蔽，这类物理防护策略得到了广泛关注和有效论证 [48, 49, 66]，本节使用安全测评优化方法，研究了电源条线对安全性的影响，得到了与上述工作相似的评估结果。在对128位AES电路进行逻辑综合后，采用不同的电源规划策略进行物理实现。AES-PG1电路为参考基准，M3和M4金属层用作电源网格，M1金属层用作电源轨线，如图4-15 (a)所示。在不考虑I/O单元面积的情况下，AES-PG1版图面积为1140mm × 840mm，包含14345个逻辑单元和637227条金属线，其中352条金属线属于顶层电源布线。在此基础上，AES-PG2电路在M5金属层内增加两组垂直的电源条线，在M6金属层内增加两组水平的电源条线。这些电源条线宽度为40μm，且在垂直和水平方向均匀分布，如图4-15 (b)所示。AES-PG2包含14338个逻辑单元和730470个金属线，其中1186条金属线属于顶层电源布线。供电电压和时钟频率分别设置为1.8V和25MHz。



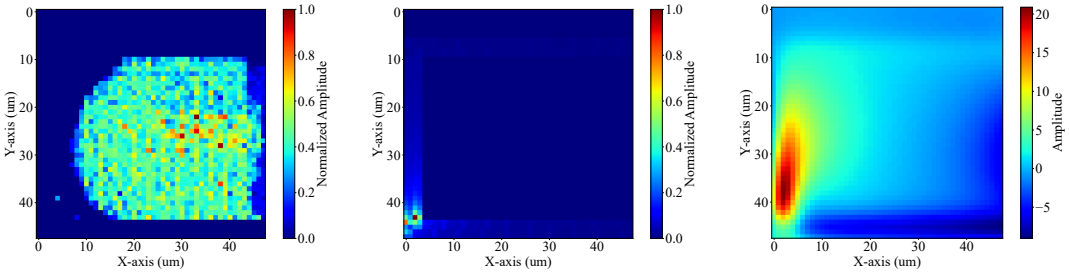
(a) AES-PG1　　(b) AES-PG2

图 4-15　两种不同类型的电源规划策略

4.4.2.1 数据集和实验设置

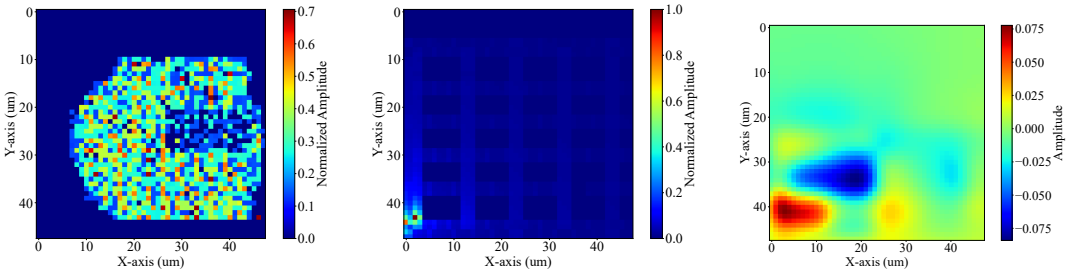
首先创建模型训练环节的数据集。使用EMSim仿真在100μm高度的磁场平面，将其表示成48 × 48 × 20的磁场输出样本。与此同时，从版图数据库中提取输入样本，得到48 × 48 × 20的单元电流和48 × 48 × 1的电源网格。通过以上操作，构建了模型训练使用的1000组配对数据集，其中900组数据用作训练集，100组数据用作验证集。其他实验设置与上节保持一致，具体流程如算法6所示，最终得到收敛状态的最优生成器和判别器。其中，AES-PG1的生成器在验证集

的损失值为1.4×10^{-3}，判别器的损失函数值为0.3752。AES-PG2的生成器在验证集的损失值为2.028×10^{-4}，判别器的损失函数值为0.2507。其次在风险量化环节，根据1万组随机明文的输入样本，使用训练好的生成器合成了磁场数据。图4-16为AES-PG1电路的预测结果，图4-17为AES-PG2电路的预测结果，包括单元电流分布、电源网格分布和合成的磁场分布。



(a) 单元电流分布　　(b) 电源网格分布　　(c) 合成的磁场分布

图 4-16　AES-PG1电路的预测结果

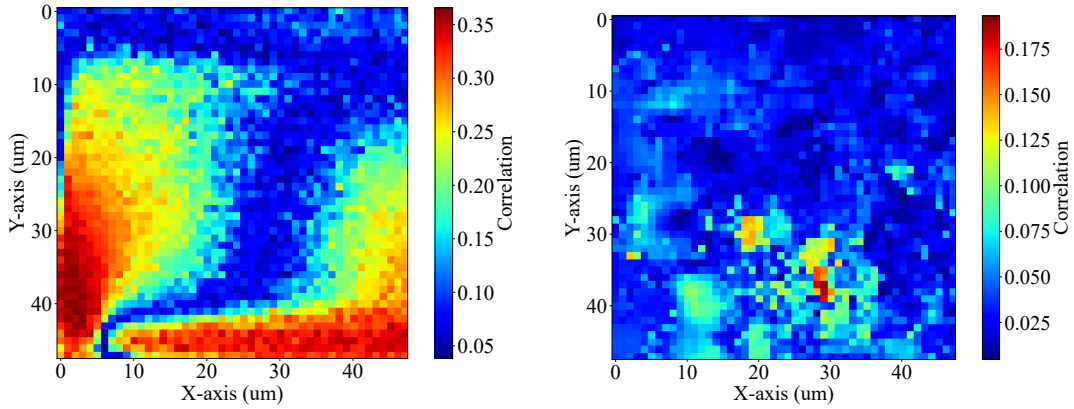


(a) 单元电流分布　　(b) 电源网格分布　　(c) 合成的磁场分布

图 4-17　AES-PG2电路的预测结果

4.4.2.2　实验结果分析

将首轮S-Box输出作为攻击目标，构建密码中间值的汉明距离矩阵，对所有格点进行电磁分析攻击，得到图4-18所示的信息泄露分布。图4-18 (a)中具有泄露风险的区域很多，在AES-PG1的信息泄露热点处，正确密钥对应的最大相关性为0.36。比较可知，图4-18 (b)中泄露风险已大幅降低，而且在AES-PG2的信息泄露热点，正确密钥对应的最大相关性降低到0.17。总体而言，AES-PG2电路具有更高的电磁安全抗性，这归因于以下两个原因。首先，电源条线的引入使电源网格更加稳健，从而衰减了顶层金属层内的瞬时电流。其次，如图4-15 (b)所示，电源条线流动有不同方向的瞬时电流，产生的电磁辐射一定程度地相互抵消。以上结果说明，使用本章提出的测评优化方法，可以辅助定制更加安全的物理防护策略。



(a) AES-PG1　　(b) AES-PG2

图 4-18　两种电路的信息泄露分布

4.5　测评效率分析

为了分析测评优化方法的时间效率，本节统计了上述四组实验的时间成本，单位为分钟/数据量。所有实验都运行在相同的硬件环境，其中CPU型号为Intel(R) Xeon(R) W-2235，GPU型号为NVIDIA GeForce RTX 3090。在测评优化方法中，数据准备和模型训练的时间b是固定成本，风险量化的时间a与数据量n有关，对于测评规定的数据规模N，总的时间成本遵循$Y = (a/x) \cdot N + b$的函数关系。在传统测评方法中，由EMSim仿真所有的磁场数据，其时间成本X随数据量线性增长，符合$X = b \cdot N$的函数关系。由表4-4可知，DUT-1电路由14559个逻辑单元构成，当安全测评需要1000条数据时，测评优化方法需要2344.8分钟，而传统测评方法需要2282分钟。在相同的测评条件下，对于14598个逻辑单元构成的DUT-2电路，传统测评方法需要1540分钟，测评优化方法需要1602.6分钟。当规定的数据规模为1万时，如分析AES-MA电路的安全性，传统测评方法需要10937分钟，测评优化方法只需1186.3分钟。在分析后两种密码电路时，相比于传统测评方法，测评优化方法也具有明显的优势。

表 4-4　安全测评的效率分析(分钟/数据量)

密码电路	单元数目	数据准备	模型训练	风险量化	优化方法	传统方法
DUT-1	14559	2282/1K	59.7/1K	3.1/1K	2344.8/1K	2282/1K
DUT-2	14598	1540/1K	58.8/1K	3.8/1K	1602.6/1K	1540/1K
AES-MA	10360	1093/1K	59.8/1K	33.5/1W	1186.3/1W	10937/1W
AES-PG1	14345	1613/1K	62.2/1K	33.0/1W	1708.2/1W	16130/1W
AES-PG2	14338	1934/1K	61.7/1K	37.4/1W	2033.1/1W	19340/1W

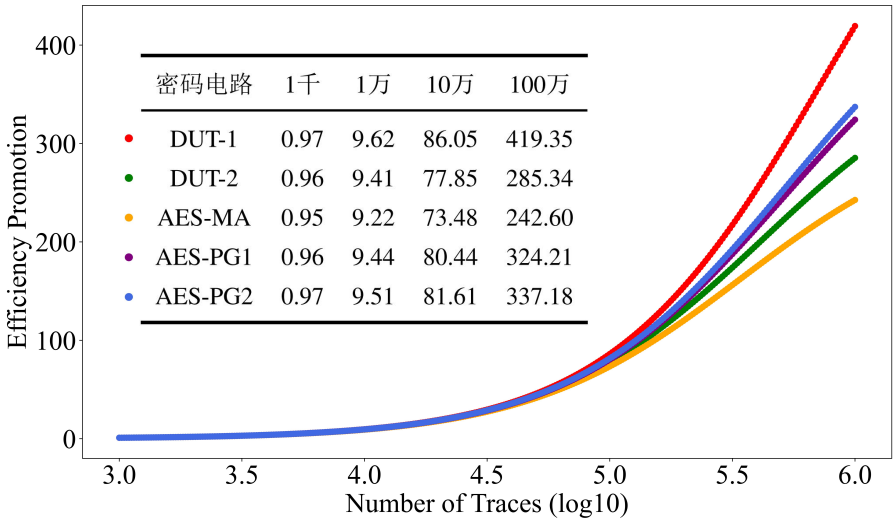


图 4-19　不同测评曲线数目的效率提升值

进一步地，对于不同的数据规模，本节计算了两种方法的时间比值Y/X，作为安全测评的效率提升值，如图4-19所示。因此，对小规模数据量的安全测评场景，两种方法的时间成本相差不多，可交给传统测评方法完成。在大规模数据量的测评场景中，测评优化方法具有更高的时间效率，而且测评所需的曲线数目越多，其效率优势越明显。参照ISO/IEC 17825-2016标准，安全等级三的测评数据量为1万条，此时效率提升值为9.22 ~ 9.62倍，安全等级四的测评数据量为10万条，测评效率提升了73.48 ~ 86.05倍。而对于100万条的测评数据量，测评的时间效率将提升242.60 ~ 419.35倍。

4.6　本章小结

针对大规模数据量的测评场景，本章研究了基于生成对抗网络的测评优化方法。在介绍生成对抗网络的相关原理后，重点讨论了测评优化方法的具体流程。在数据准备环节，通过EMSim仿真芯片表面的磁场数据，从物理版图提取单元电流和电源网格，创建了模型训练和风险量化的数据集。在模型训练环节，设计了生成对抗网络的模型结构，提出了进行对抗式训练的算法流程，充分学习了输入样本到输出样本的瞬态映射。在风险量化环节，使用训练好的生成器合成磁场数据，提出了开展安全测评的算法流程。最后，分析了测评优化方法在四组密码电路的有效性，该方法不仅能准确量化信息泄露分布，还大幅提升了安全测评的时间效率。参照ISO/IEC 17825-2016标准，对于安全等级3规定的1万条曲线，测评效率提升值高于9.22倍，对于安全等级4规定的10万条曲线，测评效率提升值高于73.48倍。

第 5 章　密码芯片安全溯源和靶向增强方法研究

随着芯片设计与制造水平的提升，安全防护方法的实现方式不断丰富。然而，除了显著地增加功耗、性能或面积开销，部分方法的硬件实现还需要全定制或半定制的电路模块。为了解决上述问题，本章开展了安全溯源和靶向增强方法研究，识别密码芯片敏感信息的泄露源，针对性地设计组合型防护方案，有效地权衡功耗、性能、面积和安全指标。首先提出了泄露路径识别技术，用于实现敏感信息的安全溯源，通过动态关联度分析定位具有高泄露风险的逻辑单元集合，其后利用静态安全性检验构建完整的泄露路径。在这个基础上，组合布尔掩码和随机预充电的优点，设计了局部路径掩码方案，提出了进行靶向增强的逻辑映射算法，实现电磁安全抗性的自动化提升。最终，根据上述技术设计了增强型AES电路，通过仿真和实测结果验证了侧信道安全性，分析了增强型AES电路的功耗、性能和面积开销。

5.1　泄露路径识别技术

所谓敏感信息的泄露路径，不仅是密码电路的数据通路，还会传递敏感变量引起的信息泄漏。从泄露路径的源单元开始，信息泄露将经过多级中间单元，直到泄露风险较低的无关路径。本节将分析泄露路径的识别过程，包括动态关联度分析和静态安全性检验。

5.1.1　动态关联度分析

动态关联度分析用来确定容易泄露敏感变量的逻辑单元。首先，通过敏感信息仿真刻画逻辑单元的侧信道行为，表示为电源电流或瞬态功耗，电源电流可由瞬态功耗除以电源电压获得，两者具有内在一致性。然后，通过泄露风险排序度量其对敏感变量的依赖程度，根据信息泄露阈值挑选高泄露风险的逻辑单元，如图5-1所示。这些逻辑单元的拓扑结构起点，通常为泄露路径的源单元，即携带着最多的敏感信息。所以在本节中，动态关联度分析只用来确定上述单元集合，完整的泄露路径由后续的静态安全性检验构建。

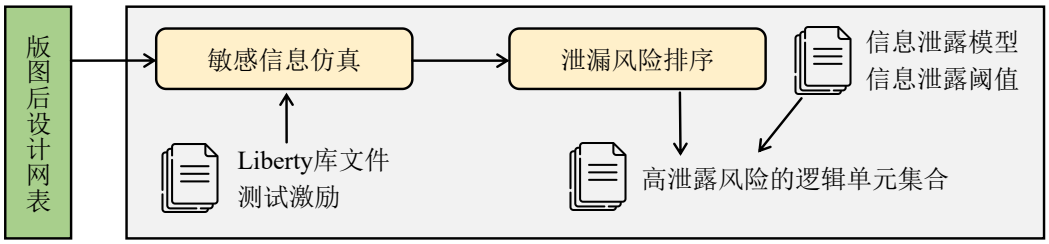


图 5-1　动态关联度分析示意图

5.1.1.1　敏感信息仿真

敏感信息仿真旨在获得电路运行期间逻辑单元的瞬态功耗，需要在仿真精度和所需资源间进行权衡。一般来讲，仿真精度越高，消耗的时间、内存以及产生的数据量就越多。模拟级仿真是最为准确的功耗建模方法，这种仿真将寄生参数标注到晶体管网表，联合电压源构成微分代数方程组，求解得到电路的节点电压和支路电流，最终准确度与寄生参数和器件模型密切相关。逻辑级仿真以牺牲部分精度为代价，减少了功耗建模所需要的资源数量。这种仿真以电路的门级网表为基础，反向注解逻辑单元和信号线网的延迟信息，通过动态门级仿真和单元功耗分析得到瞬态功耗。行为级仿真是最为快速的功耗建模方法，它基于集成电路的高层次代码，粗粒度地描述时钟周期内的平均功耗。

由上述分析可知，模拟级和逻辑级仿真是较为准确的建模方法，考虑了逻辑单元的输入状态和输出负载，能够充分刻画逻辑单元的瞬态功耗。为了提升敏感信息的仿真效率，本节选用基于门级网表的逻辑级仿真方法。与3.2.2节类似，首先利用仿真激励文件执行动态门级仿真，以Synopsys VCS工具为例，将SDF文件反向注解到版图后门级网表，在给定测试激励下记录逻辑单元的翻转活动。其后执行单元功耗分析，以Synopsys PrimeTime PX工具为例，选择瞬态仿真模式获得每个逻辑单元的实时功耗值。首先导入设计数据和工艺库信息，包括版图后门级网表、Liberty库文件、SDC文件、SPEF文件和VCD文件。将逻辑单元的翻转活动标定到版图后门级网表中，同时将SPEF文件的寄生参数注释到各单元及其线网。时序分析会针对每次信号翻转活动，计算并存储逻辑单元的输入翻转时间和输出负载。最终，以输入翻转时间和输出负载信息为索引，通过访问Liberty库文件的功耗查找表获得当前时刻的单元功耗值。

5.1.1.2　泄露风险排序

泄露风险排序旨在量化每个逻辑单元的信息泄漏，挑选出高泄露风险的逻辑单元集合。对于N个随机测试激励，敏感信息仿真已获得每个逻辑单元的瞬态功耗，表示为公式(5-1)，其中$i = 1, 2, ..., N$。将所有逻辑单元的瞬态功耗进行拼

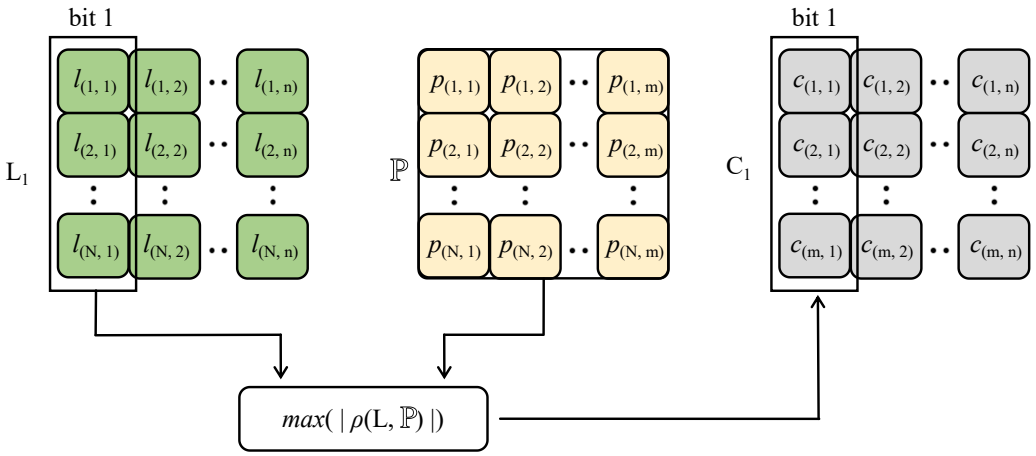


图 5-2 泄露风险排序示意图

接，得到门级网表的单元功耗矩阵$\mathbb{P}$，如公式(5-2)所示，其中||表示向量拼接操作，m表示逻辑单元的数量。

$$P = \{p_1,\ p_2,\ p_3,\ ...,\ p_i,\ ...,\ p_N\} \tag{5-1}$$

$$\mathbb{P} = \{P_1 \parallel P_2 \parallel P_3 \parallel ... \parallel P_m\} \tag{5-2}$$

信息泄露模型L是敏感变量v的函数，当应用到侧信道攻击时，能够揭示侧信道行为关联的敏感信息。而在安全溯源应用中，信息泄露模型可以辅助量化泄露风险，从而识别到需要保护的电路模块、逻辑单元或数据路径。特别地，设计者知晓密码芯片的实现细节，根据攻击场景可以构建正确的信息泄露模型。以AES算法的硬件实现为例，p和k分别为明文和密钥字节，S-Box模块的输出结果$v = S(p \oplus k)$，S为字节替换函数。密码中间值v是与密钥相关的敏感变量。对于敏感变量的每一位数据，计算N个随机测试激励的汉明距离，表示为公式5-3所示的信息泄露模型，其中$i = 1, 2, ..., N$。将所有比特的泄露矩阵进行向量拼接操作，如公式5-4所示，其中n表示敏感变量的位宽。

$$L = \{l_1,\ l_2,\ l_3,\ ...,\ l_i,\ ...,\ l_N\} \tag{5-3}$$

$$\mathbb{L} = \{L_1 \parallel L_2 \parallel L_3 \parallel ... \parallel L_n\} \tag{5-4}$$

如图5-2所示，遍历敏感变量所有比特的数据，计算信息泄露模型L和单元功耗矩阵$\mathbb{P}$的相关性$\rho(L, \mathbb{P})$，取相关性的最大值作为泄露风险C。根据构建的泄露风险矩阵，将门级网表的逻辑单元从高到低排序，对比预定义的信息泄露阈值，就能确定承载敏感信息最多的逻辑单元集合。

5.1.2 静态安全性检验

对于一条泄漏路径，敏感变量引起的信息泄漏将从源单元开始，经过多级中间单元直到无关单元。通常，源单元泄漏的信息最多。因此，具有高泄露风险逻辑单元集合中，存在着泄露路径的源单元，并且位于拓扑结构的前端。在本节中，使用拓扑结构分析从上述集合中定位源单元，借助泄露属性检验识别后续的中间单元，从而获得完整的泄漏路径，如图5-3所示。

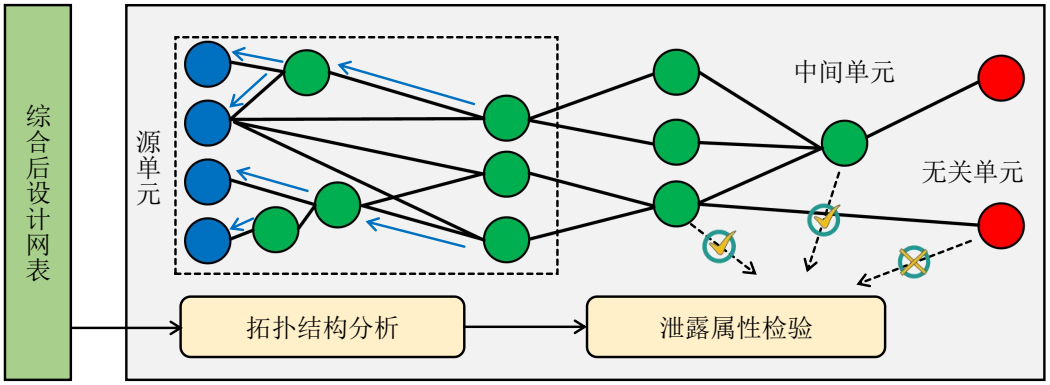


图 5-3 静态安全性检验示意图

5.1.2.1 拓扑结构分析

电路设计普遍采用层次化设计划分，将电路系统逐层分割成若干子模块。在逻辑综合和布局布线时，将默认保留各个模块的层次关系。因此，版图后门级网表由顶层模块和若干子模块构成。首先，以模块为单位拆分层次化的电路网表，通过正则匹配module和endmodule字符，提取出各个子模块的名称和内容，并表示为独立的模块文件。接下来，创建字典文件来描述每个子模块的内在拓扑结构。字典Cell记录了各个逻辑单元连接的输入信号和输出信号，字典Net记录了每个信号连接的驱动单元和负载单元。图5-4为TOP模块的原理图和门级网表，由非门、与非门、或非门和D触发器组成。以该模块为例，首先根据工艺库创建引用单元的输出引脚列表，如output_pin = [’Q’，’QN’，’Y’，’CO’，’S’]，以及模块TOP的时钟和复位信号列表，如clk_rst = [’clk’]。然后，以分号为换行符逐行读取模块网表的内容。针对图5-4的黄色区域，匹配字符串input、output和wire定位到模块所有信号，以信号名称为键值向字典Net添加驱动单元和负载单元的空列表。特别地，位宽大于1的信号需要拆成单比特信号处理，如e[1：0]信号分解为e[0]信号和e[1]信号。其后，针对图5-4的绿色区域，以单元名称为键值向字典Cell添加引用类型、输入信号和输出信号列表，由output_pin列表确定各引脚的输入和输出类型。同时，引脚类型也可以确认信号连接的前级

和后级单元，并将其填入字典Net的驱动单元和负载单元列表。最终，单元U3在字典Cell具有['NAND2X1'，['A'：'b'，'B'：'n2'，'Y'：'n3']]的形式，信号n3在字典Net具有[[['U3'，'B']], ['U2'，'Y']]的形式。

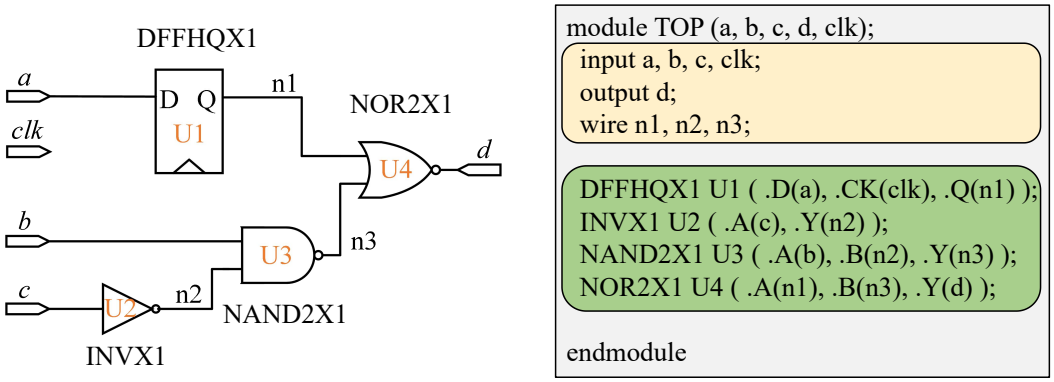
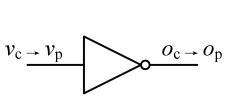


图 5-4　拓扑结构分析示意图

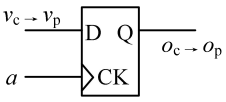
在字典Cell和字典Net的帮助下，可以快速推断出逻辑单元的驱动网络或负载网络。将高泄露风险的逻辑单元注解到综合后门级网表，在该集合范围内构建所有单元的驱动网络。由于源单元位于泄露路径的最前端，也是承载敏感信息最多的单元，处于上述集合的拓扑结构起点。因此，在驱动网络头部的逻辑单元即为泄露路径的源单元。敏感变量从源单元开始传播，产生与它们高度相关的侧信道行为。

5.1.2.2　泄露属性检验



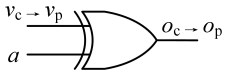
A	Y
0	1
1	0

(a) INV



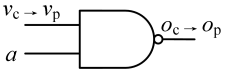
D	CK	Q[n+1]
0	↑	0
1	↑	1
x	↓	Q[n]

(b) DFF



A	B	Y
0	0	0
0	1	1
1	0	1
1	1	0

(c) XOR



A	B	Y
0	x	1
x	0	1
1	1	0

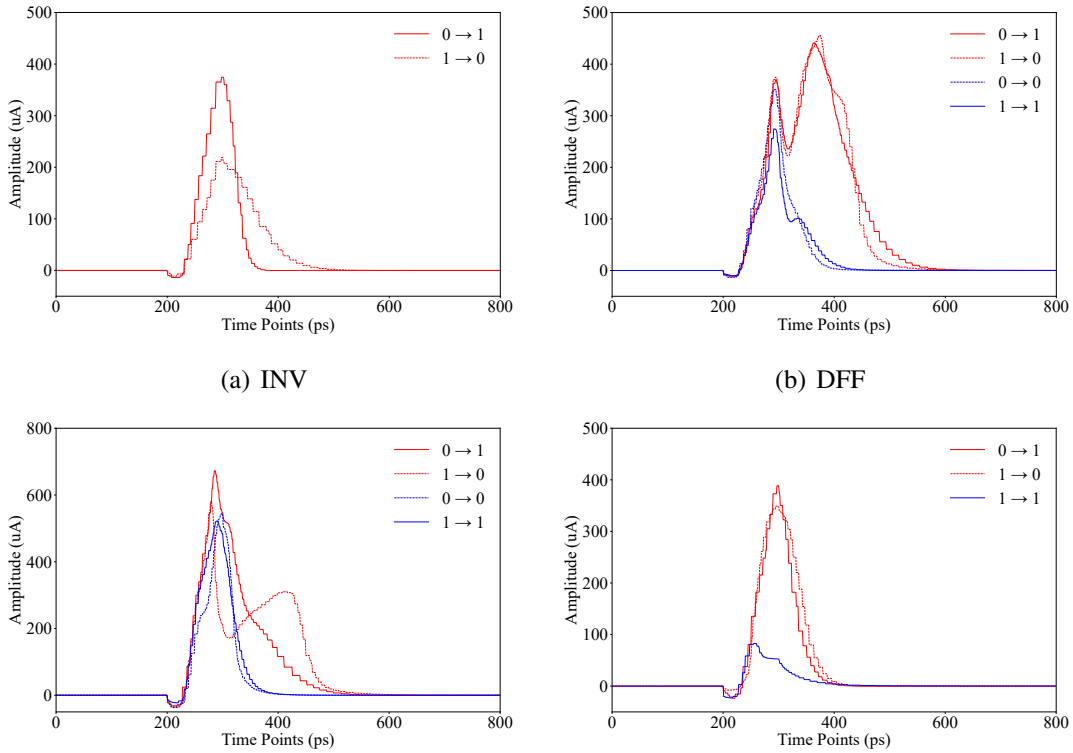
(d) NAND

图 5-5　不同逻辑单元的逻辑符号和真值表

从源单元开始，后续的泄漏路径由泄露属性检验来构造。所谓的泄露属性检验，是检查逻辑单元是否继承了敏感变量的侧信道行为。对待测逻辑单元而言，它的输入为源单元或中间单元的敏感变量v_c，由真值表对应的逻辑函数决定输出o_c。当敏感变量从v_c变化到v_p时，逻辑单元的输出状态将从o_c变化到o_p。状态翻转$v_c \rightarrow v_p$和$o_c \rightarrow o_p$分别决定了驱动单元和该单元的侧信道行为。本节以非门、D触发器、异或门和与非门为例，具体分析逻辑单元的泄露属性定义。图5-5 (a)为非门的逻辑符号和真值表，由逻辑函数$Y = \bar{A}$可知，引脚A的0 → 1(1 → 0)翻转导致引脚Y的1 → 0 (0 → 1)翻转。因此，尽管前级单元和非门的功耗幅度并非相同，它们具有相似的功耗分布方式，即非门能够继承来自敏感变量的侧信道行为。对于图5-5 (b)的D触发器，CK上升沿采样D引脚的数据并传递给输出Q引脚，此时D引脚和Q引脚具有相同的状态翻转，从而继承了来自敏感变量的侧信道行为。而对于多输入的逻辑单元，则需要考虑其他输入对输出状态的影响，如图5-5 (c)所示的异或门，由逻辑函数$Y = (A \cdot \bar{B}) + (\bar{A} \cdot B)$可知，保持引脚B状态不变，引脚A的0 → 1翻转导致引脚Y的1 → 0或0 → 1翻转。反之，引脚A的1 → 0翻转导致引脚Y的0 → 1或1 → 0翻转。因此，异或门和非门以及D触发器相同，也能继承来自敏感变量的侧信道行为。而对于图5-5 (d)的与非门，由逻辑函数$Y = \overline{(A \cdot B)}$可知，当B引脚状态为0时，输出Y引脚的状态总为1，而与引脚A的状态无关。因此，与非门有着与敏感变量不同的侧信道行为，不属于泄露路径的中间单元。公式(5-5)给出了上述泄露属性的定义式。

$$\forall(a_1, a_2, ...a_{n-1}), \left|O_c - O_p\right| = \left|v_c - v_p\right| \tag{5-5}$$

其中，$a_1, a_2, ..., a_{n-1}, v_c$代表逻辑单元的输入状态。如果某个逻辑单元属于泄漏路径，它应该具有与源单元或中间单元类似的功耗分布。图5-6为上述逻辑单元在不同状态翻转的瞬态电流，其分布趋势遵循输出引脚前后状态的汉明距离。以D触发器为例，状态翻转0 → 0和1 → 1的汉明距离为0，对应图5-6 (b)的蓝色电流曲线，状态翻转0 → 1和1 → 0的汉明距离为1，对应图中红色的电流曲线，相同颜色的电流分布间具有高度相似性。因此，泄露属性的定义忽略了状态翻转0 → 1(0 → 0)和1 → 0(1 → 1)的细微功耗差异。这意味着，无论其他输入状态如何变化，中间单元都会将敏感变量的状态翻转传至输出引脚。利用上述属性检查工艺库的所有逻辑单元，预先确定符合泄露属性的单元类型。通过逐步地检查单元类型，为所有模块构建完整的泄漏路径，即流经敏感变量所有数据位的单元网络。



(a) INV (b) DFF

(c) XOR (d) NAND

图 5-6 不同逻辑单元的瞬态电流分布

5.2 局部路径掩码方案

在识别出完整的泄漏路径后，联合布尔掩码和随机预充电，本节提出了局部路径掩码方案，由逻辑映射算法自动部署上述防护方案，用来提高密码芯片的侧信道安全性。

5.2.1 经典掩码方案

正如2.4.2节描述的，布尔掩码和随机预充电是常见的防护方案，具有较高的实现效率。然而，两种方法都无法直接用来消除泄露路径。如果单独使用布尔掩码方案，掩码修正的异或门将存在信息泄露风险。具体来说，针对泄露路径的寄存器，由异或门作为编码单元和解码单元，分别实现掩码添加和掩码修正操作。在第一个时钟周期内，敏感变量v_c与掩码m异或得到掩码型变量v_{mc}，在流经寄存器后被解码单元恢复为敏感变量v_c。在第二个时钟周期内，敏感变量v_p发生相同的掩码添加和掩码修正操作，寄存器的掩码型变量v_{mp}解码后输出敏感变量v_p。由于掩码随周期随机分布，寄存器的状态翻转$v_{mc} \rightarrow v_{mp}$被随机化，消除了泄露路径的敏感信息泄露。与此同时，编码单元发生$v_c \rightarrow v_p$的状态翻转，与敏感变量的状态翻转一致，从而继承了来自敏感变量的侧信道行为。因此，尽

管增强了原有泄露路径的安全性，布尔掩码的编码单元却成为新的泄露单元。若应用原始的随机预充电方案，将复制的寄存器插入到原寄存器和组合逻辑，当前时钟周期内所有逻辑单元处理随机数，下一个时钟周期再处理密码中间值。该方案混淆了泄露路径的数据流，但额外增加的时钟周期会降低运行速度，难以满足密码运算的性能需求。

5.2.2 逻辑映射算法

鉴于单一防护方案存在的问题，本节组合两种防护方案的优点，提出局部路径掩码方案。首先对泄露路径实施布尔掩码方案，随机化所有时序逻辑和组合逻辑的敏感变量。在此基础上，对组合逻辑实施随机预充电方案，通过随机码流掩盖编码单元的状态翻转。同时，利用时钟树资源设计时序控制模块，完成布尔掩码和随机预充电的时序调度。为实现局部路径掩码的自动部署，采用逻辑映射算法创建防护后的电路网表，具体流程如算法8所示。

Algorithm 8 逻辑映射算法

Input:

1: $L = \{\text{FF1}, O_1, O_2, ..., O_{n-1}\}$

2: 掩码m和预充电码r

Output: $L = \{\text{XOR1}, \text{XOR2}, \text{FF2}, \text{MUX}, \text{FF1}, O_1, O_2, ..., O_{n-1}\}$

3: 编码敏感变量 ← 编码单元XOR1

4: 传递掩码型敏感变量 ← 源单元FF1

5: 存储随机掩码 ← 存储单元FF2

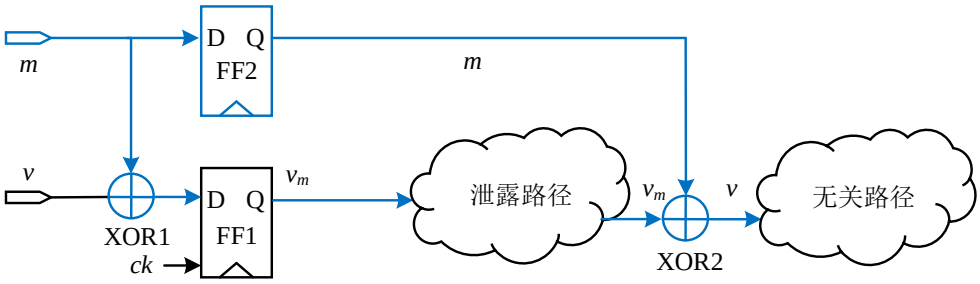
6: 解码掩码型敏感变量 ← 解码单元XOR2

7: 调度防护方案 ← 选择单元MUX

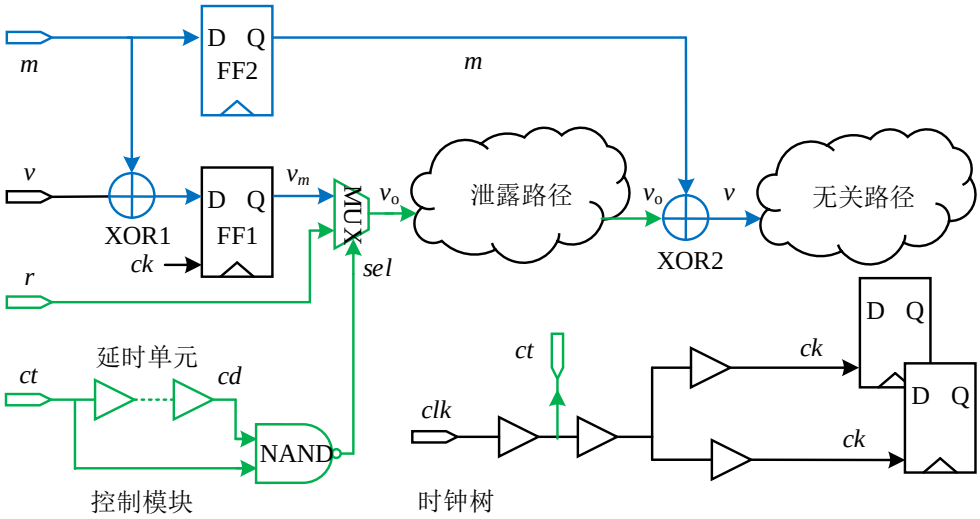
8: 产生调度信号 ← 时序控制模块

图5-7 (a)为密码电路的原始泄露路径，敏感变量v首先通过源单元FF1，流经泄露路径的中间单元到达无关路径。图中源单元表示为D触发器FF1，由时钟信号clk控制数据采样。逻辑映射将泄露路径L表示为逻辑单元O_i的集合，即$L = \{O_1, O_2, ..., O_{n-1}\}$，由字典Cell记录各逻辑单元的详细信息。此外，逻辑映射的输入还包括掩码信号m和预充电信号r，由真随机数生成器或伪随机数生成器产生。在步骤3中，从源单元开始部署布尔掩码，在输入端D引脚插入异或门XOR1，作为编码单元编码敏感变量v和掩码m。这时，源单元接收掩码型敏感变量v_m，逻辑函数为$v_m = \text{XOR1}(v, m)$。在步骤5中，添加D触发器FF2作为掩码m的存储单元，逻辑函数为$m = \text{FF2}(m)$，它的数量由泄露路径的数目确定。在步骤6中，选择泄露路径和无关路径的边界节点，添加异或门XOR2作为解码单元，恢复敏感

(a) 原始泄露路径 (黑色部分)



(b) 布尔掩码 (蓝色部分)



(c) 随机预充电 (绿色部分)

图 5-7　局部路径掩码架构图

变量v并传入后续的数据路径，逻辑函数为v = XOR2(v_m, m)。图5-7 (b)为部署布尔掩码后的泄露路径，掩码添加操作由编码单元实现，掩码修正操作由解码单元实现，而掩码转换操作由存储单元完成。此时，原始泄露路径的敏感变量被掩码随机化，混淆了敏感变量产生的侧信道行为。然而，解码单元XOR2为异或门，逻辑函数符合泄露属性的定义，将形成新的信息泄露风险点。

在此基础，随机预充电进一步增强防护效果，同时消除解码单元的泄露风险。为减少额外的时钟周期，随机预充电用来保护泄露路径的组合逻辑。在步骤7中，选择源单元和中间单元的电路节点，添加数据选择器MUX作为选择单元，由调度信号sel选择要输出的数据，即掩码型敏感变量v_m或预充电码r。如图5-7 (c)所示，时序控制模块由与非门NAND和一定数量的延迟单元构成，输入

信号*ct*来自时钟树传递的时钟信号*clk*，且位于时钟定义点附近的分布节点，输出信号即调度信号*sel*与选择单元的控制端相连。在密码电路的时钟树中，时钟信号从时钟定义点传递到各寄存器的时钟输入端，时钟定义点被视为根节点，时钟树的驱动单元叫做分布节点，寄存器的时钟输入端表示为叶节点。图5-8为预期的工作模式，时钟信号*clk*在t_0时刻发生上升沿跳变，流经分布节点到达时序控制模块的输入端。在t_1时刻，调度信号*sel*产生逻辑低到高的电平翻转，此时选择单元首先输出预充电码*r*，将中间单元和解码单元的当前数据更替为随机码流。在t_2时刻，上升沿跳变传递到源单元FF1的CK引脚，使其更新内部存储的掩码型敏感变量，由于调度信号*sel*维持高电平，选择单元阻塞了源单元FF1输出端的状态传递。其后在t_3时刻，调度信号*sel*产生逻辑高到低的电平翻转，选择单元输出掩码型敏感变量v_m，覆盖泄露路径流动的随机码流，并将正确的结果传递给后续数据路径。因此，源单元和编码单元分别得到布尔掩码和随机预充电的单重保护，而泄露路径的中间单元得到了联合方案的双重保护。假定原始泄露路径发生$v_1 \rightarrow v_2$的状态转换。在应用局部路径掩码方案后，源单元将发生$(v_1 \oplus m) \rightarrow (v_2 \oplus m)$的状态转换，中间单元将发生$r \rightarrow (v_2 \oplus m)$的状态转换，而编码单元将发生$r \rightarrow v_2$的状态转换。其中，随机的掩码*m*和预充电码值*r*均匀分布，会扰乱原始泄露路径的敏感变量及状态翻转，从而混淆由此产生的侧信道行为。对于电磁信息而言，逻辑单元的翻转活动是敏感信息来源，金属互连网络的金属线充当辐射载体。因此，局部路径掩码能够增强密码电路的安全性，同时抵御功耗分析攻击和电磁分析攻击。

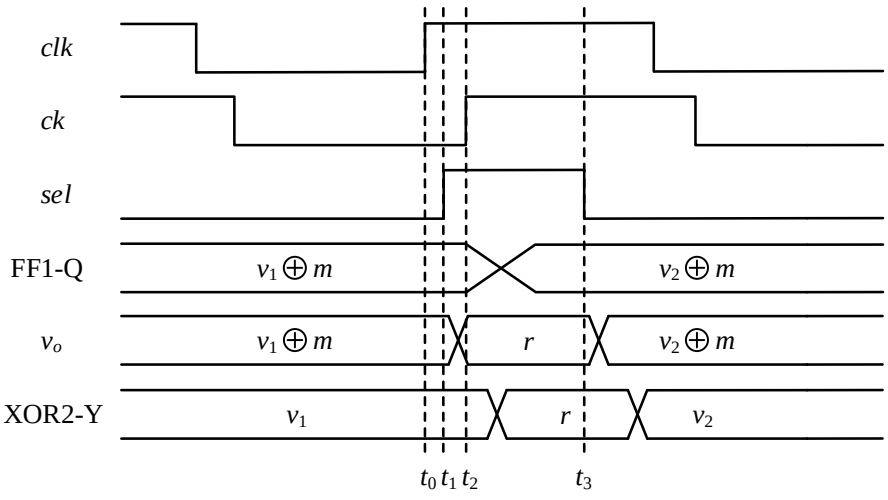


图 5-8　局部路径掩码的信号波形图

5.2.3 时序约束分析

局部路径掩码需要满足特定的时序约束，使密码电路兼顾时序收敛和安全增强的效果。在芯片设计和验证过程，静态时序分析贯穿于各个阶段，包括建立时间分析和保持时间分析，用来检查时序结果是否满足设计的约束条件。以图5-9的D触发器为例，建立时间分析要求时钟作用沿到达前，输入信号需保持一定时间的电平稳定，该段时间被称为建立时间。保持时间分析要求在时钟作用沿到达后，输入信号仍然不变且维持一段时间，该段时间被称为保持时间。两种时间由时序库标定，同属于D触发器的固有属性，同时满足才能完成正确的数据采样。考虑原始泄露路径的时序分析，时钟信号周期为T_{cycle}，组合逻辑单元的总延迟为T_{Comb}，D触发器CK端到Q端的延迟为T_{CK-Q}，建立时间为T_{setup}，保持时间为T_{hold}。为避免建立时间违例，需满足公式(5-6)的时序要求。为避免保持时间违例，则需要满足公式(5-7)的时序要求。

$$T_{CK-Q} + T_{Comb} + T_{setup} \leqslant T_{cycle} + T_{skew} \tag{5-6}$$

$$T_{CK-Q} + T_{Comb} \geqslant T_{hold} + T_{skew} \tag{5-7}$$

其中T_{skew}表示时钟信号从根节点到各个叶节点的时钟偏差。在实际电路中，根节点到达各个叶节点的路径长度不同，每条时钟路径的驱动单元种类和数量不同，所驱动的负载数目和负载电容也存在差异，因此时钟信号到达各个叶节点时存在延时偏差。

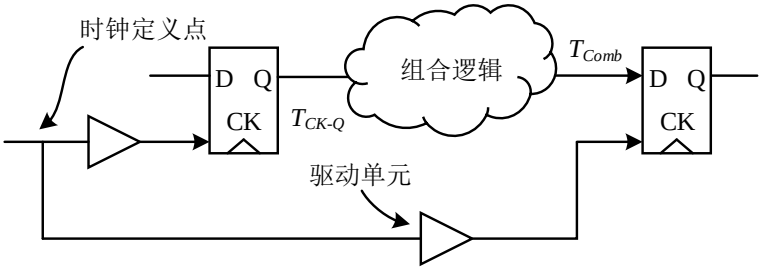


图 5-9 建立时间和保持时间

由图5-8可知，局部路径掩码提出了更高的时序要求，特别是调度信号*sel*的上升沿和下降沿，需要在合理的时间范围内发生跳变，这也决定了时序控制模块的内部结构，如输入信号*ct*的位置以及延时单元的类型和数量。T_{clk-ct}和T_{clk-ck}分别表示根节点到时序控制模块和叶节点的延迟，T_{ct-cd}表示延时单元链及线负载的延迟，T_{cd-sel}表示与非门NAND及线负载的延时。对于调度信号*sel*的时序要求，公式(5-8)定义了上升沿跳变的最早时间，此时预充电码*r*流经泄露路径和无关路径。若上升沿提前到达，将留给预充电码*r*充足的传播时间，

被下一级时序逻辑接收从而输出错误结果。公式(5-9)定义了上升沿跳变的最迟时间，保证预充电码r先于掩码型敏感变量v_m输出。若上升沿过晚到达，选择单元将提前输出源单元更新的状态，使得随机预充电的保护作用失去效果。

$$T_{clk-ct} + T_{Comb} + T_{cd-sel} > T_{clk-ck} + T_{CK-Q} + T_{hold} \tag{5-8}$$

$$T_{clk-ct} + T_{cd-sel} < T_{clk-ck} + T_{CK-Q} \tag{5-9}$$

类似地，公式(5-10)定义了下降沿跳变的最早时间，关系到掩码型敏感变量v_m能否正常输出。若下降沿提前到达，且源单元FF1的数据采样尚未完成，后续数据路径将传递错误的采样结果。公式(5-11)定义了下降沿跳变的最晚时间，与叶节点ck信号的上升沿相比，超出的延迟会增加数据路径的传递时间，若下降沿过晚到达，输入数据无法在建立时间之前到达下一级时序逻辑，将造成建立时间违例。在公式(5-8)到公式(5-11)中，T_{cycle}由时序约束提供，T_{hold}和T_{setup}由时序库标定，T_{clk-ck}、T_{CK-Q}和T_{Comb}由时序报告记录，联立不等式可确定T_{clk-ct}、T_{ct-cd}、T_{cd-sel}的取值空间。在该取值空间中，三个参数的取值互相影响，任意两个参数可确定第三个参数，构成完整的时序控制模块。例如，已选定输入信号ct的位置和与非门NAND的类型，即可知道延时单元链的组成结构。

$$T_{clk-ct} + T_{ct-cd} + T_{cd-sel} > T_{clk-ck} + T_{CK-Q} \tag{5-10}$$

$$T_{clk-ct} + T_{ct-cd} + T_{cd-sel} + T_{Comb} < T_{clk-ck} + T_{cycle} - T_{setup} \tag{5-11}$$

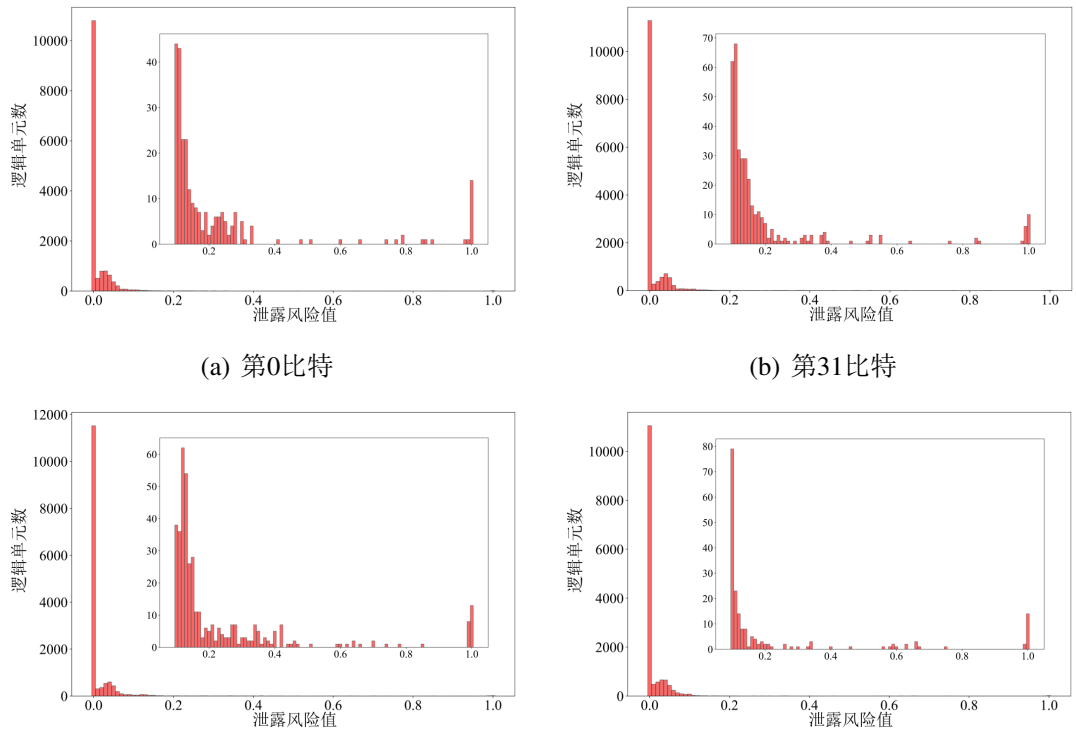
为了降低局部路径掩码的性能影响，还需更新时序约束文件的相关参数，用于指导密码芯片的物理实现过程。时序约束文件主要有时钟、输入延迟和输出延迟三部分，与时钟本身相关的参数包括时钟定义、时钟延滞和时钟不确定性，分别由create_clock、create_clock_latency和create_clock_uncertainty命令控制。时钟延滞是从时钟源到寄存器的插入延迟，包括时钟源插入延迟和时钟网络插入延迟。除了时钟偏差之外，时钟不确定性还包括时钟抖动，是实际时钟信号和理想时钟信号的差值，其组成部分有确定抖动和随机抖动。在局部路径掩码中，时钟信号从根节点开始，有时钟树和时序控制模块两种传播路径，$|T_{clk-ct} + T_{cd-s} - T_{clk-ck}|$为路径延迟的近似差值。将上述延迟差值添加到时序约束文件中，作为时钟不确定性指标的一部分，模拟更为恶劣的时序情况，从而在确保安全增强的前提下，降低局部路径掩码的性能开销。

5.3 增强型AES电路实现

针对3.5节设计的AES电路，本节借助泄漏路径识别完成安全溯源，应用局部路径掩码实现靶向增强，形成具有侧信道抗性的增强型AES电路。这之后，对

其进行CEMA和CPA仿真攻击，以验证局部路径掩码的防护效果，并分析了防护后的功耗、面积和性能开销。

5.3.1 安全溯源结果



(a) 第0比特　(b) 第31比特

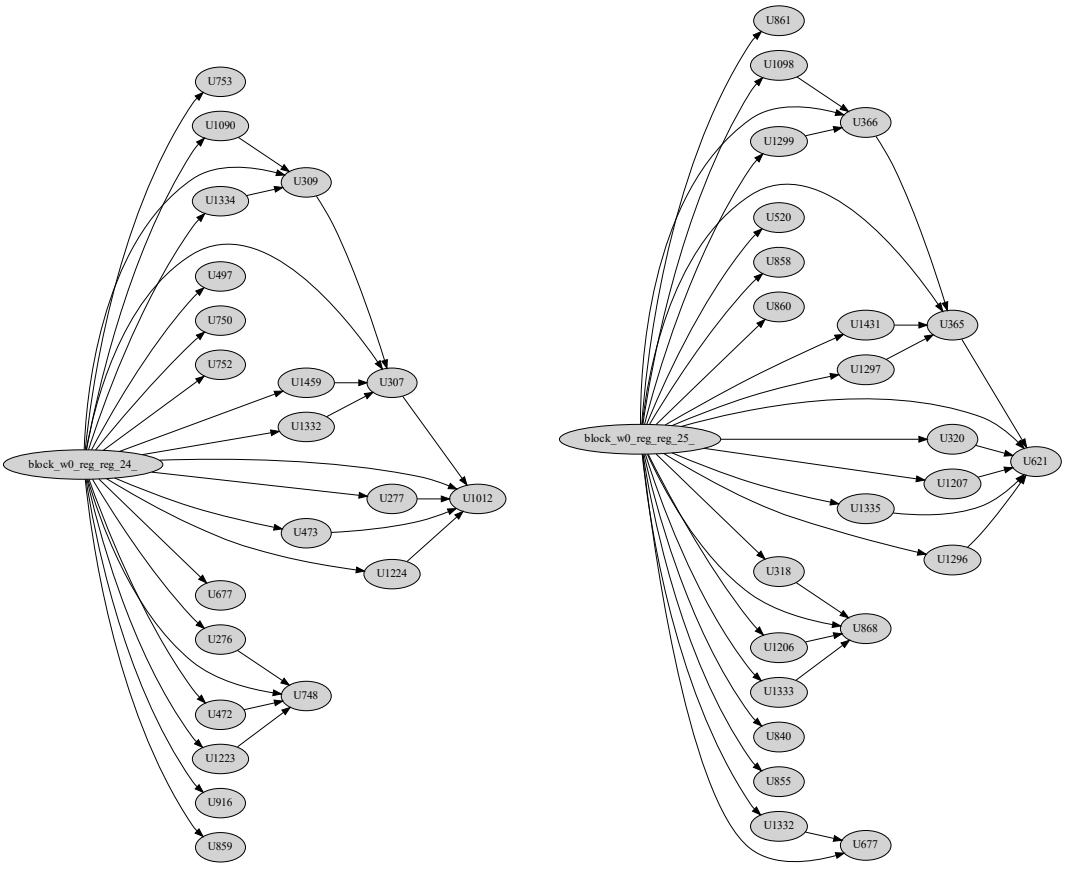
(c) 第63比特　(d) 第95比特

图 5-10 特定比特对应的泄露风险分布

在对AES电路进行逻辑综合和物理实现时，收集泄露路径识别所需的电路文件，包括综合后设计网表、版图后设计网表、SDC文件、SDF文件和SPEF文件等。首先执行敏感信息仿真。给定1000条随机测试激励，使用Synopsys VCS工具进行动态门级仿真，生成记录单元翻转活动的VCD文件。以此为输入，借助Synopsys PrimeTime PX工具进行单元功耗分析，获得所有逻辑单元的瞬态电流值。为了执行泄露风险排序，选择初始密钥加结果作为敏感变量，即$v = p \oplus k$，p和k分别为明文和密钥字节。在这之后，敏感变量将经历十轮次的轮加密运算。根据正确密钥和给定明文，计算敏感变量的汉明距离值，构建所有比特位的信息泄露模型，结合单元功耗矩阵求解逻辑单元的泄露风险值。图5-10为特定比特对应的泄露风险分布，包括敏感变量的第0比特、第31比特、第63比特和第95比特。版图后门级网表共有14559个逻辑单元，泄露风险值低于0.1的逻辑单元约占总数的97.93%，仅有大约20个逻辑单元的泄露风险值超过0.9。由此可见，对于敏感变量的单个数据位，密码电路中只有少部分逻辑单元泄露敏感信息。本节

将信息泄露阈值设为0.95，分析敏感变量所有比特的泄露风险，共有1082个逻辑单元超过预定义的阈值，由此确定出具有高泄露风险的逻辑单元集合。以上过程中，使用Shell脚本和TCL脚本控制敏感信息仿真，编写Python脚本处理泄露风险排序，在18.54分钟内完成了动态关联度分析。

在综合后设计网表上执行拓扑结构分析，从上述逻辑单元集合中定位到164个源单元，包含128个时序逻辑和36个组合逻辑。从源单元开始，泄露属性检验构建了AES电路的泄漏路径。以上过程均由Python脚本实现，仅需9.12秒完成静态安全性检验。部分支路结构如图5-11所示，起点为时序逻辑block_w0_reg_reg_24_和block_w0_reg_reg_25_，图中顶点为源单元或中间单元，边代表单元间的连接关系。整个泄露路径具有5级深度，由2120个逻辑单元构成，涉及4893条单元连接关系，不同支路间存在重叠单元和连接关系，如图5-11 (a)和图5-11 (b)中的U1332和U677。因此，在对AES电路部署防护策略时，需要将泄漏路径作为整体进行重点保护。



(a) 泄露路径支路1　　(b) 泄露路径支路2

图 5-11　AES电路的泄露路径结构

5.3.2 靶向增强结果

使用Python语言实现逻辑映射算法，将局部路径掩码部署到综合后门级网表，用时0.13秒创建了增强型AES电路的主模块。为了降低性能开销，主模块采用4个时序控制模块，将调度信号的扇出数目降为32。对于掩码信号和预充电信号，选择线性反馈移位寄存器 (Linear Feedback Shift Register，LFSR) 产生随机码流，该电路由32级D触发器和异或门构成，本征多项式为$f(x) = x^{32} + x^7 + x^5 + x^3 + x^2 + x + 1$，最大能产生$2^{32} - 1$个输出状态。在LFSR电路中，寄存器的最高比特与最低比特相连，工作时所有比特执行移位操作，同时对特定比特进行异或操作。这样，寄存器的前后级输出不再具备明显相关性。当主模块和LFSR模块网表合并后，添加使能信号控制防护生效范围，仅在加密期间生成调度信号和随机码流，从而降低增强型AES电路的功耗开销。

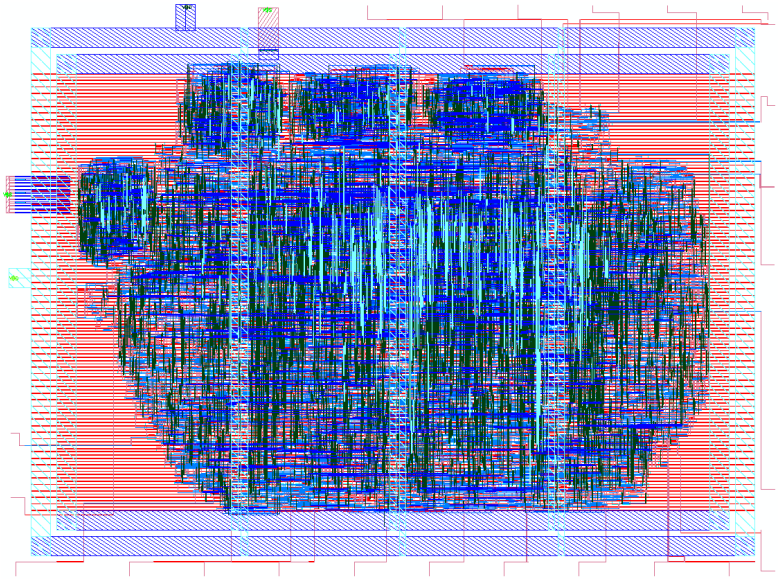


图 5-12 增强型AES电路的物理版图

为避免电源网格对侧信道信息的影响，采用与3.5节相同的电源规划，图5-12为布局布线后的物理版图，使用Synopsys VCS工具完成了功能验证，仿真结果如图5-13所示。从图中可知，round信号代表当前的加密轮数，密钥key设定为128'h0123_4567_89ab_cdef_0123_4567_89ab_cdef，当输入明文block是128'hfecc_5206_ba78_64db_0e62_240b_b1e8_613d时，经过十轮加密运算后，输出密文result为128'h82c9_37f6_ef5e_ccbb_db13_ac23_345b_abe6，输出密文与预期结果一致。此外clk为寄存器的时钟信号，sectl_byte0为调度信号，对比两者的上升沿时间可知，调度信号超前时钟信号357ps。同时，由调度信号的脉冲宽度可知，时序控制模块的延迟约为681ps。racode为预充电信号，

encode和decode分别是供给编码单元和解码单元的掩码信号，在非加密期间上述信号及调度信号均为低电平。在十轮加密运算期间，LFSR模块的输出码流在各个周期随机分布，使攻击者无法获知预充电信号和掩码信号，保证了局部路径掩码的防护效果。

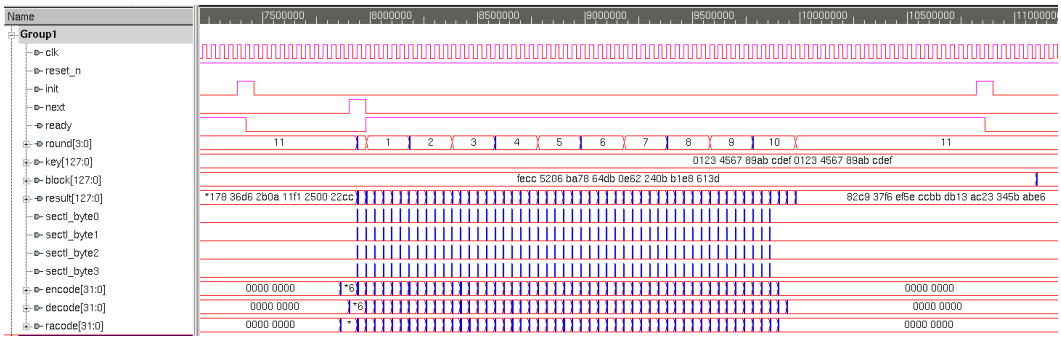


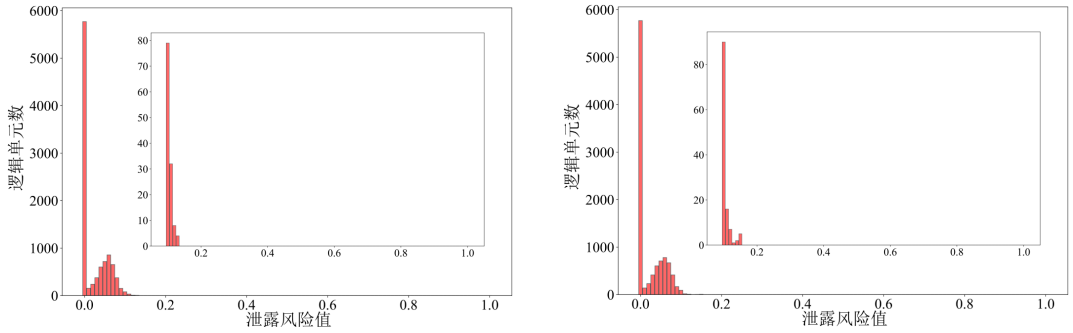
图 5-13　增强型AES电路的仿真结果

在实现局部路径掩码方案的同时，也引入了额外的功耗、性能和面积开销。包括LFSR模块在内，增强型AES电路添加了659个逻辑单元，相比原始电路的面积消耗增加6.53%。电路功耗从13.3mW增至13.9mW，引入额外的600μW功率，使得功耗开销增长4.51%。在施加防护方案后，AES电路的最高运行频率从45.5MHz降低到44.1MHz，增加了3.1%的性能开销。

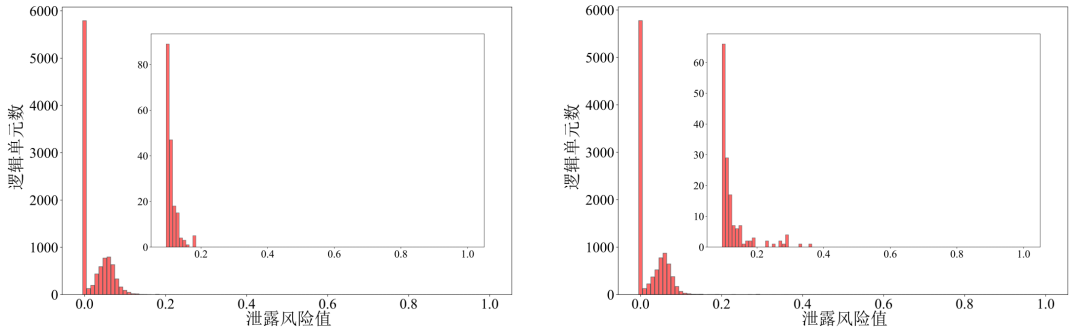
5.3.3　安全性验证结果

首先验证增强型AES电路是否存在泄露路径，重复5.3.1节的动态关联度分析过程，分析版图后门级网表的泄露风险分布，图5-14为特定比特对应的泄露风险分布，对于敏感变量的第0比特、第31比特、第63比特，所有逻辑单元的泄露风险值低于0.2。而对于敏感变量的第95比特，所有逻辑单元的泄露风险值也在0.4以下。由此可见，在应用局部路径掩码之后，消除了原始泄露路径的信息泄露风险，逻辑单元表现出与敏感变量无关的侧信道行为。

进一步地，对增强型AES电路进行CPA攻击，验证其抵抗功耗分析攻击的能力。使用Synopsys PrimeTime PX工具仿真全局功耗信息，分别收集了无防护和增强型AES电路的10万条功耗曲线。本节选择首轮字节替换作为攻击点，构建输出结果的汉明距离模型，并在该操作的时间段开展CPA仿真攻击。图5-15显示了所有猜测密钥随时间点变化的相关性曲线。对于未受保护的AES电路，正确密钥的最大相关性系数为0.391，远远大于错误密钥的相关性峰值0.185，表明其功耗曲线与攻击者使用的泄露模型高度相关。而对于增强型AES电路，局部路径掩码将正确密钥的最大相关性降低到0.018，低于错误密钥在附近时间点的相关性峰值0.033，意味着正确密钥的相关性被错误密钥完全淹没。图5-16显示了



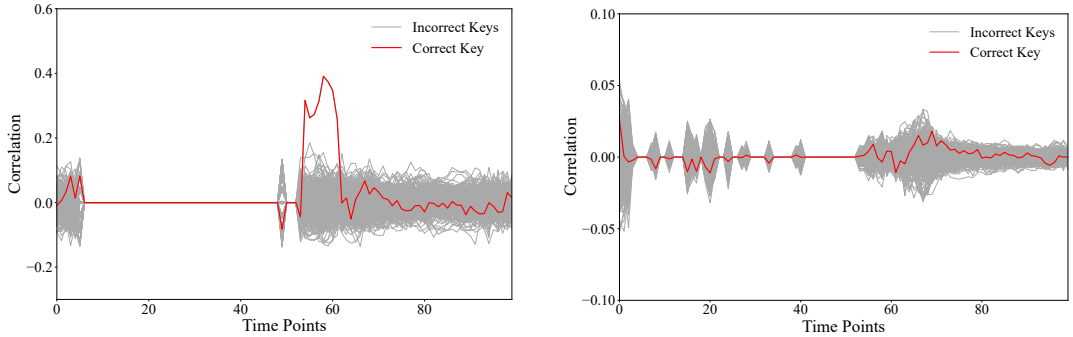
(a) 第0比特 (b) 第31比特



(c) 第63比特 (d) 第95比特

图 5-14 特定比特对应的泄露风险分布

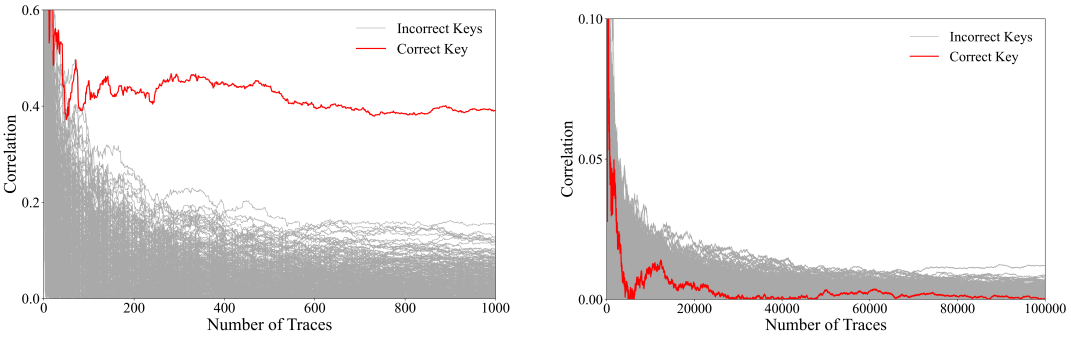
所有猜测密钥随曲线条数变化的的相关性曲线，攻击者使用84条功耗曲线恢复了无防护AES电路的正确密钥，在施加局部路径掩码后，即使采集10万条曲线也不足以获取正确密钥。这表明增强型AES电路的安全性提升了1190倍，能够有效抵御功耗分析攻击。



(a) 防护前AES电路 (b) 防护后AES电路

图 5-15 随时间点变化的相关性曲线

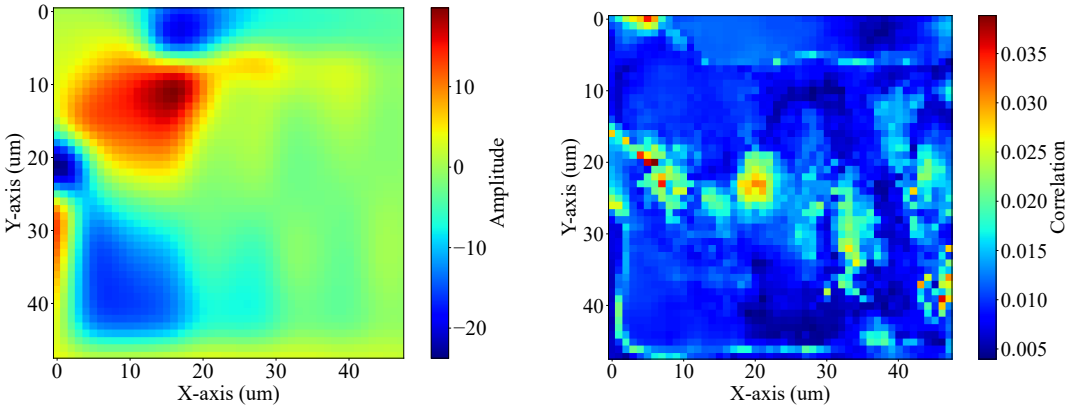
与此同时，对增强型AES电路进行CEMA攻击，验证其抵御电磁分析攻击的能力。将芯片表面划分为48 × 48的网格矩阵，使用上一章提出的测评优化方法，合成首轮字节替换操作的磁场曲线，收集了16万随机明文对应的磁场分布



(a) 防护前AES电路　　(b) 防护后AES电路

图 5-16　随曲线数目变化的相关性曲线

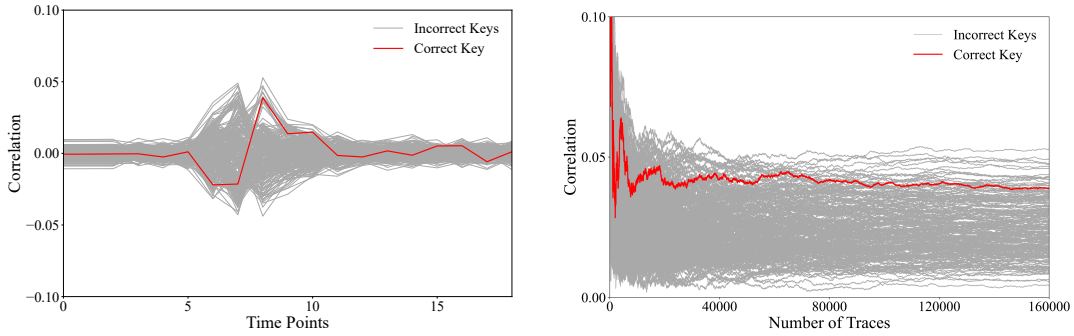
数据。对于明文128′ha6d2_125d_a3bc_8233_cf5d_2d40_3aa9_2b01，图5-17 (a)展示了距离芯片表面100μm的磁场分布情况。对网格矩阵的所有格点进行CEMA攻击，取正确密钥的最大相关系数作为信息泄露的度量，代表着电磁曲线与敏感信息的依赖程度。图5-17 (b)为随空间位置变化的信息泄露程度，在电源环线和电源条线附件有5处信息泄露热点，其中正确密钥的最大相关性系数为0.039。在该信息泄露热点处，所有猜测密钥的相关性曲线如图5-18 (a)所示，防护之后的正确密钥已被错误密钥完全掩盖。图5-18 (b)显示了随曲线条数变化的的相关性曲线，由3.5.3节可知，攻击者使用150条电磁曲线即可破解无防护的AES电路，在施加局部路径掩码后，即使采集16万条曲线也不足以恢复正确密钥。这表明增强型AES电路的安全性提升了1066倍，能够有效抵御电磁分析攻击。



(a) 空间磁场分布　　(b) 信息泄露分布

图 5-17　增强型AES电路的空间磁场和信息泄露

表5-1比较了相关工作的功耗、性能、面积和安全指标。Moradi等人设计了AES电路的门限掩码，将MTD指标提升了100倍，但是面积和功耗消耗分别增加了3倍和2倍，同时额外增加了40个时钟周期[76]。最近，Moradi等人优化了上述掩码方案，将电路面积开销降低至196%，额外的时钟周期缩减了一半数



(a) 随时间点变化的相关性曲线　　(b) 随曲线条数变化的相关性曲线

图 5-18　增强型AES电路的CEMA攻击结果

表 5-1　相关工作的安全水平和电路开销

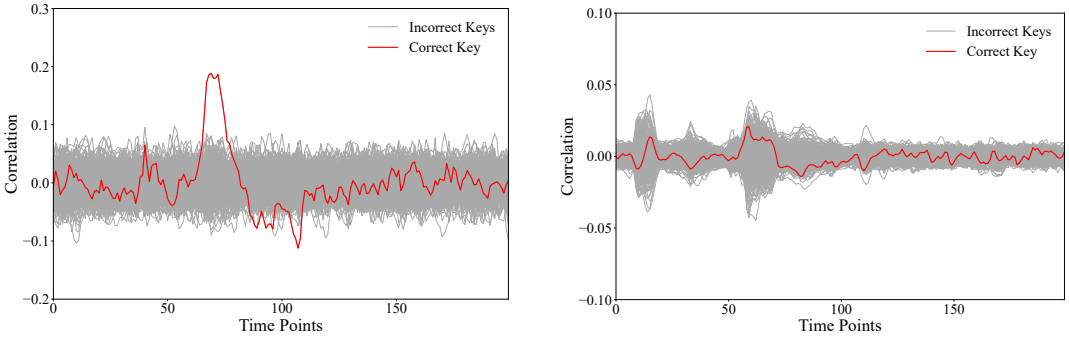
相关工作	安全指标		开销指标		
	功耗	电磁	面积	功耗	性能
Moradi [76]	100×	–	359%	262%	40
Moradi [83]	10000×	–	196%	–	20
Yao [117]	4×	–	10%	–	–
KF [119]	16×	–	31.9%	–	31.25%
SLPSK [118]	107×	–	0%	0%	0%
Singh [57]	4210×	136×	96.7%	32%	10.4%
Das [58]	–	167×	23%	49%	0%
Das [59]	125000×	83333×	36.7%	49.8%	0%
Li [61]	–	150×	20%	–	70%
本论文	1190×	1066×	6.53%	4.51%	3.1%

量[83]。Yao等人提出了架构相关性分析，通过泄露窗口缩窄、架构关联分析和泄露因子计算，定位具有信息泄露风险的逻辑单元，将其替换为行波动态差分逻辑单元，由此正确密钥的相关性最大值降低了4倍，相比原始电路增加了10%的面积开销 [117]。KF等人提取泄露模型和仿真曲线的距离向量，分析各模块的侧信道脆弱性系数，在识别到泄露模块后，设计了四轮费斯妥网络来混淆运行数据 [119]。结果显示MTD提高了16倍，同时牺牲了31.9%的面积和31.25%的性能。以上两种方法同属于安全溯源和靶向增强的研究范畴。SLPSK等人提出了逻辑单元的参数配置流程，在不增加开销的条件下将MTD提升了107倍，但该方案存在多种电源电压、阈值电压和驱动能力，大幅增加了物理实现和芯片制造的难度 [118]。Singh等人提出了安全敏感的片上低压差线性稳压器，这种方法将功耗和电磁攻击抗性分别增加了4210倍和136倍 [57]。然而，由于负载电容较大，面积开销约为100%。Das等人提出的STELLAR方法具有167倍的安全提升，但引入

了23%的面积开销和50%的功耗开销[58]。其后，他们优化了STELLAR方法的电流衰减电路，将密码模块的信号波动减弱了350倍，大幅提升了AES电路的安全水平[59]。Li等人提出的数据流空间随机化方法，将抗局部电磁分析的能力提高了50倍，但是，该方法使得AES电路的性能下降了70%[61]。在本论文中，局部路径掩码将MTD提高了1190倍和1066倍，能够成功抵御功耗和电磁分析攻击。在电路面积、功耗和性能消耗方面，仅产生6.53%、4.51%和3.1%开销。取得上述结果的原因是，本论文将多个易受攻击的逻辑单元作为整体，进行泄露路径的安全溯源和靶向增强，既降低了对大量逻辑单元的保护难度，也避免了电路模块中不相关逻辑单元的额外影响，能以较少的功耗、性能和面积开销提升侧信道抗性。

5.3.4 延展性验证结果

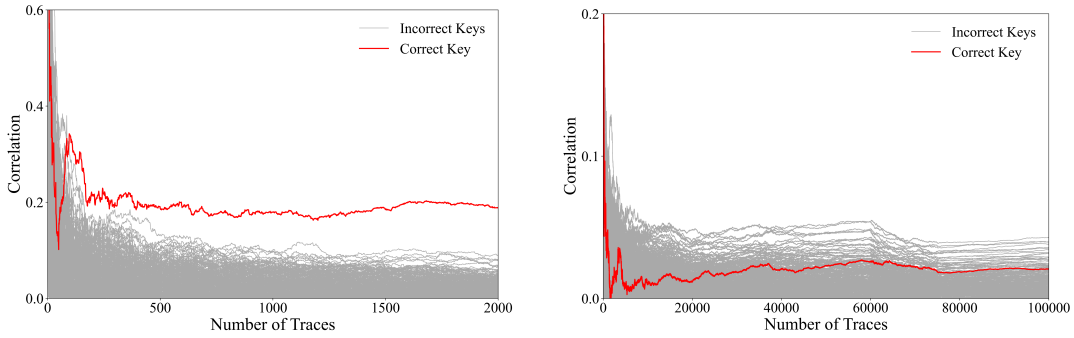
尽管局部路径掩码是为ASIC芯片设计的，但增强型AES电路可迁移到FPGA芯片，这需要调整防护后的电路门级网表，并重新编写逻辑单元的底层代码。以Spartan-6系列FPGA芯片为例，Xilinx ISE工具使用LUT、FF、超前进位链和多路选择器等进行编译和实现。为了防止逻辑被优化，使用硬件原语构造编码单元、解码单元、选择单元和时序控制模块的逻辑功能，对上述信号和模块设置KEEP和DONT_TOUCH约束。为验证其侧信道安全水平，选取了SAKURA-G FPGA开发平台，该平台板载了Spartan-6 XC6SLX75和Spartan-6 XC6SLX9两块FPGA芯片，其中增强型AES电路部署在主FPGA上，而它与上位机的通信由控制FPGA完成。



(a) 防护前AES电路　　(b) 防护后AES电路

图 5-19　随时间点变化的相关性曲线

在进行硅后安全测评时，使用LANGER公司的RF-B 3-2磁场探头，调整磁场探头与FPGA芯片的空间距离，使磁场探头尽可能接近FPGA芯片表面。保持固定的密钥输入，将随机明文输入到增强型AES电路，通过比较预期密文验证了功能正确性。示波器在平均模式下，以2.5GSa/s的采样率收集了10万条磁场



(a) 防护前AES电路　　(b) 防护后AES电路

图 5-20　随曲线数目变化的相关性曲线

曲线。图5-19展示了CEMA攻击结果，在无防护的AES电路中，正确密钥的相关性峰值远大于错误密钥的最大相关性。应用局部路径掩码后，正确密钥的最大相关性从0.19降低到0.02，攻击者无法观测到可利用的信息泄露。如图5-20所示，CEMA攻击只需要92条曲线恢复了原始AES电路的正确密钥。针对增强型AES电路，相同的CEMA攻击在10万条曲线之后也无法恢复正确密钥。由此可见，局部路径掩码可以延展到FPGA芯片，提高了抗电磁分析攻击的能力，使得MTD指标提升1085倍以上。

5.4　本章小结

为解决当前安全防护手段存在的问题，本章研究了密码芯片安全溯源和靶向增强方法。首先针对敏感信息的安全溯源问题，提出了动态关联度分析和静态安全性检验方法，形成了泄露路径识别技术。其中，动态关联度分析执行敏感信息仿真和泄露风险排序，提取到具有高泄露风险的逻辑单元集合。在这之后，静态安全性检验联合拓扑结构分析和泄露属性检验，从上述集合定位源单元并构建了完整的泄露路径。其次，为了消除敏感信息的泄露路径，组合布尔掩码和随机预充电的特点，提出了进行靶向增强的局部路径掩码方案，采用逻辑映射算法自动地部署到泄露路径，有效提升了密码芯片的侧信道安全性。最后，基于上述技术设计了增强型AES电路，通过仿真实验证明了安全溯源和靶向增强的有效性，将抵御侧信道攻击的能力提升了三个数量级，且仅引入少量的功耗、面积和性能开销。

第 6 章　总结与展望

6.1　总结

密码芯片是保障现代信息系统的硬件基石，广泛地应用在关系国计民生的诸多领域。但是受侧信道分析攻击的影响，密码芯片的物理安全不容乐观。其中，电磁分析攻击能够非接触式测量，并利用电磁辐射的众多信息维度，包括时域、频域和空间域信息，是最具威胁性的攻击手段之一，对此进行安全测评与防护已成为业界共识。针对这两类技术面临的关键问题，本论文进行了硅前安全测评和增强技术研究，开展了测评与增强相结合的安全设计。

1. 当前安全测评集中在硅后阶段，不利于安全漏洞的尽早发现，还可能拖延密码芯片的上市时间。为此，本论文深入研究了硅前安全测评技术，提出了集成电路版图级电磁仿真方法，在设计阶段模拟真实芯片的电磁信息，结合电磁分析技术评估芯片安全性。首先构建了集成电路的电气模型，通过电流聚合效应和金属屏蔽效应的数学推导，阐述了电磁信息的根本来源和主导因素。在此基础上，提出了多种模型简化和仿真加速技术，包括器件模型近似、寄生网络约减和GPU并行计算，优化了电流分析和电磁计算环节，形成了完整的版图级电磁仿真方法，降低了复杂物理结构对计算成本的影响。基于SMIC 180nm CMOS工艺，设计了S-Box和AES芯片并完成流片制造，搭建了近场扫描系统并开展实际测试，证明了版图级电磁仿真方法的有效性。

2. 随着芯片安全水平的提高，安全测评的数据规模不断增加，为了适应大规模数据量的安全测评，提出了基于生成对抗网络的测评优化方法，使用机器学习提高磁场数据的获取速度。以单元电流和电源网格为输入，以空间磁场为输出，设计了生成对抗网络的模型结构，通过生成器和判别器的对抗训练，优化了生成器的数据合成能力。其后，在硅前阶段的风险量化中，使用训练好的生成器合成磁场数据，量化了密码芯片的信息泄露风险。四种密码电路的验证结果表明，测评优化方法能准确量化泄露风险，相比于传统测评方法，提升了大规模数据量的测评效率，尤其适合高安全等级的芯片测评场景。

3. 为了提升密码芯片的安全性，业界已经提出了很多防护方法，但现有方法会导致较大的电路开销，有些还具有特殊的设计要求。针对此，本论文从敏感信息的泄露路径入手，提出了密码芯片安全溯源和靶向增强方法。首先，提出了动态关联度分析和静态安全性检验，形成了泄露路径识别技术，能够确定

承载高泄露风险的逻辑单元，并以此为起点构建完整的泄露路径。在这之后，设计了局部路径掩码方案，形成了自动部署防护方案的逻辑映射算法，有效降低了泄露路径的信息泄露。最后，基于上述技术设计了增强型AES电路，验证结果表明，该电路可以充分抵御侧信道分析攻击，包括功耗分析攻击和电磁分析攻击，且具有很少的面积、功耗和性能开销。

6.2 展望

在硅前安全测评和增强技术方面，本论文深入研究了芯片电磁仿真、安全测评优化、芯片安全溯源和靶向增强方法，取得了一定的研究成果，但是还存在着一些不足之处，需要在以下几点开展后续研究：

1. 对于本论文提出的电磁仿真方法，由于研发周期和流片成本的限制，仅在两款180nm工艺的密码芯片上验证了有效性，未来还需在更多工艺平台(130nm、55nm、28nm等) 上开展验证实验。同时，随着机器学习的快速发展，生成式模型的种类不断增多，后续将研究它们在测评优化方法的适用性，进一步提升安全测评的实现效率。

2. 根据安全溯源和靶向增强方法，本论文在少量额外开销的条件下，设计了高安全等级的增强型AES电路，该方法未来将扩展到更多的密码电路。特别地，由于后量子密码的研究较为前沿，本论文仅对Kyber算法开展了安全测评，后续将对其进行安全溯源和靶向增强，提升后量子密码芯片的安全性。

3. 与电磁辐射相关的安全威胁，不仅包括电磁分析攻击，还包括电磁故障攻击。在电磁故障攻击中，攻击者注入电磁脉冲诱导密码芯片出错，利用故障带来的额外信息恢复算法密钥，同样威胁着密码芯片的信息安全。因此，为了抵抗电磁故障攻击，需要研究对应的硅前安全测评和增强技术。

参考文献

[1] Longo J, Mulder E D, Page D, et al. SoC it to EM: electromagnetic side-channel attacks on a complex system-on-chip [C]. International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2015: 620–640.

[2] Xiao Y, Xin J, Shen Y. CNN based electromagnetic side channel attacks on SoC [C]. IOP Conference Series: Materials Science and Engineering. Qingdao, China: IOP Publishing, 2020: 032055.

[3] Won Y-S, Bhasin S. A Systematic Side-Channel Evaluation of Black box AES in secure MCU: Architecture Recovery and Retrieval of PUF based Secret Key [C]. 2021 IEEE International Symposium on Circuits and Systems (ISCAS). Daegu, Korea: IEEE, 2021: 1–5.

[4] Haas G, Aysu A. Apple vs. EMA: electromagnetic side channel attacks on apple CoreCrypto [C]. Proceedings of the 59th ACM/IEEE Design Automation Conference. San Francisco, CA, USA: ACM, 2022: 247–252.

[5] Kocher P, Jaffe J, Jun B. Differential power analysis [C]. Annual international cryptology conference. Berlin, Heidelberg: Springer, 1999: 388–397.

[6] Gandolfi K, Mourtel C, Olivier F. Electromagnetic analysis: Concrete results [C]. International workshop on cryptographic hardware and embedded systems. Berlin, Heidelberg: Springer, 2001: 251–261.

[7] Quisquater J-J, Samyde D. Electromagnetic analysis (ema): Measures and counter-measures for smart cards [C]. International Conference on Research in Smart Cards. Berlin, Heidelberg: Springer, 2001: 200–210.

[8] Agrawal D, Archambeault B, Rao J R, et al. The EM side—channel (s) [C]. International workshop on cryptographic hardware and embedded systems. Berlin, Heidelberg: Springer, 2002: 29–45.

[9] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model [C]. International workshop on cryptographic hardware and embedded systems. Berlin, Heidelberg: Springer, 2004: 16–29.

[10] GRechberger C, Oswald E. Practical template attacks [C]. International Workshop on Information Security Applications. Berlin, Heidelberg: Springer, 2004: 440–456.

[11] Gebotys C H, Ho S, Tiu C C. EM analysis of Rijndael and ECC on a wireless Java-based PDA [C]. International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2005: 250–264.

[12] Homma N, Nagashima S, Imai Y, et al. High-resolution side-channel attack using phase-based waveform matching [C]. International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2006: 187–200.

[13] Meynard O, Réal D, Flament F, et al. Enhancement of simple electro-magnetic attacks by pre-characterization in frequency domain and demodulation techniques [C]. 2011 Design, Automation & Test in Europe. Grenoble, France: IEEE, 2011: 1–6.

[14] Perin G, Torres L, Benoit P, et al. Amplitude demodulation-based EM analysis of different RSA implementations [C]. 2012 Design, Automation & Test in Europe Conference & Exhibition (DATE). Dresden, Germany: IEEE, 2012: 1167–1172.

[15] Hospodar G, Gierlichs B, De Mulder E, et al. Machine learning in side-channel analysis: a first study [J]. Journal of Cryptographic Engineering, 2011, 1 (4): 293–302.

[16] Heyszl J, Ibing A, Mangard S, et al. Clustering algorithms for non-profiled single-execution attacks on exponentiations [C]. International Conference on Smart Card Research and Advanced Applications. Cham: Springer, 2013: 79–93.

[17] Özgen E, Papachristodoulou L, Batina L. Template attacks using classification algorithms [C]. 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). McLean, VA, USA: IEEE, 2016: 242–247.

[18] Picek S, Heuser A, Jovic A, et al. The curse of class imbalance and conflicting metrics with machine learning for side-channel evaluations [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019, 2019 (1): 1–29.

[19] Yu H, Shan H, Panoff M, et al. Cross-Device Profiled Side-Channel Attacks using Meta-Transfer Learning [C]. 2021 58th ACM/IEEE Design Automation Conference (DAC). San Francisco, CA, USA: IEEE, 2021: 703–708.

[20] Standaert F-X, Malkin T G, Yung M. A unified framework for the analysis of side-channel key recovery attacks [C]. Annual international conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg: Springer, 2009: 443–461.

[21] Gilbert G, Benjamin J, Jaffe J, et al. A testing methodology for side-channel resistance validation [C]. NIST non-invasive attack testing workshop. Nara, Japan: Springer, 2011: 115–136.

[22] Schneider T, Moradi A. Leakage assessment methodology [C]. International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2015: 495–513.

[23] Moradi A, Richter B, Schneider T, et al. Leakage detection with the x2-test [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 2018 (1): 209–237.

[24] Heyszl J, Mangard S, Heinz B, et al. Localized electromagnetic analysis of cryptographic implementations [C]. Cryptographers' track at the RSA conference. Berlin, Heidelberg: Springer, 2012: 231–244.

[25] Heyszl J, Merli D, Heinz B, et al. Strengths and limitations of high-resolution electromagnetic field measurements for side-channel analysis [C]. International Conference on Smart Card Research and Advanced Applications. Berlin, Heidelberg: Springer, 2012: 248–262.

[26] Unterstein F, Heyszl J, Santis F D, et al. Dissecting leakage resilient prfs with multivariate localized em attacks [C]. International Workshop on Constructive Side-Channel Analysis and Secure Design. Berlin, Heidelberg: Springer, 2017: 34–49.

[27] Immler V, Specht R, Unterstein F. Your rails cannot hide from localized EM: how dual-rail logic fails on FPGAs [C]. International Conference on Cryptographic Hardware and Embedded Systems. Cham: Springer, 2017: 403–424.

[28] Specht R, Immler V, Unterstein F, et al. Dividing the threshold: Multi-probe localized EM analysis on threshold implementations [C]. 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). Washington, DC, USA: IEEE, 2018: 33–40.

[29] Iyer V V, Yilmaz A E. An adaptive acquisition approach to localize electromagnetic information leakage from cryptographic modules [C]. 2019 IEEE Texas Symposium on Wireless and Microwave Circuits and Systems (WMCS). Waco, TX, USA: IEEE, 2019: 1–6.

[30] Danial J, Das D, Ghosh S, et al. SCNIFFER: Low-cost, automated, efficient electromagnetic side-channel sniffing [J]. IEEE Access, 2020, 8: 173414–173427.

[31] Vasselle A, Maurine P, Cozzi M. Breaking mobile firmware encryption through near-field side-channel analysis [C]. Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop. New York, NY, USA: ACM, 2019: 23–32.

[32] 邓高明，赵强，张鹏，等. 针对密码芯片的电磁频域模板分析攻击 [J]. 计算机学报，2009，32 (04)： 602–610.

[33] 张鹏，邓高明，陈开颜，等. 针对AES密码芯片的远场相关性电磁分析攻击 [J]. 华中科技大学学报(自然科学版)，2009，37 (08)： 31–34.

[34] 陈开颜，余浩，邹程，等. 针对FPGA密码芯片的近场差分电磁分析攻击 [J]. 计算机工程与应用，2013，49 (18)： 89–93.

[35] 段二朋，严迎建，李佩之. 针对AES密码算法FPGA实现的CEMA攻击 [J]. 计算机工程与设计，2012，33 (08)： 2926–2930.

[36] 段二朋. 分组密码芯片的电磁分析攻击技术研究 [D]. 郑州: 解放军信息工程大学, 2012.

[37] 孙春辉，李晖，杨旸，等. PRESENT密码算法的差分电磁攻击研究 [J]. 电子科技大学学报，2013，42 (03)： 25–30.

[38] 刘飚. 基于机器学习的密码芯片电磁攻击技术研究 [D]. 北京: 北京邮电大学, 2014.

[39] Zhang H-x, Han G, Li J. Wavelet Transform-principal component analysis in electromagnetic attack [C]. 2015 7th Asia-Pacific Conference on Environmental Electromagnetics (CEEM). Hangzhou, China: IEEE, 2015: 420–423.

[40] Zhou X, Sun D, Wang Z, et al. An adaptive singular value decomposition-based method to enhance correlation electromagnetic analysis [C]. 2016 IEEE International Symposium on Electromagnetic Compatibility (EMC). Ottawa, ON, Canada: IEEE, 2016: 170–175.

[41] Ou C, Wang Z, Sun D, et al. A new efficient interesting points enhanced electromagnetic attack on AT89S52 [C]. 2016 IEEE International Symposium on Electromagnetic Compatibility (EMC). Ottawa, ON, Canada: IEEE, 2016: 176–181.

[42] Zhou W-h, Kong F-t. Electromagnetic side channel attack against embedded encryption chips [C]. 2019 IEEE 19th International Conference on Communication Technology (ICCT). Xi'an, China: IEEE, 2019: 140–144.

[43] Khan A W, Wanchoo T, Mumcu G, et al. Implications of distributed on-chip power delivery on EM side-channel attacks [C]. 2017 IEEE International Conference on Computer Design (ICCD). Boston, MA, USA: IEEE, 2017: 329–336.

[44] Li H, Markettos A T, Moore S. Security evaluation against electromagnetic analysis at design time [C]. International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2005: 280–292.

[45] Peeters E, Standaert F-X, Quisquater J-J. Power and electromagnetic analysis: Improved model, consequences and comparisons [J]. Integration, 2007, 40 (1): 52–60.

[46] Ordas T, Lisart M, Sicard E, et al. Near-field mapping system to scan in time domain the magnetic emissions of integrated circuits [C]. International Workshop on Power and Timing Modeling, Optimization and Simulation. Berlin, Heidelberg: Springer, 2008: 229–236.

[47] Lomné V, Maurine P, Torres L, et al. Modeling time domain magnetic emissions of ICs [C]. International Workshop on Power and Timing Modeling, Optimization and Simulation. Berlin, Heidelberg: Springer, 2010: 238–249.

[48] Kumar A, Scarborough C, Yilmaz A, et al. Efficient simulation of EM side-channel attack resilience [C]. 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). Irvine, CA, USA: IEEE, 2017: 123–130.

[49] Poggi D, Ordas T, Sarafianos A, et al. Checking Robustness Against EM Side-Channel Attacks Prior to Manufacturing [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021: 1–1.

[50] 杜逸璇. 集成电路电磁干扰建模与精确预测方法研究 [D]. 哈尔滨: 哈尔滨工程大学, 2016.

[51] He J, Ma H, Guo X, et al. Design for EM side-channel security through quantitative assessment of RTL implementations [C]. 2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC). Beijing, China: IEEE, 2020: 62–67.

[52] Yamaguchi M, Toriduka H, Kobayashi S, et al. Development of an on-chip micro shielded-loop probe to evaluate performance of magnetic film to protect a cryptographic LSI from electromagnetic analysis [C]. 2010 IEEE International Symposium on Electromagnetic Compatibility. Fort Lauderdale, FL, USA: IEEE, 2010: 103–108.

[53] Homma N, Hayashi Y-i, Miura N, et al. EM attack is non-invasive?-design methodology and validity verification of em attack sensor [C]. International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2014: 1–16.

[54] Homma N, Hayashi Y-i, Miura N, et al. Design methodology and validity verification for a reactive countermeasure against EM attacks [J]. Journal of Cryptology, 2017, 30 (2): 373–391.

[55] Ngo X T, Danger J-L, Guilley S, et al. Cryptographically secure shield for security IPs protection [J]. IEEE Transactions on Computers, 2016, 66 (2): 354–360.

[56] Singh A, Kar M, Mathew S K, et al. Improved power/EM side-channel attack resistance of 128-bit AES engines with random fast voltage dithering [J]. IEEE Journal of Solid-State Circuits, 2018, 54 (2): 569–583.

[57] Singh A, Kar M, Chekuri V C K, et al. Enhanced power and electromagnetic SCA resistance of encryption engines via a security-aware integrated all-digital LDO [J]. IEEE Journal of Solid-State Circuits, 2019, 55 (2): 478–493.

[58] Das D, Nath M, Chatterjee B, et al. STELLAR: A generic EM side-channel attack protection through ground-up root-cause analysis [C]. 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). McLean, VA, USA: IEEE, 2019: 11–20.

[59] Das D, Danial J, Golder A, et al. 27.3 EM and power SCA-resilient AES-256 in 65nm cmos through > 350× current-domain signature attenuation [C]. 2020 IEEE International Solid-State Circuits Conference (ISSCC). San Francisco, CA, USA: IEEE, 2021: 424–426.

[60] Das D, Danial J, Golder A, et al. EM and power SCA-resilient AES-256 through > 350× current-domain signature attenuation and local lower metal routing [J]. IEEE Journal of Solid-State Circuits, 2020, 56 (1): 136–150.

[61] Li G, Iyer V, Orshansky M. Securing AES against localized EM attacks through spatial randomization of dataflow [C]. 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). McLean, VA, USA: IEEE, 2019: 191–197.

[62] Blackstone J, Das D, Althoff A, et al. iSTELLAR: intermittent Signature aTtenuation Embedded CRYPTO with Low-Level metAl Routing [C]. 2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD). Munich, Germany: IEEE, 2021: 1–9.

[63] Ghosh A, Das D, Danial J, et al. 36.2 An EM/Power SCA-Resilient AES-256 with Synthesizable Signature Attenuation Using Digital-Friendly Current Source and RO-Bleed-Based Integrated Local Feedback and Global Switched-Mode Control [C]. 2021 IEEE International Solid-State Circuits Conference (ISSCC). San Francisco, CA, USA: IEEE, 2021: 499–501.

[64] Ghosh A, Das D, Danial J, et al. Syn-STELLAR: An EM/Power SCA-Resilient AES-256 With Synthesis-Friendly Signature Attenuation [J]. IEEE Journal of Solid-State Circuits, 2021, 57 (1): 167–181.

[65] Nath M, Das D, Sen S. A Multipole Approach Toward On-Chip Metal Routing for Reduced EM Side-Channel Leakage [J]. IEEE Microwave and Wireless Components Letters, 2021, 31 (6): 685–688.

[66] Wang M, Iyer V V, Xie S, et al. Physical Design Strategies for Mitigating Fine-Grained Electromagnetic Side-Channel Attacks [C]. 2021 IEEE Custom Integrated Circuits Conference (CICC). Austin, TX, USA: IEEE, 2021: 1–2.

[67] Fang Q, Lin L, Zu Wong Y, et al. Side-Channel Attack Counteraction via Machine Learning-Targeted Power Compensation for Post-Silicon HW Security Patching [C]. 2022 IEEE International Solid-State Circuits Conference (ISSCC). San Francisco, CA, USA: IEEE, 2022: 1–3.

[68] Oswald E, Mangard S, Pramstaller N, et al. A side-channel analysis resistant description of the AES S-box [C]. International workshop on fast software encryption. Berlin, Heidelberg: Springer, 2005: 413–423.

[69] Canright D. A very compact S-box for AES [C]. International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2005: 441–455.

[70] Canright D, Batina L. A very compact “perfectly masked” S-box for AES [C]. International Conference on Applied Cryptography and Network Security. Berlin, Heidelberg: Springer, 2005: 446–459.

[71] Giraud C. An RSA implementation resistant to fault attacks and to simple power analysis [J]. IEEE Transactions on computers, 2006, 55 (9): 1116–1120.

[72] Mangard S, Pramstaller N, Oswald E. Successfully attacking masked AES hardware implementations [C]. International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2005: 157–171.

[73] Mangard S, Popp T, Gammel B M. Side-channel leakage of masked CMOS gates [C]. Cryptographers’ Track at the RSA Conference. Berlin, Heidelberg: Springer, 2005: 351–365.

[74] Mangard S, Schramm K. Pinpointing the side-channel leakage of masked AES hardware implementations [C]. International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2006: 76–90.

[75] Nikova S, Rijmen V, Schläffer M. Secure hardware implementation of nonlinear functions in the presence of glitches [J]. Journal of Cryptology, 2011, 24 (2): 292–321.

[76] Moradi A, Poschmann A, Ling S, et al. Pushing the limits: A very compact and a threshold implementation of AES [C]. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 2011: 69–88.

[77] Maistri P, Tiran S, Maurine P, et al. Countermeasures against EM analysis for a secured FPGA-based AES implementation [C]. 2013 International Conference on Reconfigurable Computing and FPGAs (ReConFig). Cancun, Mexico: IEEE, 2013: 1–6.

[78] Masoumi M, Rezayati M H. Novel approach to protect advanced encryption standard algorithm implementation against differential electromagnetic and power analysis [J]. IEEE Transactions on Information Forensics and Security, 2014, 10 (2): 256–265.

[79] De Cnudde T, Reparaz O, Bilgin B, et al. Masking AES with $d+1$ shares in hardware [C]. International Conference on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2016: 194–212.

[80] Groß H, Iusupov R, Bloem R. Generic low-latency masking in hardware [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 2018 (1): 1–21.

[81] De Meyer L, Reparaz O, Bilgin B. Multiplicative masking for AES in hardware [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 2018 (1): 431–468.

[82] Sasdrich P, Bilgin B, Hutter M, et al. Low-latency hardware masking with application to AES [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020, 2020 (1): 300–326.

[83] Shahmirzadi A R, Moradi A. Re-consolidating first-order masking schemes: Nullifying fresh randomness [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021, 2021 (1): 305–342.

[84] Shelton M A, Chmielewski L, Samwel N, et al. Rosita++: Automatic Higher-Order Leakage Elimination from Cryptographic Code [C]. Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, USA: ACM, 2021: 685–699.

[85] Bayrak A G, Regazzoni F, Novo D, et al. Automatic application of power analysis countermeasures [J]. IEEE Transactions on Computers, 2013, 64 (2): 329–341.

[86] Huss S A, Stein O. A novel design flow for a security-driven synthesis of side-channel hardened cryptographic modules [J]. Journal of Low Power Electronics and Applications, 2017, 7 (1): 4.

[87] Kumar R, Liu X, Suresh V, et al. A SCA-Resistant AES Engine in 14nm CMOS with Time/Frequency-Domain Leakage Suppression using Non-linear Digital LDO Cascaded with Arithmetic Countermeasures [C]. 2020 IEEE Symposium on VLSI Circuits. Honolulu, HI, USA: IEEE, 2020: 1–2.

[88] Kumar R, Suresh V, Kar M, et al. A 4900-μm^2 839-Mb/s Side-Channel Attack-Resistant AES-128 in 14-nm CMOS With Heterogeneous Sboxes, Linear Masked MixColumns, and Dual-Rail Key Addition [J]. IEEE Journal of Solid-State Circuits, 2020, 55 (4): 945–955.

[89] Kumar R, Suresh V B, Anders M A, et al. An 8.3-to-18Gbps Reconfigurable SCA-Resistant/Dual-Core/Blind-Bulk AES Engine in Intel 4 CMOS [C]. 2022 IEEE International Solid-State Circuits Conference (ISSCC). San Francisco, CA, USA: IEEE, 2022: 1–3.

[90] 常小龙，丁国良，武翠霞，等. 抗电磁侧信道攻击的AESS盒设计 [J]. 计算机工程，2011，37 (17)： 93–95.

[91] Wang C, Cai Y, Wang H, et al. Electromagnetic equalizer: An active countermeasure against EM side-channel attack [C]. Proceedings of the International Conference on Computer-Aided Design. San Diego, CA, USA: ACM, 2020: 1–8.

[92] 赵毅强，曹宇文，何家骥，等. 抗电磁侧信道攻击随机预混淆逻辑单元设计 [J]. 西安电子科技大学学报，2022： 1–9.

[93] Primas R, Pessl P, Mangard S. Single-trace side-channel attacks on masked lattice-based encryption [C]. Cryptographic Hardware and Embedded Systems – CHES 2017. Cham: Springer International Publishing, 2017: 513–533.

[94] Ravi P, Roy S S, Chattopadhyay A, et al. Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020, 2020 (3): 307–335.

[95] Xu Z, Pemberton O, Roy S S, et al. Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of kyber [J]. IEEE Transactions on Computers, 2021, 71 (9): 2163–2176.

[96] Sim B-Y, Kwon J, Lee J, et al. Single-trace attacks on message encoding in lattice-based KEMs [J]. IEEE Access, 2020, 71: 183175–183191.

[97] Lu Y, O’ Neill M, McCanny J. Evaluation of random delay insertion against DPA on FPGAs [J]. ACM Transactions on Reconfigurable Technology and Systems (TRETS), 2010, 4 (1): 1–20.

[98] Bayrak A G, Velickovic N, Regazzoni F, et al. An EDA-friendly protection scheme against side-channel attacks [C]. 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE). Grenoble, France: IEEE, 2013: 410–415.

[99] Tiri K, Verbauwhede I. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation [C]. Proceedings Design, Automation and Test in Europe Conference and Exhibition. Paris, France: IEEE, 2004: 246–251.

[100] Tiri K, Akmal M, Verbauwhede I. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards [C]. Proceedings of the 28th European solid-state circuits conference. Florence, Italy: IEEE, 2002: 403–406.

[101] Schulz R B, Plantz V, Brush D. Shielding theory and practice [J]. IEEE Transactions on Electromagnetic Compatibility, 1988, 30 (3): 187–201.

[102] Knoth C, Jedda H, Schlichtmann U. Current source modeling for power and timing analysis at different supply voltages [C]. 2012 Design, Automation & Test in Europe Conference & Exhibition (DATE). Dresden, Germany: IEEE, 2012: 923–928.

[103] Abrishami M S, Pedram M, Nazarian S. CSM-NN: Current source model based logic circuit simulation-a neural network approach [C]. 2019 IEEE 37th International Conference on Computer Design (ICCD). Abu Dhabi, United Arab Emirates: IEEE, 2019: 393–400.

[104] Sharifi M M, Rajaei R, Cadareanu P, et al. A Novel TIGFET-based DFF Design for Improved Resilience to Power Side-Channel Attacks [C]. 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE). Grenoble, France: IEEE, 2020: 1253–1258.

[105] Rewieński M. A perspective on fast-SPICE simulation technology [C]. Simulation and Verification of Electronic and Biological Systems. Dordrecht: Springer, 2011: 23–42.

[106] Tokui S, Okuta R, Akiba T, et al. Chainer: A deep learning framework for accelerating the research cycle [C]. Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. Anchorage AK USA: ACM, 2019: 2002–2011.

[107] Morton J M, Kaszyk K, Li L, et al. DelayRepay: delayed execution for kernel fusion in Python [C]. Proceedings of the 16th ACM SIGPLAN International Symposium on Dynamic Languages. Virtual USA: ACM, 2020: 43–56.

[108] McCann D, Oswald E, Whitnall C. Towards Practical Tools for Side Channel Aware Software Engineering:'Grey Box'Modelling for Instruction Leakages [C]. 26th USENIX Security Symposium (USENIX Security 17). Vancouver, BC, Canada: USENIX Association, 2017: 199–216.

[109] Tsukioka A, Srinivasan K, Wan S, et al. A fast side-channel leakage simulation technique based on IC chip power modeling [J]. IEEE Letters on Electromagnetic Compatibility Practice and Applications, 2019, 1 (4): 83–87.

[110] Goodfellow I, Pouget-Abadie J, Mirza M, et al. Generative adversarial networks [J]. Communications of the ACM, 2020, 63 (11): 139–144.

[111] Lu Y-C, Lee J, Agnesina A, et al. GAN-CTS: A generative adversarial framework for clock tree prediction and optimization [C]. 2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). Westminster, CO, USA: IEEE, 2019: 1–8.

[112] Alawieh M B, Li W, Lin Y, et al. High-definition routing congestion prediction for large-scale FPGAs [C]. 2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC). Beijing, China: IEEE, 2020: 26–31.

[113] Chhabria V A, Ahuja V, Prabhu A, et al. Thermal and IR drop analysis using convolutional encoder-decoder networks [C]. 2021 26th Asia and South Pacific Design Automation Conference (ASP-DAC). New York, NY, USA: ACM, 2021: 690–696.

[114] Zhou H, Jin W, Tan S X-D. GridNet: Fast data-driven EM-induced IR drop prediction and localized fixing for on-chip power grid networks [C]. 2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD). San Diego, CA, USA: IEEE, 2020: 1–9.

[115] Isola P, Zhu J-Y, Zhou T, et al. Image-to-image translation with conditional adversarial networks [C]. Proceedings of the IEEE conference on computer vision and pattern recognition. Venice, Italy: IEEE, 2017: 1125–1134.

[116] Xing Y, Li S. A compact hardware implementation of CCA-secure key exchange mechanism CRYSTALS-KYBER on FPGA [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021, 2021 (2): 328–356.

[117] Yao Y, Kathuria T, Ege B, et al. Architecture correlation analysis (ACA): Identifying the source of side-channel leakage at gate-level [C]. 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). San Jose, CA, USA: IEEE, 2020: 188–196.

[118] Slpsk P, Vairam P K, Rebeiro C, et al. Karna: A gate-sizing based security aware EDA flow for improved power side-channel attack protection [C]. 2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). Westminster, CO, USA: IEEE, 2019: 1–8.

[119] KF M A, Ganesan V, Bodduna R, et al. PARAM: A microprocessor hardened for power side-channel attack resistance [C]. 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). San Jose, CA, USA: IEEE, 2020: 23–34.

发表论文和参加科研情况说明

（一）发表的学术论文

[1] **Haocheng Ma**, Max Panoff, Jiaji He, et al. EMSim: A Fast Layout Level Electromagnetic Emanation Simulation Framework for High Accuracy Pre-Silicon Verification [J]. IEEE Transactions on Information Forensics and Security. (SCI 一区，DOI: 10.1109/TIFS.2023.3239184)

[2] **Haocheng Ma**, Shijian Pan, Ya Gao, et al. Vulnerable PQC against Side Channel Analysis - A Case Study on Kyber [C]. 2022 Asian Hardware Oriented Security and Trust Symposium (AsianHOST). (DOI: 10.1109/AsianHOST56390.2022.10022165)

[3] **Haocheng Ma**, Qizhi Zhang, Ya Gao, et al. PathFinder: Side Channel Protection through Automatic Leaky Paths Identification and Obfuscation [C]. Proceedings of the 59th ACM/IEEE Design Automation Conference. (CCF-A，DOI: 10.1145/3489517.3530413)

[4] **Haocheng Ma**, Jiaji He, Max Panoff, et al. Automatic On-Chip Clock Network Optimization for Electromagnetic Side-Channel Protection [J]. IEEE Journal on Emerging and Selected Topics in Circuits and Systems. (SCI 二区，DOI: 10.1109/JETCAS.2021.3077842)

[5] **Haocheng Ma**, Jiaji He, Yanjiang Liu, et al. On-Chip Trust Evaluation Utilizing TDC-Based Parameter-Adjustable Security Primitive [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. (SCI 二区，DOI: 10.1109/TCAD.2020.3035346)

[6] **Haocheng Ma**, Jiaji He, Yanjiang Liu, et al. Security-Driven Placement and Routing Tools for Electromagnetic Side-Channel Protection [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. (SCI 二区，DOI: 10.1109/TCAD.2020.3024938)

[7] **Haocheng Ma**, Jiaji He, Yanjiang Liu, et al. CAD4EM-P: Security-Driven Placement Tools for Electromagnetic Side Channel Protection [C]. 2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST). (DOI: 10.1109/AsianHOST47458.2019.9006705)

[8] Jiaji He, **Haocheng Ma**, Max Panoff, et al. Security Oriented Design Frame-

work for EM Side-Channel Protection in RTL Implementations [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. (SCI 二区，DOI: 10.1109/TCAD.2021.3112884)

[9] Zhendong Shi, **Haocheng Ma**, Qizhi Zhang, et al. Test Generation for Hardware Trojan Detection Using Correlation Analysis and Genetic Algorithm [J]. ACM Transactions on Embedded Computing Systems (TECS). (SCI 四区，DOI: 10.1145/3446837)

[10] Honggang Yu, **Haocheng Ma**, Kaichen Yang, et al. DeepEM: Deep Neural Networks Model Recovery through EM Side-Channel Information Leakage [C]. 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). (DOI: 10.1109/HOST45689.2020.9300274)

（二）申请及已获得的专利

[1] 赵毅强，**马浩诚**，刘燕江等. 一种PCA与朴素贝叶斯分类融合的硬件木马检测方法：中国，202010423062.9.

[2] 赵毅强，**马浩诚**，刘燕江等. 基于空间电偶极子阵列的电磁侧信道建模方法：中国，201811344721.9.

[3] 赵毅强，**马浩诚**，刘燕江等. 基于EMD降噪数据预处理的硬件木马检测优化方法：中国，201811183928.2.

[4] 赵毅强，**马浩诚**，刘燕江等. 基于HHT降噪的硬件木马检测优化方法：中国，201811173119.3.

（三）参与的科研项目

[1] 嵌入式安全微处理器体系结构，国家自然科学基金重点项目. 课题编号：61832018.

[2] 纳米级芯片硬件综合安全评估关键技术研究，国家重点研发计划“网络空间安全治理”重点专项项目. 课题编号：2021YFB3100900.

致 谢

光阴荏苒，日月如梭，五年博士生涯已临近尾声。回首在天大求学的九年时光，一时之间感慨良深，在这里我学到了很多知识，认识了许多良师益友，积累了弥足珍贵的经验，并即将开启新的人生篇章。在此，向所有关心、帮助和爱护我的人致以最真诚的感谢。

首先，万分感谢我的博士生导师赵毅强教授。本论文是在赵老师的悉心指导下完成的，感谢赵老师提出的宝贵意见和建议。在攻读博士学位期间，赵老师兢兢业业地传道授业，孜孜不倦地排难解惑，不仅为我指明了科研方向，还在日常生活给予了无微不至的关怀。在赵老师的言传身教下，我学到了“仰望星空，脚踏实地”的科研精神，培养了迎难而上的工作态度，收获了立身处世的人生哲理，再次由衷感谢赵老师的悉心栽培。

同时，非常感谢金意儿教授对我的无私帮助。金老师有着开拓创新的科研态度、严谨求实的工作作风，激发了我对科学研究的持续热情。在攻读博士学位期间，有幸遇到金老师并接受到他的指导，我获得了全面的科研训练，培养了系统的科研思维，提高了科研论文写作能力，以上这些让我收获良多，在科研道路上少走了许多弯路。在此，谨向金老师表示衷心的感谢。

此外，十分感谢实验室的师兄师姐们，尤其是何家骥师兄、刘燕江师兄和辛睿山师兄，给予我非常多的鼓励和帮助，带领我完成了很多科研项目，使我能够快速适应研究生生活。还要感谢实验室同届的蔡里昂、宋凯悦、王佩瑶、甄帅、李松、赵子龙、傅晓娟、王品同学，感谢你们的陪伴和包容，让我度过了愉快的两年半时光。同时我要感谢曹宇文、石振东、李宗哲、李博文、张启智、蒯钧、赵鑫宇、王庆雅、高雅、魏鑫、刘梓潼、潘仕坚等师弟师妹们，感谢他们对实验室工作的热心协助，是你们让实验室成为温馨和睦的大家庭。

最后，特别感谢我的家人、父母对我的关爱，感谢我的爱人张探琛女士对我的支持，感谢我的爱猫三三、九九带来的快乐，你们是我最坚强的后盾，是我勇毅前行的动力，希望我的家人们健康常乐，我永远爱你们!