**华 中 科 技 大 学**

**网络空间安全学院**

《芯片安全与测试技术导论》  
课程报告

文献阅读报告

姓 名 邬雪菲

班 级 网安2104班

学 号 U202112131

联系方式 18172029686

分 数

评 分 人

2024年11月11日

**课程报告要求**

**1. 报告不可以抄袭，发现雷同者记为0分。**

**2. 报告中不可以只粘贴大段文字或代码，应是文字与图、表结合的，需要说明流程的时候，也应该用流程图或者伪代码来说明；如果发现有大段文字或代码粘贴者，报告打回重写。**

**3. 报告格式要求规范。**

**报告评分表**

|  |  |  |  |
| --- | --- | --- | --- |
| **评分项目** | **分值** | **评分标准** | **得分** |
| **论文 一** | | | |
| 论文概述 | 10 | 10-8：概述准确，包含论文发表刊物、发表时间、研究背景、目的、方法等；  7-4：基本包括上述条目，但不够具体或准确；  3-0：描述过于简单或不完整，未包含研究背景、研究目的、研究方法等 |  |
| 结构与内容分析 | 20 | 20-16：描述准确，方法分析深入，实验结果比较与分析清晰，各部分之间的逻辑关系把握正确‌；  15-9：包含上述条目，但不够具体或准确；  8-0：叙述简单，内容缺乏、不充足 |  |
| 优缺点评述 | 15 | 15-13：讨论深入，阐述研究发现的实际意义和理论价值，评价客观，优缺点论述合理‌；  12-7：基本覆盖上述内容，部分欠缺；  6-0： 仅包括优点或缺点，且描述不够具体 |  |
| 心得体会 | 5 | 5-4：体会真实具体；  3-2：体会比较空洞；  1-0：没有写什么体会 |  |
| **论文 二** | | | |
| 论文概述 | 10 | 10-8：概述准确，包含论文发表刊物、发表时间、研究背景、目的、方法等；  7-4：基本包括上述条目，但不够具体或准确；  3-0：描述过于简单或不完整，未包含研究背景、研究目的、研究方法等 |  |
| 结构与内容分析 | 20 | 20-16：描述准确，方法分析深入，实验结果比较与分析清晰，各部分之间的逻辑关系把握正确‌；  15-9：包含上述条目，但不够具体或准确；  8-0：叙述简单，内容缺乏、不充足 |  |
| 优缺点评述 | 15 | 15-13：讨论深入，阐述研究发现的实际意义和理论价值，评价客观，优缺点论述合理‌；  12-7：基本覆盖上述内容，部分欠缺；  6-0： 仅包括优点或缺点，且描述不够具体 |  |
| 心得体会 | 5 | 5-4：体会真实具体；  3-2：体会比较空洞；  1-0：没有写什么体会 |  |
| **总 分** | | | |
| **评分人** | | | |

**目 录**

**（完成报告后更新）**

**《Security analysis of logic obfuscation》**

**阅读报告**

1. **论文概述：**

《Security analysis of logic obfuscation》这篇论文的作者是美国的[Jeyavijayan Rajendran](https://ieeexplore.ieee.org/author/37542437600)，[Youngok Pino](https://ieeexplore.ieee.org/author/38232859200)，[Ozgur Sinanoglu](https://ieeexplore.ieee.org/author/37273781800)和[Ramesh Karri](https://ieeexplore.ieee.org/author/37269471300)。该论文于2012年发表在第49届年度国际设计自动化会议（DAC，Design Automation Conference）上，此会议被公认为电子设计自动化领域水平最高的四大国际会议之一。

研究背景是集成电路全球化时代，盗版、过度制造和逆向工程已经成为电子和国防工业的重要挑战。为保护知识产权，逻辑混淆技术被提出。这是一种有效保护芯片设计的安全技术，通过在芯片设计过程中插入复杂的逻辑混淆，使得攻击者难以理解和分析芯片设计，从而增强芯片安全性和抵御反向攻击，防止芯片被盗用或仿造。

本文旨在对逻辑混淆技术进行安全性分析，探寻其是否存在可利用的攻击漏洞并尝试提出解决方案。对于2008年提出的逻辑混淆技术EPIC，文章存在安全漏洞，攻击者可以通过使密钥值对输出敏感，在与键数成线性的时间内破译混淆的网表。并且，论文中针对该漏洞开发出了一种修复技术，使混淆在插入的键数量上真正呈指数级增长，由此防范密钥位破译。论文通过理论分析和实验验证来评估逻辑混淆技术的有效性并提出防御方案，结论具有说服力。

1. **结构与内容分析：**

**2.1 结构分析**

论文遵循经典的引言、方法和结论三段式结构，分为六个章节书写。

第一部分是引言，本文使用一个章节的篇幅来叙述，并使用漏斗型逻辑，从集成电路全球化发展的大背景入手，将其中的芯片设计盗版问题作为研究动机，并逐渐由大到小书写，先介绍逻辑混淆技术，再讨论可能的攻击方式和更完善的技术方案，由此聚焦到论文涉及的核心问题，即逻辑混淆技术的安全性分析，最终总结文章的贡献。这部分内容结构清晰，详略得当，旨在通过较短的篇幅让读者对该论文的工作有一个整体把握和了解，由此在清晰思路的引领下进一步阅读后文的研究细节。

第二部分是方法，分为攻击策略、强逻辑混淆、结果共三个章节。论文先理论分析了逻辑混淆技术存在的漏洞，并提出了一种利用该漏洞的攻击方案，由此证明该技术存在安全隐患；进一步，论文又提出了一种强逻辑混淆方案，该方案有效地修补了上一章提到的漏洞；最后，论文列出了详细的实验结果。该部分内容逻辑严密，层层递进，旨在通过系统的分析和实验验证，展示逻辑混淆技术的脆弱性以及提出的改进方案的有效性。这种结构不仅有助于读者理解逻辑混淆技术的复杂性，也为后续的讨论和结论部分奠定了坚实的基础。

最后一个部分是结论，分为相关工作和结论两个章节。此部分篇幅较短，先是回顾了其他与逻辑混淆技术安全分析相关的研究工作，然后讨论了论文的贡献，并指出了逻辑混淆技术的局限性和研究方向。论文的该部分内容上稍有不足，更像是为了完善结构性书写的篇章。

三个部分相辅相成，先由引言提供研究的背景和动机，为后续的技术细节和分析结果奠定基础，接着在之后的几个章节中详细展开理论和技术细节，最后做总结，文章结构布局完整。

**2.2 内容分析**

第一章引言，首先设定了研究的背景，即集成电路设计的全球化趋势，以及由此带来的知识产权保护挑战。论文强调了盗版、逆向工程和硬件木马等问题的严重性，并指出了这些问题对电子和国防工业的影响。接着，引言部分介绍了逻辑混淆技术作为一种保护芯片设计安全的技术，其通过在芯片设计中插入复杂的逻辑门来防止攻击者理解和分析芯片设计。最后，引言部分明确了本文的研究目的：对逻辑混淆技术的安全性进行分析，并探索可能的攻击漏洞及解决方案。

第二章攻击策略，这一章节详细介绍了攻击者可能采用的策略来破解逻辑混淆技术。论文首先分析了逻辑混淆技术的潜在漏洞，并提出了一种攻击方案，该方案通过特定的输入模式观察输出，从而破译密钥。这一章节的核心在于展示了逻辑混淆技术的脆弱性，并证明了攻击者可以在与密钥数量成线性的时间内破译混淆的网表。

第三章强逻辑混淆，在确认了现有逻辑混淆技术的漏洞后，论文在这一章节提出了一种改进的强逻辑混淆方案。这种方案通过在设计中插入具有复杂干扰的密钥门来增强安全性，使得攻击者难以通过简单的方法破译密钥。论文详细描述了如何构建干扰图来分析密钥门之间的干扰，并基于此图来插入密钥门，以最大化非可变边缘的数量。

第四章实验结果，实验部分展示了使用ISCAS-85组合基准电路对不同逻辑混淆技术的实验结果。论文比较了随机插入、无连续门插入、未加权插入和加权插入四种不同的逻辑混淆技术，并展示了它们的有效密钥大小、测试模式数量、面积开销和功耗-延迟乘积等关键指标。这一章节通过实验数据验证了强逻辑混淆技术的有效性，并与现有技术进行了比较。

第五章是相关工作，论文补充了对另一类逻辑混淆技术即顺序混淆的安全性分析，并提到逻辑混淆插入记忆元件带来的显著的额外性能开销。

第六章是结论，总结了本文的主要发现和贡献，并指出了集成电路自身设计的局限性使得攻击者通过仅控制输入和观察输出就能窥探电路设计，不过，防御者也可以从攻击方式中研究应对方案，为后续研究提供了思路。

1. **优缺点评价：**

论文的优点如下：

首先是创新性。论文提出了一种新的逻辑混淆技术，通过构建干扰图来分析和设计逻辑混淆，提高了集成电路设计的安全性。其次是研究方法的严谨性。论文通过理论分析和实验验证相结合的方法，全面评估了逻辑混淆技术的有效性。最后是论证的合理性。论文通过对比不同逻辑混淆技术的性能开销和安全性，合理地论证了加权插入技术的优势。

当然，论文也存在着一些缺点。论文研究的内容存在一定局限性，论文主要关注了组合逻辑混淆，对于时序逻辑混淆的安全性分析不足。此外存在研究方法不足的问题，虽然论文提出了基于干扰图的逻辑混淆技术，但对于如何自动化这一过程的讨论不够充分。并且论证不充分，在讨论逻辑混淆技术的性能开销时，未能充分考虑不同应用场景下的实际需求，可能存在一定的局限性。最后，文章的书写方面有一些缺陷，第五章相关工作和第六章结论内容不够充实。

1. **心得体会：**

通过阅读这篇论文，我对集成电路设计的安全性问题有了一个基本了解。特别是在全球化的背景下，如何保护知识产权和防止非法复制成为了一个重要课题。逻辑混淆技术作为一种有效的硬件安全技术，其安全性分析对于提高集成电路设计的安全性具有重要意义。论文提出的基于干扰图的逻辑混淆方法，不仅提高了设计的安全性，也提供了一种新的视角来思考如何设计更安全的硬件系统。此外，论文中针对攻击者思维进行防御方案设计的思路也值得应用到其他领域。然而，论文也存在一些局限性，例如对于时序逻辑混淆的讨论不足，以及对于自动化设计过程的探索不够深入。这篇论文不仅增进了我的专业知识，也为未来的研究工作提供了宝贵的启示。

**《Quantum Physical Unclonable Functions: Possibilities and Impossibilities》 阅读报告**

1. **论文概述‌：**

**2、论文结构与内容分析‌：**

**2.1 结构分析**

**2.2内容分析**

**3、优缺点评价‌：**

**4、心得体会‌：**

|  |
| --- |
| 原创性声明 |
| 本人郑重声明本报告内容，是由作者本人独立完成的。有关观点、方法、数据和文献等的引用已在文中指出。除文中已注明引用的内容外，本报告不包含任何其他个人或集体已经公开发表的作品成果，不存在剽窃、抄袭行为。  已阅读并同意以下内容。  判定为不合格的一些情形：  （1） 请人代做或冒名顶替者；  （2） 替人做且不听劝告者；  （3） 报告内容抄袭或雷同者；  （4） 报告内容与实际实验内容不一致者；  （5） 代码抄袭者。  **作者签名：** |