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 7 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

《Security analysis of logic obfuscation》 阅读报告 1
1、 论文概述： 1
2、 结构与内容分析： 1
2.1 结构分析 1
2.2 内容分析 2
3、 优缺点评价： 3
4、 心得体会： 4
《Quantum Physical Unclonable Functions: Possibilities and Impossibilities》 阅读报告 5
1、 论文概述： 5
2、 论文结构与内容分析： 5
2.1 结构分析 5
2.2 内容分析 7
3、 优缺点评价： 8
4、 心得体会： 9

《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，Youngok Pino，Ozgur Sinanoglu 和 Ramesh Karri。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。

2、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，即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。

3、优缺点评价：

作为一篇被权威会议接收的论文，该论文不乏优点。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。

4、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，例如对于顺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：

《Quantum Physical Unclonable Functions: Possibilities and Impossibilities》这篇论文的作者是 Myrto Arapinis, Mahshid Delavar, Mina Doosti 和 Elham Kashfi，该论文于 2021 年发表于量子科学期刊《Quantum》上，属于 SCI Q1 区。论文主要从量子物理角度对 PUFs 进行拓展研究。

研究背景是量子技术发展时代下，量子计算机的计算能力不断提升，传统的物理不可克隆函数（PUF）面临着新的挑战。量子 PUF（qPUF）作为一种新型的安全技术，利用量子状态的不可克隆性来增强安全性。

本论文的研究目的是全面研究量子物理不可克隆函数（qPUFs），定义 qPUFs，并探讨其在量子密码学工具中的安全性级别，以及它们在实际应用中的潜力和局限性。

研究方法如下所述：论文通过形式化定义 qPUFs，引入量子游戏框架来定义不同级别的安全性，包括量子指数不可伪造性、量子存在不可伪造性和量子选择不可伪造性。同时，论文提出了一种基于通用量子仿真算法的新的量子攻击技术，并证明了没有 qPUF 能提供量子存在不可伪造性。另一方面，论文证明了一大类 qPUF（称为酉 PUFs）可以提供量子选择不可伪造性，这是大多数基于 PUF 应用所需的安全级别。

2、论文结构与内容分析：

2.1 结构分析

论文遵循了典型的科研论文结构，依然是三段式的叙述方式，由引言引入，再使用量子仿真算法和量子物理不可克隆函数两个章节详细介绍方法，最后结论部分讨论和展望。其逻辑关系和整体结构清晰有序，各个部分相互关联层层递进，逻辑严谨，共同支撑起论文的研究主题和结论。

引言部分作为论文的开篇，承担着引入研究背景、明确研究动机和目标的重要作用。论文首先指出了物理不可克隆函数（PUF）在传统安全领域的应用和局限性，随后引入量子技术的发展对 PUFs 带来的新挑战和机遇。这一部分为读者提供了研究的背景知识，同时引出了量子物理不可克隆函数的概念，为后续章节的深入讨论奠定了基础。

第二章量子仿真算法，详细介绍了量子仿真算法，这是分析 qPUFs 安全性的关键工具。论文通过描述量子过程学习工具的原理和应用，为读者展示了如何利用量子技术来模拟和分析未知的量子过程。这一部分不仅为非专业读者提供了必要的技术背景，也为后续的安全性分析提供了理论基础。

第三章是量子物理不可克隆函数。在这一章中正式定义了 qPUFs，并提出了 qPUFs 应满足的基本要求，包括鲁棒性、唯一性和抗碰撞性。这些要求是评估 qPUFs 安全性的基础，也是后续安全性分析的前提。这一部分的逻辑关系在于，它建立了 qPUFs 的理论框架，并为实验和安全性评估提供了标准。同时，本章对 aPUF 进行了安全性分析，这是论文的核心部分。论文通过量子游戏框架来定义不同级别的安全性，并对 qPUFs 进行了详细的安全性评估。这一章节将前文提出的理论要求与实际的安全威胁相结合，通过具体的分析来验证 qPUFs 的安全性。这一部分的分析结果直接影响到论文的结论和未来研究方向的提出。

最后是讨论和未来工作。论文总结了 qPUFs 与其他类型的 PUFs 的关系，并提出了未来研究的方向。这一部分的逻辑关系在于，它不仅回顾了论文的主要发现，还指出了 qPUFs 在实际应用中可能面临的挑战和未来的改进空间。这一部分为读者提供了一个全面的视角，帮助他们理解 qPUFs 的潜力和局限性，为整篇论文画上了句号。

整体来看，这篇论文的结构严谨而有序，每个部分都紧密相连，共同构建了一个完整的研究故事。从引言到结论，每个部分都在逻辑上承接前文，为后续内容做铺垫，使得整篇论文的论述流畅而有说服力。通过这样的结构安排，作者不仅成功地传达了 qPUFs 的概念和重要性，也为读者提供了一个清晰的研究路径，使得论文的研究成果和观点具有较高的可信度和影响力。

2.2 内容分析

第一章引言部分为读者提供了论文的研究背景、目的和意义。在集成电路全球化发展的背景下，集成电路设计的安全性问题日益凸显，尤其是知识产权保护方面。由于制造过程中的随机物理变化，PUFs 能够提供独特的硬件特征，这些特征难以被克隆，从而成为一种安全的身份验证手段。随着量子技术的发展，量子态的不可克隆性为 PUF 提供了新的实现可能，即量子 PUF（qPUF）。论文的研究目的是对 qPUF 进行全面的研究，包括其定义、安全性要求和潜在的量子攻击技术。研究意义在于，qPUF 可能为基于硬件的安全协议提供更强的安全保障，尤其是在面对量子计算机威胁时。

第二章量子仿真算法和第三章量子物理不可克隆函数部分详细介绍了论文提出的 qPUF 概念和安全性分析框架。作者首先定义了 qPUF 作为量子信道，并提出了 qPUF 应满足的基本要求，包括鲁棒性、唯一性和抗碰撞性。接着，作者使用量子游戏框架定义了 qPUF 的三种安全性概念：量子指数不可伪造性、量子存在不可伪造性和量子选择不可伪造性。这些概念捕捉了不同攻击模型下 qPUF 的安全性。此外，作者介绍了一种基于通用量子仿真算法的量子攻击技术，用于证明没有 qPUF 能提供量子存在不可伪造性。最后，作者证明了酉 PUFs 可以提供量子选择不可伪造性，这是大多数基于 PUF 应用所需的安全级别。实验部分展示了 qPUF 的安全性分析结果。作者使用 ISCAS-85 组合基准电路作为实验平台，通过量子测试工具确定用于静音和传播密钥的输入模式。实验比较了随机插入、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。实验结果显示，加权插入技术在提高安全性方面最为有效，但同时也带来了较大的性能开销。具体来说，实验数据包括有效密钥大小、测试模式数量、面积开销和功耗-延迟乘积等关键指标。这些结果通过图表和数据分析的形式呈现，为读者提供了直观的比较和理解。

最后一章是讨论与结论，总结了论文的主要发现和贡献，并指出了 qPUF 的局限性和未来研究方向。论文中强调，尽管 qPUF 在理论上提供了一种新的安全机制，但在实际应用中仍面临许多挑战，如量子记忆的需求和量子攻击的可行性。此外，论文提出了未来研究的方向，包括 qPUF 的具体实现、非酉 qPUF 的研究

以及量子攻击技术的发展。最后，论文强调了在量子时代保护硬件安全的重要性，并呼吁更多的研究来探索 qPUF 的潜力和限制。

3、优缺点评价：

本论文具有较多优点。首先是创新性方面，它首次全面地研究了量子物理不可克隆函数（qPUFs），并提出了量子密码学工具中的 qPUFs 的正式定义。这一定义不仅包含了传统 PUFs 的所有要求，还引入了量子设置中特有的测试性特征，为量子安全研究提供了新的视角和工具。此外，论文通过量子游戏框架来定义 qPUFs 的不同安全级别，并使用量子攻击技术来分析 qPUFs 的安全性。这种方法不仅理论上具有创新性，而且为实际的量子安全协议设计提供了指导。论文中提出的量子攻击技术，特别是基于通用量子仿真算法的攻击，展示了量子计算能力如何影响 qPUFs 的安全性，这对于理解和预测未来量子技术在安全领域的应用具有重要意义。并且，论文通过详细的理论分析和数学证明，建立了 qPUFs 的安全性界限。这些界限不仅有助于理解 qPUFs 在面对量子攻击时的脆弱性，还为设计更安全的 qPUFs 提供了理论基础。

当然，论文也存在着一些局限性。比如篇幅较长不利于非专业领域读者阅读等等。虽然论文在理论上提供了 qPUFs 的安全性分析，但实际的 qPUFs 构造和实现仍然是一个开放的问题。论文中提出的安全模型和攻击技术需要在实际的量子设备上进行验证，这可能需要克服当前量子技术的局限性。其次，论文主要关注了 qPUFs 的理论分析，对于 qPUFs 在特定应用场景中的性能和实用性的讨论不够充分。例如，qPUFs 在实际硬件中的集成、量子记忆的需求以及与其他安全协议的兼容性等问题，都需要进一步的研究。最后，论文在讨论 qPUFs 的安全性时，主要关注了量子攻击的可能性，而对于量子攻击的实际可行性和成本效益的分析不足。这可能会影响到 qPUFs 在实际安全协议中的应用，因为实际的攻击者可能会基于成本效益来选择攻击策略。因此，未来的研究需要更加全面地考虑 qPUFs 在实际应用中的安全性和效率。

4、心得体会：

通过阅读这篇论文，我对量子物理不可克隆函数有了一个简单的了解。论文不仅介绍了 qPUFs 的概念和理论基础，还分析了它们的安全性和应用潜力。这让我认识到量子技术在硬件安全领域的重要作用，以及 qPUFs 在保护知识产权和防止非法复制方面的潜力。此外，论文也指出了 qPUFs 在实际应用中可能面临的挑战。

不过，本论文的篇幅较长，且量子科学的加持让我一个非专业研究者阅读起来稍有困难，需要较多时间梳理，对整篇论文的理解仍有许多不清晰的地方。这也让我又一次意识到自己所学所知的局限性，无论是学习广度和深度上都有很大的欠缺，应当继续不断虚心求学，在广阔的专业知识海洋中汲取更多的智慧。

随着量子计算的发展，传统的加密方法面临着前所未有的挑战，而 qPUFs 作为一种基于物理特性的安全技术，提供了一种可能的解决方案。它们的独特性和不可克隆性为硬件安全提供了新的保护机制，这对于保护关键基础设施、确保通信安全以及防止敏感信息泄露等方面具有重要意义。论文中对于 qPUFs 安全性的深入分析，让我对量子安全技术有了更全面的认识。特别是在面对量子攻击时，qPUFs 的某些特性可能使其比传统方法更为安全。

总之，这篇论文不仅增进了我对 qPUFs 的理解，也让我对网络安全的未来发展有了更深的思考。我将继续努力学习，以便在未来的安全领域中发挥积极作用。

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：