北京大学攻读硕士学位研究生选题报告审核表

（本表先由硕士生在校内门户填写有关内容后打印，由指导教师、考评小组签署意见后，一式一份存学校档案）

院、系：信息科学技术学院　　专　业：微电子学与固体电子学

姓　名：唐文懿　　导师姓名：贾嵩

学　号：1301214150

选题报告完成时间：　2015年10月10日

拟定学位论文题目：　物理不可克隆函数的建模攻击和防御策略研究

本人陈述：	（选题来源、研究意义、国内外研究状况、主要研究内容、拟采取的研究方法、预期研究结果和论文写作计划等）

一、选题来源、研究意义及国内外研究现状

信息安全是IC产业的重要研究方向之一，关系到个人、企业、甚至国家的利益。硬件安全是近几十年来新兴的研究热点，随着反向工程、功耗分析、错误注入分析等手段的进步和成熟，如何在硬件层面上防范上述攻击有着不同的研究进展。

密钥是保密芯片的关键数据，当下无论是对称密码系统（如AES）或者是非对称密码系统（如RSA）均需要在本地保留密钥副本，目前密钥主要存储在非易失性存储器中，而一旦芯片被入侵者获取（比如偷盗、捡拾等），由于非易失性存储器易被反向探查获取密钥，会造成用户资料、财产的损失，因此如何安全的保存密钥是密码学和系统设计中的一个关键问题，随机密钥遂应运而生。

2001年MIT的Pappu Srinivasa Ravikanth在其毕业论文中提出了物理不可克隆函数（Physically Unclonable Function, PUF），是一种基于物理现象产生单向映射的想法；2002年MIT的Gassend等人提出了用集成电路实现的PUF结构，由此诞生了硅基PUF研究领域；经过几年缓慢发展，2007年之后开始受到各项顶级会议和期刊的重视，该领域发表文章数逐年增多，有越来越多的研究者参与进来。

PUF定义为这样一类映射：单一PUF将输入（n bits）映射到输出（往往1 bit），映射方式由结构决定；而基于同一结构的不同PUF之间的映射由于物理上的随机性（基于某些现在不可知的过程）而不同。硅基PUF利用集成电路制造工艺的不确定性，即工艺波动，使得人为不能判断其电路的确切输出，即便知道了原电路详细的设计，也不能制造出完全一样的电路。利用这一特性，PUF可被应用在密钥生成、伪随机种子生成、芯片认证、IP保护、保密通信等多个领域。

PUF可以分为弱PUF和强PUF两类。其中弱PUF是指输入-输出对（CRP）很少的结构，它仅有有限个CRP，激励过程比较隐私，没有对外输入的接口，弱PUF可以应用于单一密钥及芯片ID的生成等；强PUF指具有极大量CRP的结构，有对外输入的接口，外界通过输入激励获取响应，强PUF多用于认证、保密通信等。

PUF在芯片失陷时也能保证信息安全：以强PUF为例。首先，入侵者不可能获取全部的CRP（计算能力有限），仅通过可以枚举的有限CRP，不能推断出剩下的CRP关系，所以对认证过程不构成威胁；其次，若入侵者想反向芯片，则必然造成电路电气特性的改变，使之不再产生相同的响应，破坏了原有的电路系统，因此不能得到有效信息。

目前国内外对于PUF的研究都处于起步与探索阶段，主要集中于高可靠性PUF结构、低功耗小面积PUF结构、应用协议开发和安全性分析等问题。其中MIT的Lim的毕业论文《Extracting Secret Keys from Integrated Circuit》提出了一种采用模式识别的算法，可以推断出强PUF输入与输出的映射关系，从而复制PUF，后研究者将这种攻击称为建模攻击（Modeling Attack），并利用机器学习的相关知识对已知的多种PUF结构进行建模和分析。目前建模攻击是强PUF在安全性能上的主要威胁。在国际文献中，已经对经典结构（Arbiter PUF及其衍生类型，RO-PUF）进行了建模攻击研究并成功抽象出物理模型；另一方面针对建模攻击的威胁，也提出了提高安全性的方案，比如增加前馈路径、采用多路异或等。而由于PUF历史较短，国内目前在PUF建模攻击及防范上的研究几乎是一片空白，本人的毕业论文旨在对新型PUF的建模和安全分析上填补国内研究的空缺。

二、主要研究内容

论文主要针对强PUF结构进行研究。

经典结构包括Arbiter PUF、RO PUF和SRAM PUF。

Arbiter PUF比较两路信号的延迟，延迟的差异来自于工艺涨落，通过一个D触发器采样，若上路数据信号先于下路时钟信号到达，则输出1，反之输出0；RO PUF比较两个相邻环振的振荡周期，用计数器计算振荡次数，当两个计数器不相等时比较大小，输出0或者1；SRAM PUF比较SRAM单元中耦合反相器的驱动能力，在上电伊始确定单元会驱动哪一侧节点下拉，以单侧节点的电压作为输出。

这三种结构各有优劣。Arbiter PUF占用面积小，CRP空间大，但是易被建模，安全性较差；RO PUF稳定性高，易用FPGA实现，但是占用面积大，CRP空间相对较小，熵值低；SRAM PUF可集成在成熟SRAM中，因此可视为几乎不占用额外面积，CRP随SRAM大小而定，但整体较小，容易被枚举，且稳定性不高，易翻转。

与这三种结构相比，一种新型强PUF结构Bistable Ring PUF（BRPUF）具有更多优点。BRPUF是在2011年H.O.S.T.会议上由慕尼黑工业大学的Qingqing Chen提出的，它采用偶数级反相器链构成环路，以环路的两种状态（0-1-0-1和1-0-1-0）作为激励的响应，其输入则是从两个与非门中选出其一接入环路中，不同与非门的接入可造成电路收敛于不同的状态，对于N bit输入的BRPUF，总共有2^N个CRP。当前对于BRPUF有两组研究文献，分别用单层神经网络（ANN）对进行输出预测和用FPGA统计输入输出。本论文基于前人研究成果，深入分析BRPUF的响应机理，提出了基于延迟时间的电路模型。该模型能够准确描述BRPUF的响应过程，基于此模型的模式识别算法可使对BRPUF的输出预测率达到95%以上。论文详细给出了该模型的推导过程。

为了改进BRPUF的不良结果，论文继续提出了改进型PUF结构，提出的结构综合了Arbiter PUF和BRPUF的优点，利用级联交换器代替与非门在环路中的延迟路径，降低BRPUF的系统偏移，改进了PUF的分布结果；论文同样给出了改进型PUF的模型，模式识别算法对于此模型并不能很好的预测输出结果，经过1000对CRP的训练，对32 bit 新PUF的预测率最高不超过87%。

三、拟采取的研究方法

采用HSPICE与FPGA交替仿真的方法，通过HSPICE模拟低Bit PUF的所有节点电压特性，利用FPGA测试32 bit的实时响应。收集的数据按CSR格式存储，通过Matlab编写脚本加以分析，Matlab中自带支持向量机（SVM）的训练和预测函数，用以拟合超平面表达式。

PUF的结果需要统计分析，因此需要借助脚本语言自动化辅助仿真。在仿真低Bit PUF时，采用Monte Carlo方法，在SMIC 40nm工艺制程下仿真，取仿真次数为1000，自动采样输出接点电压，通过特定算法判断电路输出。在用FPGA实现高Bit PUF时，用多个FPGA下载同样的SOF文件，同时在单FPGA上实现多PUF单元，用于模拟晶圆不同位置之间的工艺偏差。为了使FPGA中布线结果尽可能平衡，用Quartus II中的Logiclock功能将元件锁定在指定LAB，指定LAB位置的参数由Python脚本程序生成并输入给Quartus II。所有FPGA采用同一电压、同一室温，以杜绝PVT变化的干扰。同时也在同一FPGA上实现了BRPUF和Arbiter PUF，以作对比。

最后将收集到的数据按统一格式处理，输入到Matlab程序中，Matlab对数据进行计算，得到分布结果并拟合SVM超平面，最后用拟合结果对数据进行分类，将分类结果与FPGA和仿真结果对比得到预测率。

由于实验条件限制，FPGA电路不能提供电压、温度的波动测量，因此PVT特性主要由HSPICE仿真产生数据。

四、预期研究结果

PUF的设计指标如下：

独立性应为不同硅片之间若干长度回应码串之间汉明距离与码串长度的商符合N~(0.5,<0.1)的正态分布；均匀性应为单一硅片内任意激励组对应回应码串的汉明距离与码串长度的商符合N~(0.5,<0.1)的正态分布；稳定性应使使用环境下的误码率低于1%；安全性应使入侵者不能在有限时间内推断出CRP的模型。

根据模型推断，BRPUF的独立性和均匀性会偏离0.5均值，其安全性在本论文为BRPUF总结的模型下能够使预测率超过95%；而本论文设计的PUF结构应具有理想的片内和片间分布，其均匀性和独立性的统计结果应符合均值50%，方差小于0.1的正态分布，能够在1%的电压波动，10%的温度波动下，误码率应低于1%。

五、论文写作计划

论文以实验为主，尊重实验数据，写作计划安排如下：

2015年10月——2015年12月，进行电路仿真、测试、数据收集；

2015年12月——2016年2月，进行数据统计分析，主要针对已有数据进行分析，判断是否与理论吻合，否则找出问题所在；其次从实验结果中总结规律，发现提出结构的不足之处，并分析有无改进的余地；

2016年2月——2016年4月，总结工作，撰写论文。利用最后两个月的时间梳理知识脉络，完成毕业论文。

本人签名：　　年　　月　　日

指导教师对选题报告的意见：

信息安全是IC产业的重要研究方向，物理不可克隆函数（PUF）的建模和安全分析研究在国内尚属空白，唐文懿同学以此作为毕业论文选题，具有较好的理论意义和实用价值；论文工作从PUF的原理分析、优缺点比较，到提出一种基于延迟时间的电路模型和一种改进型PUF结构，最后进行HSPICE仿真、FPGA测试和数据统计分析，工作量充足，工作计划可行。

同意开题。

指导教师签名：　　年　　月　　日

选题报告考评小组	姓名	职称	所在单位	签字
成员 1	吉利久	教授	北京大学信息科学技术学院	
成员 2	何燕冬	教授	北京大学信息科学技术学院	
成员 3	贾嵩	副教授	北京大学信息科学技术学院	

考评小组意见：

该生的论文选题来源于实际需求，具有较好的理论意义和实际应用价值。工作量充足，满足硕士学位要求，工作计划切实可行。

同意开题。

考评小组成员签名：

年　　月　　日