附件：

大学生主题创新区创新项目发布

## 一、主题创新区介绍

集成电路硬件安全主题创新区依托南京航空航天大学新兴集成电路与系统（EICAS）实验室设立。本主题创新区拥有以国家特聘教授、万人计划领军人才、国家优青等为核心的高水平师资团队。主题创新区聚焦集成电路设计领域，研究方向主要包括新兴计算芯片、密码芯片等，近年来取得了一批具有自主知识产权的标志性科研成果。本创新区也拥有丰厚的创新创业培养基础，注重培养学生的专业能力与综合素养，拥有完善的培育体系与经验丰富的指导老师，指导学生多次获得过“互联网+”、“挑战杯”等国家级重点赛事的最高奖项。

## 二、课题介绍（仅供参考，表格格式可修改）

|  |  |
| --- | --- |
| **课题一** | |
| 指导教师： | 崔益军 |
| 项目名称： | 高性能自动化可信安全硬件自动化测试平台 |
| 项目来源： | 教师纵向科研项目 |
| 项目简介： | 通过cypress芯片，实现上位机对Xilinx系列FPGA程序配置。便携上位机程序，实现FPGA配置文件对目标FPGA阵列的自动编程，从而实现可信安全硬件的自动化测试。 |
| 学生要求： | 了解verilog硬件设计语言，熟悉FPGA的开发应用；掌握MCU编程，开发温控单元。 |

|  |  |
| --- | --- |
| **课题二** | |
| 指导教师： | 王成华 |
| 项目名称： | 基于FPGA的Saber公钥加密方案电路设计与实现 |
| 项目来源： | 教师纵向科研项目 |
| 项目简介： | 熟悉Verilog硬件设计语言，掌握Vivado套件工具的使用。能够独立编写测试台文件调试设计代码，以及时钟约束文件使整体时序收敛。设计Saber公钥加密方案的各个分立电路模块，理解最影响Saber整体性能的模块。重点设计多项式乘法和哈希函数。 |
| 学生要求： | 熟悉Verilog硬件设计语言，掌握Vivado套件工具的使用。能够独立编写测试台文件调试设计代码，以及时钟约束文件使整体时序收敛。 |

|  |  |
| --- | --- |
| **课题三** | |
| 指导教师： | 刘伟强 |
| 项目名称： | 基于CMOS技术的高可靠性PUF电路设计及实现 |
| 项目来源： | 教师纵向科研项目 |
| 项目简介： | 学习基于CMOS技术的PUF电路的设计思路与改进方案，总结电路存在的问题以及优化的方法，建立基于模拟/混合信号PUF数学模型数据库，设计基于CMOS技术的高可靠性PUF电路结构。 |
| 学生要求： | 掌握CMOS集成电路设计知识，学习PUF设计的相关知识以及Cadence，Matlab，Vivado等相关仿真软件的使用。 |

|  |  |
| --- | --- |
| **课题四** | |
| 指导教师： | 崔益军 |
| 项目名称： | 基于FPGA的处理器PUF设计与实现 |
| 项目来源： | 教师纵向科研项目 |
| 项目简介： | 学习常见物理不可克隆函数（PUF）电路结构，掌握PUF的各项评估指标；在RISC-V等处理器架构上，设计并实现高性能的处理器PUF。 |
| 学生要求： | 熟悉Verilog硬件语言设计，掌握Vivado工具使用。了解Xilinx Spartan6 FPGA 逻辑单元排布以及文件约束控制。 |

|  |  |
| --- | --- |
| **课题五** | |
| 指导教师： | 崔益军 |
| 项目名称： | AES算法高效硬件实现及侧信道攻击研究 |
| 项目来源： | 教师纵向科研项目 |
| 项目简介： | AES 算法集合了安全性、高效性和灵活性等多种优势，目前依然是对称密码体制中应用最广泛的密码算法之一，本课题研究基于FPGA的AES算法的高效硬件实现，并利用侧信道攻击等方式评估其安全性。 |
| 学生要求： | 熟悉Verilog硬件语言设计，掌握Vivado、ISE等工具的使用；理解AES算法的加解密流程和软件实现方法。 |

|  |  |
| --- | --- |
| **课题六** | |
| 指导教师： | 周玉斐 |
| 项目名称： | 应用于运动健康管理的能量采集系统 |
| 研究方向： | 微能量采集技术 |
| 项目简介： | 环境能量采集技术利用环境中的机械能、太阳能、热能等能量转换产生电能，具有能量来源广泛、能源清洁等特点，且环境能量采集器随着MEMS技术的进步，呈集成化、智能化发展趋势，在微电子系统如可穿戴电子设备上的研究得到重视。同时随着物联网的发展，无线传感器节点（WSN）的供能设备也急需推进，可见环境能量采集系统作为微小功率供能系统成为一大热点。但环境能量采集器具有能量来源不稳定、能量转换收集效率低等缺陷，目前还没有得到普遍应用。  本课题将针对人体运动过程中的压电振动能进行采集，设计出适用于健康管理的能量采集系统，提供无线传感器电能，测量人体运动时的心率温度等参数。该系统通过设计能量管理电路和控制方式，最大程度地将人体运动过程中的振动能转换为电能为WSN提供能源。 |
| 学生要求： | 建模分析以及方案论证 |
| 电路设计、仿真 |
| 程序设计、电路调式 |
| 报名方式： | （联系方式）13813990850  （邮箱）zhouyf@nuaa.edu.cn  （办公室）院楼416 |

|  |  |
| --- | --- |
| **课题七** | |
| 指导教师： | 周玉斐 |
| 项目名称： | 多负载感应式无线电能传输系统 |
| 项目来源： | 无线能量传输 |
| 项目简介： | 无线电能传输技术(Wireless Power Transmission,WPT)凭借其灵活、方便、干净等优点得到了快速的发展，无线电能传输技术与其他领域的结合更是推动了电源技术及其相关领域的科技进步。作为一种安全、可靠、灵活的供电方式，无线电能传输技术的引入，促进了各类电子设备无线充电功能的研制。  作为WPT技术中最常用的一种技术，感应式电能传输技术(The Inductively Coupled Power Transfer Technology，ICPT）利用电磁感应原理实现电能传输。与传统的变压器结构相比，它们的感应耦合磁路分开，初、次级绕组分别绕在不同的磁性结构上，不需要机械连接进行能量耦合传输，不仅消除了传统变压器会带来的摩擦触电等危险，还大大提高了系统电能传输的灵活性，减小了系统的体积重量。  本课题采用ICPT技术实现，在单个发射线圈的情况下，设计出接收端为两个工作在不同频率下的负载且接收端功率高效可控的方案，并对所设计系统进行分析，在满足功率可控的情况下并保证能量传输系统的效率，对整个系统结构进行优化设计。本课题提出了工作在不同频下一对多的无线充电策略，使得无线充电系统中负载的自由度更高，应用面更广。 |
| 学生要求： | 需要2-3名学生，熟练掌握数字逻辑电路、模拟线路、电子线路等专业课知识。主要负责电路设计以及软件的仿真。 |
| 报名方式： | （联系方式）13813990850  （邮箱）zhouyf@nuaa.edu.cn  （办公室）院楼416 |

## 三、报名组队事宜

选题方式：个人报名

联系人：崔益军，周玉斐老师指导项目可直接联系周老师

QQ群：179323608

