

软件工程实践课题（2020）

- 1. 题目：**Python虚拟机设计与实现（指导老师：华保健）

背景：Python是一个动态类型语言，其解释器是一个基于栈式字节码的抽象机器。

目标：本项目拟实现一个新的研究型的Python虚拟机，探索支持动态类型语言的虚拟机的设计与实现技术。

要求：对虚拟机设计与实现的一般原理感兴趣；熟悉Python、C语言。（2人）
- 2. 题目：**Python的C语言本地方法接口的安全性研究（指导老师：华保健）

背景：Python的C本地方法接口容易出现安全性问题，已经被大量研究过。

目标：探索Python的C语言本地方法接口的安全性，提出安全解决方案，构造原型系统。

要求：能够熟练阅读相关英文文献；熟悉Python、C语言。（2人）
- 3. 题目：**支持RISC-V的寄存器分配器的研究与实现（指导老师：华保健）

背景：RISC-V是一个新的开放硬件平台，具有一定的前瞻性和技术优势；如何对RISC-V提供更好的编译器支持，以便最大化使能芯片性能，是一个有挑战性的课题。

目标：探索各种寄存器优化算法在RISC-V架构上的实现，并完成性能评测与比较。

要求：能够熟练阅读相关英文文献；对编译器、算法、指令集等有深入理解；愿意学习图论、线性规划、非线性优化等相关知识；熟悉某种函数式编程语言。（2人）
- 4. 题目：**基于模糊测试的智能合约漏洞挖掘工具（指导老师：华保健）

背景：智能合约在区块链平台上大受欢迎，尤其在全球市值第二的以太坊上使用最为广泛，但同时也越来越受到黑客的关注，已造成数十亿美金的损失，智能合约的安全性已刻不容缓。

目标：搭建智能合约库，搭建智能合约漏洞库，并实现智能合约漏洞挖掘工具开发。

要求：对模糊测试、以太坊智能合约有一定的了解；熟悉Haskell、Python、Solidity语言；对智能合约安全感兴趣；有一定的项目经验；（2-3人）
- 5. 题目：**基于符号执行的智能合约漏洞检测工具（指导老师：华保健）

背景：智能合约在区块链平台上大受欢迎，尤其在全球市值第二的以太坊上使用最为广泛，但同时也越来越受到黑客的关注，已造成数十亿美金的损失，智能合约的安全性已刻不容缓。

目标：搭建智能合约库，搭建智能合约漏洞库，并实现智能合约检测工具开发。

要求：对符号执行、以太坊智能合约有一定的了解；熟悉Python、Solidity语言；对智能合约安全感兴趣；有一定的项目经验；（2-3人）
- 6. 题目：**基于符号执行的Qt代码路径覆盖测试生成工具（指导老师：华保健）

背景：Qt是一款基于C++的开源的跨平台GUI框架，目前国内大量应用于核工业、航天工业等对安全性要求较高的领域。为了保证软件质量，迫切需要一款能够对Qt代码进行路径覆盖测试的工具。

目标：实现一个原型工具，能够分析Qt源码并自动生成测试用例

要求：学习过形式化方法并对符号执行有了解；熟悉C++/Qt。（2-3人）

7. **题目：**智能合约字节码行为分析工具（指导老师：华保健）
背景：每天都有数百万的智能合约在以太坊上运行，但是99%的合约是不开源的，只能获取到字节码，没有人知晓这些智能合约在如何运作。如果有工具能够辅助对字节码进行分析并且获取更多的信息，那么将能有效提升智能合约的安全性。
目标：提出解决方案；实现一个工具原型，能够从EVM Bytecode中分析期中方法的交易行为并输出为报告
要求：学习过形式化方法并对符号执行有了解；对以太坊智能合约有一定的了解，熟悉Python、Solidity语言。（2-3人）
8. **题目：**基于混合执行的Python程序测试用例生成工具（指导老师：华保健）
背景：Python语言开始只被认为是脚本语言，但是因为其易用易学以及强大的社区支持，现在已经被广泛的应用于各种领域，颇多数量的大型工程也使用Python实现。但是目前对Python语言进行可靠性测试的工具比较缺乏，急需一款工具能够提高Python代码质量。
目标：实现一个原型工具，能够分析Python代码并自动生成测试用例
要求：学习过形式化方法并对混合执行有了解；熟悉Python。（2人）