上海交通大学

本科生毕业设计（论文）任务书

课题名称：基于数据流分析的 R1CS 语言等价性验证及范式生成

执行时间：2023 年 1 月 至 2023 年 5 月

教师姓名：李国强　　职称：副教授

学生姓名：施宸昊　　学号：519021910434

专业名称：软件工程

学院(系)：电子信息与电气工程学院

毕业设计（论文）基本内容和要求：

R1CS 语言为零知识证明的机器语言，由于不同的区块链使用的编译环境不同，面对同一功能的程序，往往生成完全不同的 R1CS 语言，本研究通过数据流分析，验证了同功能的不同 R1CS 程序的等价性，并将等价的 R1CS 程序生成统一的范式，该研究对于 R1CS 语言的正确性证明具有决定性的作用。

毕业设计（论文）进度安排：

序号	毕业设计（论文）各阶段内容	时间安排	备 注
1	初步了解 Circom 和 R1CS 的相关背景知识，调研主流编译器，总结等价 R1CS 约束生成的规律。	2023.1.15~2023.2.5	
2	查阅相关文献和外文资料，熟悉数据流图的特点，设计数据流图表达 R1CS 中的数据关系。	2023.2.5~2023.2.26	
3	制定根据数据流图生成 R1CS 范式的规则。	2023.2.26~2023.3.19	
4	设计并完成范式生成的算法，使之能够正确运行。	2023.3.19~2023.4.9	
5	毕业论文的撰写、修改以及完善。	2023.4.9~2023.5.5	

课题信息：

课题性质 ：设计 √　　论文□

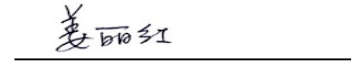
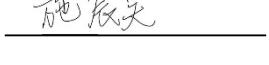
课题来源*：国家级□　　省部级□　　校级□　　横向□　　预研 √

项目编号 _____

其他_____

指导教师签名：_____

2022 年 12 月 29 日

学院（系）意见： **同意** 院长（系主任）签名：    2022 年 12 月 30 日
  学生签名：    2022 年 12 月 29 日