上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

本科生毕业设计（论文）开题报告

论文题目：基于数据流分析的 R1CS 语言等价性验证及范式生成

学生姓名：施宸昊

学生学号：519021910434

专　　业：软件工程

指导教师：李国强

学院(系)：电子信息与电气工程学院

教务处制表

填表说明

1. 根据《上海交通大学关于本科生毕业设计(论文)工作的若干规定》要求，每位学生必须认真撰写《毕业设计（论文）开题报告》。
2. 每位学生应在指导教师的指导下认真、实事求是地填写各项内容。文字表达要明确、严谨，语句通顺，条理清晰。外来语要同时用原文和中文表达，第一次出现的缩写词，须注出全称。
3. 开题前，须进行文献查阅，要求与论文研究有关的主要参考文献阅读数量不少于 10 篇，其中外文资料应占一定比例。参考文献的书写请参照《上海交通大学本科生毕业设计（论文）撰写规范》。
4. 毕业设计（论文）开题报告总字数应满足本院（系）要求。
5. 请用宋体小四号字体填写，并用 A4 纸打印，于左侧装订成册。
6. 该表填写完毕后，须请指导教师审核，并签署意见。
7. 《上海交通大学本科生毕业设计（论文）开题报告》将作为答辩资格审查的主要材料之一。
8. 本表格不够可自行扩页。

毕业设计(论文)开题报告

论文题目	基于数据流分析的 R1CS 语言等价性验证及范式生成				
课题来源	预研	课题性质	设计	项目编号	

课题研究目的和意义（含国内外研究现状综述）：

零知识证明在现代社会中越来越体现出他的重要性，越来越多的加密社区正在寻求通过零知识证明技术来解决一些区块链的最大难题：隐私安全和可扩展性问题[1]。无论是从用户角度还是从开发和角度，对信息隐私安全性的加剧都使零知识证明在隐私方面的优势越来越得到重视。随着去中心化金融（DeFi）使用量的增长，具有可扩展性和隐私安全性优势的零知识应用将有更多的机会提高行业的广泛采用率。

但是零知识证明并不能直接应用于任何计算问题，相反，我们必须将问题转换为操作的正确形式。这种形式被称为“二次算数程序（QAP）”，具体到一次零知识证明的过程中，我们首先是把问题转换成 Circom 语言，再转换成 R1CS 的约束，再由约束转换到 QAP 的形式。在此之后，还有另一个相当复杂的过程来为这个 QAP 创建实际的“零知识证明”，还有一个单独的过程验证所收到的证据，但是这些细节并不在本论文的研究范围内。

在零知识证明的底层工具链中由 Circom 到 R1CS 约束这一步转换存在着很多局限，首要问题就是 R1CS 的可合并性较差，A 与 B 合并后所生成的 R1CS 与 A 和 B 独立生成的 R1CS 在形式上毫无关联，而这与 R1CS 本身表达能力局限性有关外，根本原因便是程序本身可以生成多个等价的 R1CS 约束，所以我们需要在 R1CS 约束中提出 R1CS 约束的范式，使得对于不同的 R1CS 约束，我们可以较容易地判断其等价性和正确性。这对我们验证程序的等价性以及正确性，包括后续更加深入研究 R1CS 的可合并性方面都将大有裨益。

将 Circom 和 R1CS 视为编译前后的两种语言，R1CS 范式生成问题的研究其实更加近似于编译语义一致性的研究。目前国内外也有一部分专利和论文在其他语言的编译范式生成上提出了思路和解决方法。这些相关研究基本上从数据流[2]、语法树[3]或者语义映射[4]这几个方面出发。而基于数据流的分析，国内外关于数据流图设计[5]、数据流图分析[6]、由程序语言生成数据流图的算法[7]以及数据流图一致性检查[8]等方向均有较成熟的研究。可见在数据流与程序分析这个领域，前人的经验十分充分，对后续研究的开展将提供很多理论基础。

课题研究内容：

熟悉并掌握 Circom 语言[9]与 R1CS 约束生成的基本知识，调研主流 Circom 编译器，了解当前主流编译器中生成 R1CS 约束的方法与过程[10]，研究等价 R1CS 生成的特点与规律，设计算法验证 R1CS 的等价性以及生成 R1CS 的范式。

研究方法和研究思路（技术路线）：

1. 通过 Circom 文档以及 github 上的 circom 编译器仓库，熟悉 Circom 语言，以及当前主流 Circom 编译器生成 R1CS 的具体过程。通过构造等价的 Circom 程序，由 npm 中的 snarkjs 框架，生成等价的 R1CS 约束，总结其在形式上不同之处的产生规律。
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，并设计表达数据流图的类，实现从 R1CS 约束到数据流图的转换。
3. 查阅相关文献与算法，制定在数据流图上生成 R1CS 的规则与过程并生成 R1CS 范式，使 R1CS 约束与具体的程序实现细节解耦。

预期研究结果：（可选填）

基本分为四个小目标：

1. 较为深入的分析 Circom 编译器生成 R1CS 约束的规则，并进行详细的总结等价 R1CS 约束在形式上不同之处的产生规律。
2. 设计表达 R1CS 约束中变量逻辑关系的数据流图形。
3. 制定 R1CS 范式的生成规则，实现任意 R1CS 约束到其范式的转换过程。
4. 以数据流图为基础，设计并实现对 R1CS 范式生成以及一致性对比的算法，使得对于输入的任意等价 R1CS，均能输出形式完全一致的 R1CS 约束范式。

计划进度安排：

阶段	开始时间	结束时间	目标
初期了解	2023.1.15	2023.2.5	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。
整体设计 1	2023.2.5	2023.2.26	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。
整体设计 2	2023.2.26	2023.3.19	制定根据数据流图生成 R1CS 范式的规则。
实际操作及编程	2023.3.19	2023.4.9	设计并完成范式生成的算法，使之能够正确运行
论文撰写	2023.4.9	2023.5.5	毕业论文的撰写、修改以及完善

参考文献：

[1] MinaFans. 2022 零知识调查报告[EB/OL].(2022-06-15)[2023-01-03]. https://learnblockchain.cn/article/4243
[2] 袁子牧,冯牧玥,班固,肖扬,许家欢,俞晨东,霍玮,邹维。semantic comparison method and device between a kind of source code and binary code [P].中国专利：CN110147235A, 2019-08-20.
[3] 高丽，李忠琪，杨东升，刘荫忠。Compiling method from intermediate language (IL) program to C language program of instruction list [P].中国专利：CN103123590A, 2013-05-29.
[4] 赵勇胜，陈志勇，崔荣涛，文智力。A kind of assembly language is to th code conversion method of higher level language and device [P].中国专利：CN103123590A, 2015-11-18.
[5] Kavi K M, Buckles B P, Bhat U N. A formal definition of data flow graph models[J]. IEEE Transactions on computers, 1986, 35(11): 940-948.
[6] Allen F E, Cocke J. A program data flow analysis procedure[J]. Communications of the ACM, 1976, 19(3): 137.
[7] Lee E A. Consistency in dataflow graphs[J]. IEEE Transactions on Parallel and Distributed systems, 1991, 2(2): 223-235.
[8] Ibrahim R. Formalization of the data flow diagram rules for consistency check[J]. arXiv preprint arXiv:1011.0278, 2010.
[9] Belles-Munoz M, Isabel M, Munoz-Tapia J L, et al. Circom: A Circuit Description Language for Building Zero-knowledge Applications[J]. IEEE Transactions on Dependable and Secure Computing, 2022 (01): 1-18.
[10] García Navarro H. Design and implementation of the Circom 1.0 compiler[J]. 2020.

指导教师意见（课题难度是否适中、工作量是否饱满、进度安排是否合理、工作条件是否具备、是否同意开题等）：

该研究具有相当的前瞻性和一定的难度，工作量充足，进度安排合理，可以通过开题。

指导教师签名：

2023 年 1 月 5 日

学院（系）意见：

同意

审 查 结 果： √ 同 意 □ 不 同 意

学院（系）负责人签名：

2023 年 1 月 6 日