上 海 交 通 大 学
本科生毕业设计(论文)答辩提问录

学院（系）：电子信息与电气工程学院　　专业：软件工程

学生姓名：施宸昊　　学号：519021910434

毕业设计(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

答辩教师：饶若楠,任锐,吴刚,薛亚娟

答辩日期：2023 年 5 月 29 日　　答辩地点：软件学院 1319

答辩记录（包括答辩小组成员提出的主要问题及学生答辩的简要情况）

1.什么是零知识证明？（吴刚）

答：零知识证明是一种密码学方法，指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。″

记录人签名：姜丽红

注：① 本表供答辩小组在答辩时填写
② 答辩结束当即交给答辩组组长