
FCS 北京航空航天大学&华威大学：提出新型SNARKs框架，支持高次门电路且无需FFT运算

作者：writer 来源：科学网

本文原地址：<https://www.iikx.com/news/progress/40868.html>

本文仅供学习交流之用，版权归原作者所有，请勿用于商业用途！

FCS

北京航空

航天大学&华威大

学：提出新型SNARKs框架，支持高次门电路且无需FFT运算。论文标题：CP-SuperSpartan: commit-and-prove SNARKs for customizable constraint systems

期刊：Frontiers of Computer Science

作者：Zibo ZHOU, Zongyang ZHANG, Feng HAO, Jianwei LIU

发表时间：2 Jul 2025

DOI：10.1007/s11704-025-50244-z

微信链接：点击此处阅读微信文章

RESEARCH ARTICLE

CP-SuperSpartan: commit-and-prove SNARKs for customizable constraint systems

Zibo ZHOU¹, Zongyang ZHANG¹✉, Feng HAO², Jianwei LIU¹

1. School of Cyber Science and Technology, Beihang University, Beijing 100191, China

2. Department of Computer Science, University of Warwick, Coventry CV4 7AL, United Kingdom

Received March 7, 2025; accepted June 30, 2025

E-mail: zongyangzhang@buaa.edu.cn

© Higher Education Press 2026

引用格式：

Zibo ZHOU, Zongyang ZHANG, Feng HAO, Jianwei LIU. CP-SuperSpartan: commit-and-prove SNARKs for customizable constraint systems. *Front. Comput. Sci.*, 2026, 20(10): 2010813

阅读原文：



摘要

承诺并证明简洁非交互式知识参数 (CP-SNARKs) 是证明复杂陈述的关键技术。然而，现有方案大多仅支持2次门电路，限制了对非代数陈述的表达效率。为此，北京航空航天大学研究团队提出了CP-SuperSpartan系列方案。该方案支持可定制约束系统 (CCS)，能够处理高次门电路，且消除了昂贵的快速傅里叶变换 (FFT) 操作。通过结合多种多线性多项式承诺方案 (PCS)，CP-SuperSpartan在保持通用更新设置的同时，显著提升了大规模电路的证明生成效率，为隐私保护计算和区块链扩展提供了更高效的工具。

技术步骤

零知识证明（ZKP）是实现数据隐私与计算验证的核心。在处理包含代数与非代数混合的复杂陈述时，CP-SNARKs通过允许证明者对见证（Witness）先行承诺再进行证明，展现了巨大的应用潜力。但目前的技术痛点在于，大多数主流方案（如LegoSNARK）受限于R1CS约束系统，仅能高效表达2次门。当面对复杂的非代数运算时，这种限制会导致约束数量激增，且伴随的大规模FFT运算会消耗极高的计算资源，成为性能提升的瓶颈。

针对这一挑战，研究团队开发了CP-SuperSpartan框架。该方案通过引入可定制约束系统（CCS），不仅兼容了R1CS、Plonkish和Air等主流约束，还原生支持高次门电路，极大地增强了对复杂逻辑的表达能力。在算法设计上，CP-SuperSpartan完全摒弃了FFT运算，转而采用和校验协议（Sum-check protocol），使得证明生成时间与电路规模呈线性关系，特别适合处理超大规模的计算任务。

实验结果表明，在相同的安全性标准下，CP-SuperSpartan的证明者效率显著优于传统的LegoSNARK和Spartan方案。当使用基于配对的承诺方案时，它能提供与LegoSNARK相同的通用可更新设置；而当使用基于哈希的方案时，则能实现抗量子安全。这一多功能、高性能的架构设计，为去中心化应用中的复杂身份证明、隐私交易以及可验证计算提供了更为稳健的技术支撑。

期刊简介

Frontiers of Computer Science (FCS) 是由教育部主管、高等教育出版社和北京航空航天大学共同主办，南京大学支持，SpringerNature 公司海外发行的英文学术期刊。本刊于 2007 年创刊，月刊，全球发行。主要刊登计算机科学领域具有创新性的综述论文、研究论文等。本刊主编为周志华院士，执行主编为周昆教授。编委会及青年 AE

团队由国内外知名学者及优秀青年学者组成。本刊被 SCI、Ei、DBLP、INSPEC、SCOPUS 和中国科学引文数据库 (CSCD) 核心库等收录，为 CCF 推荐 B 类期刊；两次入选中国科技期刊国际影响力提升计划；入选第 4 届中国国际化精品科技期刊；两次入选中国科技期刊卓越行动计划（一期梯队、二期领军）。

来源：Frontiers of Computer Science

更多 科学进展 请访问 <https://www.iikx.com/news/progress/>

本文版权归作者所有，请勿用于商业用途，[爱科学iikx.com](http://iikx.com)转发