MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

26. srpna 2024

Věc: Posudek vedoucího práce "On PlonK SNARK"

Shrnutí práce:

Předložená práce popisuje kryptografický protokol PlonK od Gabizona, Williamsona a Ciobotaru (Cryptology ePrint Archive 2019), jeho možné optimalizace a jejich experimentální ověření. V úvodu práce student představil základní stavební bloky protokolu jako např. KZG závazek k polynomům a jeho vlastnosti. Poté následuje důsledný popis jednotlivých částí samotného protokolu. V závěru jsou rozebrány možné optimalizace, které by potenciálně umožnili rozšířit použitelnost protokolu PlonK na větší instance v praxi. Speciální důraz je kladen na aplikace (inverzní) Fourierovy transformace při práci s polynomy v průběhu protokolu a snahu o algebraický přístup pro zabránění neefektivity způsobené růstem stupňů zpracovávaných polynomů.

Hodnocení práce:

Jako silnou stránku práce bych chtěl vyzdvihnout, že student svou prací demonstruje pochopení netriviálního kryptografického protokolu a schopnost nejenom jej srozumitelně popsat přístupnou formou, ale také analyzovat natolik, aby mohl navrhnout a implementovat jeho optimalizace. Výsledkem je rozsáhlý text, kde autor na některých místech volil kompromisy v úrovni použitého formalismu. Specificky jsou některé kryptografické definice pojaty spíše intuitivně. Toto však akceptuji jako pochopitelné, protože by jinak text práce ještě narostl a nepomohl nutně pochopení hlavních myšlenek popisovaného protokolu jako celku. Větší výhrady bych měl k použitému matematickému stylu, pokud by snahou práce bylo například vylepšení důkazu bezpečnosti, ale toto nebylo cílem práce. Narozdíl od původního článku od Gabizona a spol., může text práce posloužit jako dobrý úvod do detailů praktických protokolů z rodiny SNARK. Část s optimalizacemi rozvíjí nové zajímavé myšlenky, které zatím nebyly nikde publikovány.

Celkově věřím, že kolega Benčík zadání práce splnil. Práci navrhuji uznat jako bakalářskou a ohodnotit známkou výborně.

Mgr. Pavel Hubáček, Ph.D.

Informatický ústav Univerzity Karlovy
Malostranské nám. 2/25, 118 00 Praha 1
telefon: 951554230, fax: 257531014
e-mail: sekretariat@iuuk.mff.cuni.cz