Posudek bakalářské práce

Matematicko-fyzikální fakulta Univerzity Karlovy

Autor práce	Benjamín Benčík
Název práce	On PlonK SNARK
Rok odevzdání	2024
Studijní program	Informatika
Specializace	Umělá inteligence

Autor posudku	Petr Chmel	Oponent
Pracoviště	Informatický ústav Univerzity Karlovy	

Popis práce

Práce se zabývá protokolem pro krátké neinteraktivní argumenty (tzv. SNARK) PlonK. Autor po krátké motivaci užitečnosti SNARKů nejprve uvádí čtenáře do základních pojmů v oblasti a dále detailněji popisuje všechny důležité součásti protokolu jako jsou eliptické křivky, schéma KZG pro polynomiální závazky, Fiatova–Shamirova transformace, aritmetizace a kontroly konzistence v PlonKu. Hlavní částí práce je pak přehledné vysvětlení celého protokolu a hledání vhodných míst pro jeho optimalizaci jak teoretickými tak praktickými úpravami. V teoretičtější části autor navrhuje možnost snížení stupně drátových polynomů skrze úpravy vycpávání polynomu pro rychlou Fourierovu transformaci a následné zpracování. V praktické části pak zkoumá přirozený způsob zrychlení skrze paralelizaci výpočtu. Oba způsoby jsou také autorem naimplementovány včetně experimentů pro vyzkoušení jejich účinnosti.

Hodnocení práce

Hlavními přínosy práce je právě detailně rozepsaný popis protokolu a analýza možných optimalizací. Samotné vlastnosti protokolu jsou zmíněny jen spíše na okraj a jejich důkaz je částečně pouze naznačen, ale vzhledem k cílům práce a náročnosti některých důkazů toto rozhodnutí vidím jako akceptovatelné. Část práce zkoumající možné optimalizace je také zajímavá, názorně ukazuje autorův postup při optimalizaci i konkrétní implementační detaily existující implementace od ZK-Garage, které poté umožnily paralelizaci výpočtu.

Práce je napsána přehledně. Po formální stránce práce obsahuje množství překlepů a typografických chyb, které je úměrné délce textu a tyto překlepy nepřekáží pochopení textu. Matematická úroveň práce je velmi dobrá, formulace jsou korektní, ačkoliv úroveň formality hlavně u definic místy kolísá. Zdroje jsou správně citovány.

Nepřesnosti a význačnější překlepy

- Na začátku první kapitoly autor uvádí, že booleovské obvody s hradly AND a OR jsou postačující k reprezentaci jakéhokoliv programu, ale ještě je potřebné hradlo NOT.
- Definice 9 a 11 jsou napsány spíše neformálně, což má za důsledek jejich nadměrné zesílení; zároveň těsně po Definici 9 následuje definice dalšího pojmu, která není nijak označena.
- Při popisu schématu KZG (str. 20) dochází v průběhu k záměně τ a ω.

- Tabulka 3.1 je lehce zavádějící, protože nebere v potaz velikost prvků grupy či tělesa a nenaznačuje na nich žádnou závislost.
- Důkaz Věty 4 je napsán jako znění Lemmatu 13 místo samotného důkazu.
- Třetí odstavec na str. 43 obsahuje pouze jednu tečku z předchozí věty, která má být součástí předchozí rovnosti.
- Autor v podkapitolách 3.5 a 3.6 mění variantu angličtiny: z „linearization“ se stává „linearisation“ a poté se vrací nazpět.
- Všechny citace z Cryptology ePrint Archive obsahují URL dvakrát.

Výše uvedené nepřesnosti však nejsou zásadního charakteru. Zadání práce je jednoznačně splněno, a proto ji doporučuji uznat jako bakalářskou.

Celkové hodnocení:	Výborně/velmi dobře
Práci navrhuji na zvláštní ocenění:	Ne

V Praze dne 23. 8. 2024
Petr Chmel