Posudek vedoucího bakalářské práce

Název: Bezpečné sdílené počítání modulo p^k
Autor: Martin Struk

Shrnutí obsahu práce

Cílem předkládané práce bylo popsat dílčí protokol sdíleného společného výpočtu funkce s tajnými vstupními hodnotami spolu s matematickým pozadím tohoto protokolu tak, aby účastníci nebyli s to o tajných hodnotách používaných ve výpočtu nic zjistit.

Text se skládá z motivačního úvodu, tří kapitol, a závěru shrnujícího autorův přínos. První kapitola představuje základy využívané teorie, především koncept sdílení tajemství s využitím volných modulů nad Galoisovými okruhy. Stručná druhá kapitola je věnována konstrukci hyperinvertibilních matic a jejich využití pro nalezení modulového izomorfismu, který je klíčovým prvkem protokolu podrobně popsaného v třetí části práce. Samotný protokol se skládá z přípravné offline fáze, která slouží především k vyřazení části účastníků protokolu tak, aby se zvýšil podíl spolehlivých participantů, a online fáze, která spočívá ve spouštění jednotlivých výpočetních bran.

Celkové hodnocení práce

Téma práce. Ačkoli bylo téma práce kompilační, studentovým úkolem bylo zpracovat několik článků, doplnit podstatné matematické detaily a prezentovat výsledky i protokol jednotným způsobem. Téma bylo podle mého mínění vhodné pro zpracování v bakalářské práci.

Vlastní příspěvek. Studentův přínos spočívá jednak v reformulaci a důkazu některých standardních výsledků lineární a polynomiální algebry pro situaci obecného komutativního okruhu, dále popisu konstrukce hyperinvertibilní matice a především srozumitelném nastínění protokolu využívajícího této teorie.

Matematická úroveň. Matematická úroveň práce je podle mého mínění dobrá, formulace jsou korektní a srozumitelné a prezentované důkazy jsou přehledné.

Práce se zdroji. Ačkoli text primárně vychází z několika nedávných článků, není na nich formulačně závislý.

Formální úprava. Po formální i jazykové stránce je práce poměrně zdařilá a nezasluhuje podle mého mínění žádné podstatnější výtky.

Připomínky a otázky

S otázkami, námitkami a připomínkami, které jsem průběžně vznášel k pracovním verzím textu, se student úspěšně vyrovnal. V odevzdané práci jsem si již žádných nedostatků nevšiml.

Závěr

Práce Martina Struka *Bezpečné sdílené počítání modulo* p^k podle mého názoru splnila zadání a rozhodně ji doporučuji uznat jako bakalářskou.

Návrh klasifikace vedoucí práce sdělí předsedovi zkušební komise.

Jan Žemlička
Katedra algebry
4.9.2023