Posudek oponenta bakalářské práce

předložené na Matematicko-fyzikální fakultě Univerzity Karlovy

Autor:	Svetlana Ivanova
Název práce:	Practical Batch Proofs of Exponentiation
Stud. program a zaměření:	informatika, obecná informatika
Rok odevzdání:	2024
Jméno a tituly oponenta:	Mgr. Martin Mareš, Ph.D.
Pracoviště:	Katedra aplikované matematiky
Kontaktní e-mail:	mares@kam.mff.cuni.cz

Popis práce

Předložená práce se zabývá interaktivními protokoly pro důkaz umocňování: dokazovatel chce přesvědčit ověřovatele, že spočítal $x^e \bmod m$ pro velmi velký exponent e. To je důležitý podproblém řady kryptografických protokolů. Práce studuje dávkovou verzi problému, v níž ověřujeme mnoho tvrzení tohoto druhu současně.

Práce popisuje několik protokolů popsaných v literatuře a navrhuje dva nové protokoly založená na kombinaci známých přístupů. Protokoly poté srovnává jak teoretickým rozborem (výpočtem průměrného počtu násobení), tak prakticky (měřením doby běhu implementace).

Hodnocení

Teoretická část práce je napsána přehledně a správně. Z analýzy efektivity plyne, že nové protokoly jsou výrazně lepší než dříve známé. Analýza bezpečnosti není v práci uvedena, ale je publikována v článku sepsaném autorkou společně s vedoucím práce.

K experimentální části bych měl některé výhrady. Implementace protokolů by měla být v práci popsána a zdrojový kód přiložen. Místo toho se v práci nachází pouze odkaz na externí gitový repozitář, v němž je holý kód bez komentářů a minimum popisu. Například není nikde řečeno, jaké knihovny pro aritmetiku program používá, ačkoliv toho rozhodnutí má zásadní vliv na výkon.

Také mi nepřijde vhodné jako hlavní kriterium použít dobu výpočtu omezenou na operace násobení. V práci se tato volba zdůvodňuje tím, že výsledky lze srovnávat s teoretickým výpočtem počtu násobení. Diskuse výsledků ale jasně ukazuje, že naměřené hodnoty teorii neodpovídají, a dokonce je vyslovena věrohodně znějící hypotéza, že za to mohou efekty paměťové hierarchie. Tím spíš by bylo lepší měřit celkovou dobu běhu a pro srovnání s teorií ještě počet provedených násobení.

Na druhou stranu experimenty nebyly zadáním práce požadovány a i samotné teoretické výsledky by vydaly na dobrou bakalářskou práci. V tomto kontextu mi nedostatky experimentů nepřijdou zásadní.

Práce je napsána čtivou angličtinou takřka bez jazykových chyb. Použité zdroje jsou korektně citovány.

Práci proto doporučuji přijmout jako bakalářskou.

Celkové hodnocení:	velmi dobře
Práci navrhuji na zvláštní ocenění:	ne

V Praze dne 30. května 2024
Martin Mareš