MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

4. června 2024

Věc: Posudek vedoucího práce "Practical Batch Proofs of Exponentiation"

Shrnutí práce:

Předložená práce studuje protokoly pro dávkové dokazování korektnosti modulárního mocnění. Studentka popsala známé protokoly od Rotema (TCC 2021) a představila dva nové protokoly, které značně vylepšují efektivitu těchto protokolů. Nové protokoly vychází ze společného článku se mnou a Charlotte Hoffmannovou z IST Austria (preprint na IACR Cryptology ePrint Archive 2024: 145). Oproti článku je v práci více rozveden úvod a motivace problému, aby byla problematika a její řešení přístupnější širšímu informatickému publiku. Cílem práce nebyla implementace těchto protokolů, ale studentka také reportuje o praktické efektivitě nových protokolů ohodnocené pomocí své vlastní implementace v C++.

Hodnocení práce:

Jako silnou stránku práce bych chtěl vyzdvihnout, že studentka svou prací demonstruje pochopení netriviálních kryptografických protokolů a schopnost je srozumitelně popsat přístupnou formou. V průběhu diskusí, jež vedly ke společnému článku s Hoffmannovou, se aktivně podílela na analýze praktických parametrů známých protokolů a poté i na návrhu nových protokolů. Důkazy bezpečnosti nových protokolů vznikly spoluprací mě a Hoffmannové, a tak je studentka ve své práci neprezentovala. Finální text práce vznikl v poměrně krátké době a některé jeho části, jako například potenciální aplikace, by mohly být rozvedeny pro doplnění kontextu. To ale není zásadní vadou práce a v prezentaci protokolů a analýze jejich efektivity nic důležitého nechybí.

Celkově věřím, že kolegyně Ivanova zadání práce splnila. 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