MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

25. ledna 2022

Věc: Posudek vedoucího práce Bc. Ľubice Jančové "Effectivity and Limitations of Homomorphic Secret Sharing Schemes"

Práce kolegyně Jančové pojednává o konstrukcích homomorfních schémat pro sdílení tajemství. Autorka v práci předkládá nové výsledky o distribuovaném problému diskrétního logaritmu (DDLog), jenž je centrálním blokem většiny známých konstrukcí homomorfních schémat pro sdílení tajemství.

Jako první výsledek práce je dokázán horní odhad pro úspěšnost generických protokolů řešících DDLog pomocí preprocessingu. Tato část práce zobecňuje známé výsledky o generických útocích na standardní problém diskrétního logaritmu pomocí preprocessingu a rozvíjí tyto techniky v kontextu distribuovaných protokolů pro DDLog. Dosažené výsledky například ukazují, že preprocessing nemůže asymptoticky pomoci v režimu parametrů relevantním v konstrukcích homomorfních schémat pro sdílení tajemství. Tyto výsledky kolegyně Jančová získala pod mým vedením a na základě diskusí s mou doktorandkou Veronikou Královou. Musím však zdůraznit, že při formalizaci důkazů a přípravě textu práce postupovala samostatně a není pochyb o tom, že má hlavní podíl na autorství těchto výsledků.

Jako druhý výsledek práce je představena modifikace Joyeho-Libertova kryptosystému, která umožňuje efektivní konstrukci protokolu pro DDLog. Autorka tak velice zajímavým způsobem rozšiřuje škálu předpokladů, které lze využít k efektivním konstrukcím homomorfních schémat pro sdílení tajemství. K důkazu bezpečnosti modifikovaného Joyeho-Libertova kryptosystému jsou představeny nové předpoklady o výpočetní obtížnosti problémů z teoriie čísel, které by mohly stimulovat další výzkum. Na této části práce pracovala kolegyně Jančová na stáži na IMDEA Software Institute u konzultanta práce Ignacia Cascuda.

Obě části práce kolegyně Jančové přinášejí nové poznatky o problému distribuovaného disktrétního logaritmu, které lze publikovat v kvalitních konferencích se zaměřením na kryptografii. Práce je celkově velice dobře napsaná. Strohý styl textu odpovídá spíše článku pro specialistu, což je však akceptovatelné vzhledem k tomu, že práce předkládá nové výsledky a nejedná se o přehledovou práci o známém tématu.

Doporučuji práci k obhájení jako diplomovou a dle uvážení komise také k navržení na ocenění.

Mgr. Pavel Hubáček, Ph.D.

Pavel Hubáček

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