MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

6. září 2022

Věc: posudek vedoucího práce Bc. Kateřiny Bžatkové "Multivariate polynomial commitment schemes"

Práce kolegyně Bžatkové studuje schémata pro závazky k polynomům více proměnných. Cílem takovýchto schémat je umožnit dokazovateli zavázat se k polynomu jedné nebo více proměnných tak, aby mohl později ověřovateli sdělit funkční hodnotu tohoto polynomu na zvoleném vstupu se zárukou, že sdělená funkční hodnota odpovídá danému vstupu a nedošlo ke změně polynomu. Efektivní schémata pro závazky k polynomům jsou zásadní v moderních konstrukcích praktických důkazových systémů, protože umožňují modulární návrhy protokolů s dokazatelnou bezpečností – bezpečnost protokolu lze uvažovat v idealizovaném světě a poté ukázat, že tento lze implementovat pomocí bezpečných závazků k polynomům.

Hlavním přínosem práce jsou nové konstrukce schémat pro závazky k polynomům více proměnných. Většina známých prací v kryptografické literatuře uvažuje schémata pro polynomy jedné proměnné. Relativně přímočará rozšíření známých schémat na polynomy více proměnných existují, ale za cenu značného navýšení komunikační složitosti. Kolegyně Bžatková kombinuje techniky ze dvou nedávných článků a představuje nový přístup k efektivním konstrukcím schémat pro polynomy více proměnných. V článcích, na kterých práce staví, se využívá převodu problému vyhodnocování polynomu odpovídajícího závazku na konstrukce interaktivních důkazových systémů pro testování polynomiálních rovností. Jako hlavní technický přínos práce kolegyně Bžatková tuto myšlenku značně rozvádí pomocí teorie ideálů polynomiálních okruhů tak, aby představila konstrukce schémat s lepší komunikační složitostí.

Samotná práce nejdříve představuje základní výsledky z teorie polynomiálních okruhů a kryptografické definice pro uvažovaná schémata. Následně jsou popsána dvě nová schémata. První konstrukce demonstruje autorčin nový přístup. Druhé schéma využívá prvního pro efektivní paralelní vyhodnocování závazku na mnoha vstupních hodnotách. Práce je přehledně strukturována se snahou ilustrovat koncepty v úvodních kapitolách na jednoduchých příkladech. Vzhledem k tomu, že články, na kterých práce staví jsou součástí delší série článků, je problematické obsáhnout detaily předchozích prací a jejich motivace bez změny stylu práce na rešerši. Věřím, že autorka v tomto směru našla rozumný kompromis.

Autorka rozhodně splnila zadání, a tak doporučuji práci k obhájení jako diplomovou.

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