Posudek diplomové práce

Matematicko-fyzikální fakulta Univerzity Karlovy

Autor práce	František Mejzlík
Název práce	Fast hash-based signing protocol for message stream authentication
Rok odevzdání	2023
Studijní program	Informatika **Studijní obor** Softwarové systémy

Autor posudku	Jan Kofroň **Role** oponent
Pracoviště	KDSS

Text posudku:

Cílem práce je navrhnout message-stream autentizační komunikační protokol, odolný vůči kvantovým útokům a zároveň dostatečně efektivní pro praktické použití.

Autor práce se tématu zhostil velmi dobře, výsledkem je nejen knihovna implementující navržené řešení, ale i ukázková aplikace používající tuto knihovnu a analýza parametrů knihovny vzhledem k různým reálným scénářům (např. frekvence ztrácení zpráv, velikost režie, ...).

Text práce je psán v angličtině a je na velice dobré stylistické i typografické úrovni, jen s nepatrným množstvím nedostatků. Text je dobře čitelný a srozumitelný, autor vše dostatečně podrobně popisuje.

Implementace knihovny v jazyce Rust je přehledná, dobře navržená a dostatečně okomentovaná. Programátorská dokumentace je na rozumné úrovni. Ukázková aplikace realizující „internetové rádio“ s jedním vysílajícím uzlem a několika přeposílajícími a přijímacími uzly je velmi dobrým příkladem použití knihovny, demonstrujícím její snadnou a praktickou použitelnost.

Celkově práci hodnotím jako velmi zdařilou, ačkoliv technické detaily týkající se šifrování a podepisování zpráv jsou mimo můj obor, a nedokážu je proto spolehlivě zhodnotit.

Práci doporučuji k obhajobě.

Práci nenavrhuji na zvláštní ocenění.

V Praze dne 28. 8. 2023

Podpis: