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	RNDr. Filip Zavoral, PhD. **Role** Vedoucí
Pracoviště	KSI

Text posudku:

Hlavním tématem předkládané práce je zkoumání možnosti využití hash-based signatures pro autentikaci datových proudů zejména v real-time aplikacích. Autor po prostudování potřebné teorie navrhl a implementoval efektivní protokol odolný proti kvantovým útokům pro zabezpečený přenos dat ve formě knihovny pro programovací jazyk Rust. Nad tímto protokolem potom implementoval aplikaci pro vysílání a příjem zvukového vysílání. Autor velmi detailně analyzoval výkonnost, vliv parametrizace a další vlastnosti vyvinutého protokolu a jeho použití v reálné aplikaci.

Na předkládané práci velmi oceňuji zejména její komplexnost. Autor musel nastudovat větší množství netriviální teorie, analyzoval požadavky na uvažovaný protokol, tento navrhl a implementoval, implementoval i reálně použitelnou aplikaci a vše detailně vyhodnotil. Jak textovou tak implementační část práce považuji za velice kvalitní a doporuřuji k obhajobě.

Práci doporučuji k obhajobě.

Práci navrhuji na zvláštní ocenění.

Pokud práci navrhujete na zvláštní ocenění (cena děkana apod.), prosím uveďte zde stručné zdůvodnění (vzniklé publikace, významnost tématu, inovativnost práce apod.).

Oceňuji zejména komplexnost předkládané práce. Autor nastudoval větší množství teorie, analyzoval požadavky na uvažovaný protokol, tento navrhl a implementoval, implementoval i reálně použitelnou aplikaci a vše detailně vyhodnotil. Jak textovou tak implementační část práce považuji za velice kvalitní.

Datum 27. srpna 2023 **Podpis**