Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA BAKALÁŘSKÉ PRÁCE

Jméno studenta: Matěj Boura

Název práce: Zabezpečení certifikátů Eliptických křivek

Autor posudku: Ing. Tomáš Svoboda, Ph.D

Cíl práce: Cílem práce je představení nutných teoretických základů ohledně kryptografie a matematiky, a následná analýza s komparací algoritmů ECC s návazností na problematiku zabezpečení ECC s využitím v současnosti.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)					
	A	**B**	**C**	**D**	**E**	**F**
Práce svým zaměřením odpovídá studovanému oboru	☐	☒	☐	☐	☐	☐
Vymezení cíle a jeho naplnění	☐	☐	☐	☒	☐	☐
Zpracování teoretických aspektů tématu	☐	☐	☒	☐	☐	☐
Zpracování praktických aspektů tématu	☐	☐	☐	☐	☒	☐
Adekvátnost použitých metod, způsob jejich použití	☐	☐	☐	☐	☒	☐
Hloubka a správnost provedené analýzy	☐	☐	☐	☐	☒	☐
Práce s literaturou	☐	☐	☐	☐	☐	☒
Logická stavba a členění práce	☐	☐	☐	☒	☐	☐
Jazyková a terminologická úroveň	☐	☐	☐	☒	☐	☐
Formální úprava a náležitosti práce	☐	☐	☐	☒	☐	☐
Vlastní přínos studenta	☐	☐	☐	☐	☒	☐
Využitelnost výsledků práce v teorii (v praxi)	☐	☐	☐	☐	☒	☐

Vyjádření k výsledku anti-plagiátorské kontroly

Antiplagiátorská kontrola eVSKP identifikovala celkovou podobnost: 7 %.

Dílčí připomínky a náměty:

Hloubka provedené analýzy je nedostatečná. V práci se vyskytuje mnoho gramatických chyb a nepřesností, včetně prázdných kapitol (přílohy).

Autor práce měl lépe pracovat s použitými zdroji. Autor neuvedl dle výsledku anti-plagiátorské kontroly všechny použité zdroje, ze kterých čerpal.

Praktická část je velice povrchní a odpovídá rešeršní problematice. Podrobně jsou připomínky k praktické části uvedeny v následující kapitole.

Celkové posouzení práce a zdůvodnění výsledné známky:

Předložená práce je rozdělena do čtyř hlavních kapitol. Nejprve autor práce ve druhé kapitole podrobně představuje problematiku teorie eliptických křivek a základy teorie kryptografie. Ve třetí

kapitole autor plynule navazuje na představenou problematiku a představuje principy a možnosti využití eliptických křivek v certifikátech a digitálních podpisech s důrazem na algoritmy ECDSA a ECDH. Praktická část práce je součástí kapitoly 3.4. Praktická část práce je zaměřena na uvedení příkladů využití elipckých křivek v bitcoin blockchain, SSH, TLS, elektronickém ID a elektronickém podpisu.
Analýza praktického využití je velice povrchní. Autor uvádí pouze omezenou množinu protokolů a technologií, kde jsou využity algoritmy založené na eliptických křivkách. Není zřejmé, na základě jakých kritérií autor vybral právě tyto technologie. Popis technologií se omezuje pouze na obecné konstatování, že jsou využity eliptické křivky. Autor měl zvolit a obhájit vhodná kritéria výběru použitých technologií s detailním rozborem, jakým způsobem a s jakou efektivitou jsou využívány právě eliptické křivky se zaměřením např. na porovnání výhod a nevýhod využitých algoritmů na základě výkonnostního porovnání apod.
Přes výše uvedené nedostatky doporučuji práci k obhajobě a navrhuji klasifikační stupeň E.

Otázky k obhajobě:

Na základě jakých kritérií byly vybrány technologie a protokoly využívající eliptické křivky v praktické části práce?

Práci doporučuji k obhajobě.

Navržená výsledná známka: E

V Hradci Králové**, dne 11. května 2022**

_____

podpis