FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student: Matouš Skála
Oponent práce: doc. Ing. Štěpán Starosta, Ph.D.
Název práce: Bitcoin Wallet for Android with TREZOR Hardware Wallet Support
Obor: Teoretická informatika

Datum vytvoření: 11. 6. 2018

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*1=mimořádně náročné zadání,* ***2=náročnější zadání,*** *3=průměrně náročné zadání,* *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Zadání hodnotím jako náročnější: ukládá nastudovat fungování kryptoměny Bitcoin do dostatečné míry, aby mohla být implementována Bitcoin peněženka na hardwarovém zařízení TREZOR, které bylo také nutno nastudovat.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Zadání je splněno.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***1=splňuje požadavky,*** *2=splňuje požadavky s menšími výhradami,* *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Rozsah písemné zprávy je adekvátní.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*80 (B)*

Popis kritéria:
Posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře.

Komentář:
Celková logická návaznost kapitol je na dobré úrovni, nicméně některé části jsou stručné nebo příliš stručně uvedé do kontextu. Stručnost vede někdy i k věcným chybám, například:
* V části 1.1.1 chybí zmínka o diskriminantu eliptické křivky (také by se v tomto případě mělo zmínit, že p nemůže být mocnina 2);
* Z hlediska teoretické informatiky beru za přehmat prohlášení na konci části 1.1.2, že problém diskrétního logaritmu je stejně složitý jako hledání hrubou silou: tvrzení není nijak vysvětelné a s přihlédnutím na nejlepší algoritmy (index calculus) řešící tento problém, byť ne pro eliptické křivky, je to tvrzení velmi zavádějící.
* U vzorců na straně 7 není na první pohled jasné, o jaké operace se jedná.
* v části 1.2.3. není jasné, co je myšleno "uvedením/vložením entropie"

U první kapitoly nevím, proč je v názvu "design".

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*80 (B)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Komentář:
Práce je psaná anglicky. Jazyk je na dobré úrovni, uchyluje se však často k neformální výrazům, především zkráceným formám "it's" apod. Výskyt gramatických chyb není nijak častý.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*95 (A)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Práce se zdroji je na výborné úrovni. Na několika místech by se hodilo ocitovat zdroj, nebo jej přimonenout

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*100 (A)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Vytvořená aplikace je zcela funkční a může sloužit jako peněženka pro systém Adroid, která plně využívá zařízení TREZOR.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Jedná se o první aplikaci pro systém Andoid využívající zařízení TREZOR. Vzhledem k rostoucí popularitě kryptoměn je tedy výsledek využitelný. Text práce je zároveň vhodným výhozím zdrojem informací o této problematice odmyslíme-li nepřesnosti v teoretické části.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
Nemám.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*89 (B)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Mým hlavním důvodem pro nenavržení známky A je kombinace oboru autora, teoretická informatika, a nejasných až chybných vyjádření právě v teoretické části. Celkově ovšem práci považuji za velmi zdařilou: místy by se sice čtenáři hodilo více detailů, nicméně to je způsobeno rozsáhlostí celého tématu. Výsledná aplikace je velmi dobrá a ihned použitelná.

Podpis oponenta práce: