FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Petr Socha
Student:	Bc. David Pokorný
Název práce:	Analýza postranních kanálů postkvantového podpisu Rainbow
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	15. května 2021

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
- [2] zadání splněno s menšími výhradami
- [3] zadání splněno s většími výhradami
- [4] zadání nesplněno

Práce se zabývá dvěma aktuálními výzkumnými tématy, a sice bezpečností postranních kanálů a postkvantovou kryptografií. Splnění některých bodů zadání vyžaduje přístup do vybavené laboratoře. Navzdory nadprůměrné složitosti a významným komplikacím způsobeným pandemií Covid-19 splnil student zadání bez výhrad.

2. Písemná část práce 95 /100 (A)

Písemná práce je koherentní, vyvážená, informačně bohatá a obsahuje všechny podstatné informace. Zároveň je práce přiměřeně stručná a bez nadbytečných částí. Student v práci cituje relevantní zdroje a kreativně navazuje na současné poznatky. Drobné výhrady směřují pouze k jazykovým prohřeškům a nekonzistencím, které nicméně nijak negativně neovlivňují srozumitelnost díla.

3. Nepísemná část, přílohy 95 /100 (A)

Student v rámci práce navrhuje útok postranním kanálem a dvě varianty protiopatření proti takovému útoku. Výpočty související s útokem byly implementovány v jazyce Python, protiopatření pak v jazyce C. Zdrojové kódy jsou řádně komentované, slabinou je pouze jejich struktura a s ní související horší udržitelnost kódu. Útok i protiopatření byly otestovány s využitím řádné experimentální metodologie a obvyklého hardwarového vybavení, což podporuje věrohodnost výsledků a z nich plynoucích závěrů, a zároveň umožňuje snadnou opakovatelnost provedených experimentů.

4. Hodnocení výsledků, jejich využitelnost 100 /100 (A)

Práce se zabývá aktuálními výzkumnými tématy, má potenciál oslovit vědeckou komunitu a zároveň přispět k probíhajícímu standardizačnímu procesu NIST. Část dosažených výsledků byla již publikována na prestižní konferenci DATE 2021, další publikace je v přípravě.

5. Aktivita studenta

▸ [1] **výborná aktivita**
[2] velmi dobrá aktivita
[3] průměrná aktivita
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

Student byl v průběhu řešení práce velmi aktivní, účastnil se pravidelných konzultací.

6. Samostatnost studenta

▸ [1] **výborná samostatnost**
[2] velmi dobrá samostatnost
[3] průměrná samostatnost
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Student prokázal výbornou samostatnost, a to jak v oblasti teoretické/matematické, tak v oblasti čistě inženýrské. Řádně analyzoval postup práce a informovaně konzultoval všechna kritická rozhodnutí.

Celkové hodnocení 99 /100 (A)

Splnění zadání vyžadovalo náročnou teoretickou přípravu, kterou student plně zužitkoval ve vlastní kreativní činnosti. Prokázal při tom schopnost samostatné tvůrčí práce napříč matematikou, kryptologií, počítačovým inženýrstvím a experimentální algoritmikou. Dosažené výsledky jsou relevantní pro mezinárodní akademickou obec i průmysl. Práci navrhuji hodnotit stupněm A – výborně.

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále 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. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.