FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Miroslav Pospíšek, CSc.
Student:	Vojtěch Sedlák
Název práce:	Aplikace homomorfního šifrování v praxi
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	10. června 2024

Hodnotící kritéria

1. Splnění zadání

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

Splněny byly všechny body zadání.

2. Písemná část práce 100 / 100 (A)

Bakalářská práce se zabývá kryptografickou metodou úplného homomorfního šifrování (FHE).
Všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Jednotlivé části jsou obsahově vzájemně provázány.
V části popisující tuto metodu (kap. 1 a 2) oceňuji zdůraznění základních principů, srozumitelné a čtivé vysvětlení problematiky v rozsahu a hloubce dané možnostmi bakalářské práce.
Prezentovaný přehled o současném stavu vychází z historického vývoje, je dostatečně informativní a přitom stručný.
Jsou popsána tři schémata FHE, která jsou implementována v open-source knihovně Microsoft SEAL, použité v praktické části.
Je zde také zmíněna odolnost schémat vůči tzv. kvantové hrozbě.
Z diskuze možností praktické aplikace (kap. 3) oceňuji úvahu o kombinaci s protokolem ZKP. Vhodná kombinace různých metod se v praxi ukazuje jako nejúčinnější postup řešení.
Vybrané možnosti praktické aplikace FHE ukazují, že autor byl schopen se v poměrně krátkém čase zorientovat v problematice.
Kapitoly 4 a 5 obsahují popis sestavené praktické ukázky, shrnují autorovy zkušenosti při vývěru open-source knihovny a diskutují vliv základních parametrů metody na kvalitu výsledku šifrování.

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

Praktické použití FHE se často přirovnává k programování v assembleru. Sestavení konkrétní aplikace závisí na volbě vhodné knihovny, která implementuje potřebné schéma a je snadno použitelná. To vyžaduje základní teoretickou znalost problematiky a jisté programátorské zkušenosti.
Autor práce ukázkovou aplikaci sestavil a s její pomocí dokázal zhodnotit základní parametry použitého schématu.
Bonusem této bakalářské práce je jednoduchý výkonnostní test porovnávající sestavenou aplikaci s profesionálně vyvíjeným software.

Příloha obsahuje zdrojovou formu bakalářské práce ve formátu Latex, dále ukázkovou aplikaci, zdrojový kód, přeložené moduly a návod na použití

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

Přehled možností využití homomorfního šifrování ukazuje na jejich vhodnost pro nasazení v mnoha oblastech, ať už jde o aplikace v cloudu nebo zpracování citlivých dat.
Výpočty se zašifrovanými daty jsou často pokládány za něco z oblasti science-fiction.
Tato práce však ukazuje, že to může být realita a že i v relativně velmi krátké době je možno sestavit funkční aplikace.
Může tak být inspirací a impulsem pro využití této metody v praxi.

5. Aktivita studenta

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

Student byl aktivní, dodržoval dohodnuté termíny. Svá řešení průběžně konzultoval a na konzultace byl připraven.

6. Samostatnost studenta

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

Celkové hodnocení 100 /100 (A)

Stránky ZP, které nejvíce ovlivnily hodnocení: Dodržení zadání, časové rozvržení prací, samostatnost, snaha o porozumění problematice, schopnost nalézt potřebné informace a zorientovat se v nich, programátorská zručnost.

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. 52/2021, 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.