FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Ivana Trummová
Student:	Vojtěch Sedlák
Název práce:	Aplikace homomorfního šifrování v praxi
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	9. 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

Cílem práce bylo nastudovat si problematiku homomorfního šifrování a současného state-of-the-art, diskutovat možnosti praktické aplikace a demonstrovat praktickou ukázku. Ke splnění zadání mám menší výhrady, zejména k prvnímu a druhému bodu pokynů (teoretická část práce), která sice rozsahem pokrývá současný stav poznání v oblasti, ale hloubku i kvalitu by mohla mít o mnoho větší.

2. Písemná část práce 65 / 100 (D)

Písemná část práce je, co se týče rozsahu a členění, v pořádku.
Následující body prosím berte jako konstruktivní zpětnou vazbu.
Mám ale výhrady, co se týče tvorby v základu matematického textu, jímž by měl být popis problematiky homomorfního šifrování (kapitola 1 a 2).
Jazykově je práce v pořádku a dobře se čte, ale bohužel je na mnoha místech jazyk nepřesný a chybí definice toho, co přesně autor zamýšlel sdělit.
Konkrétní postřehy:
- šifrový text vs. šifrovaný text (str. 3, str.15) - předpokládám, že autor myslel na obou místech ciphertext, ale vzhledem ke konvenci "ciphertext" = "šifrový text" mi to nebylo vždy jasné
- pojmy definované až potom, co je autor používá (např. bootstrapping, str. 4, nebo BFV, BGV, a CKKS na straně 9)
- str. 3 - "provádět na nich určité operace" je celkem nešťastné vyjádření, klidně bych tam rovnou uvedla příklad pro lepší pochopení kontextu,
- kapitola 1.1 o historii končí rokem 2009 a v pokračování (1.2) je už jen popsáno, které společnosti mají kolik patentů. Informace o patentech neříká o vývoji mnoho - a ačkoli se

autor dalšímu vývoji věnuje v kapitole o schématech, bylo by dobré to v kapitole 1.1 nebo 1.2 zmínit.
- pokud je poprvé použitá zkratka, bylo by vhodné zmínit, z čeho vychází, např. TFHE (str. 5), PHE (str. 5 - tam to je z kontextu jasné, ale je tam pouze český název, ze kterého zkratka nevychází)
- v matematických textech bývá konvencí, že pokud autor píše důkaz, musí být jasné, co dokazuje. V sekci 1.3.1 to jasné není, a navíc chybí např. definice "multiplikativně homomorfní" šifry.
- při odkazování na jiné práce je vhodné přidat zdroj (str. 6, konec sekce 1.3.1, a konec sekce 1.3.3)
- značení vektoru v definici soukromého klíče v sekci 2.1.1 se mi zdá nedostatečné (chtělo by to závorky?)
- sekce 2.2 (BFV): Autor používá pojem "kruh", který nedefinuje, a z kontextu usuzuji, že se jedná o okruh polynomů. Před použitím pojmu matematické struktury, který byl nejspíš přeložen z anglického zdroje, by bylo dobré porovnat to s českými zdroji, jelikož to vzbuzuje dojem chaosu v terminologii.
- v popisu matematických schémat bych se vyhnula používání hodnotících adjektiv (např. sekce 2.2.2, "negativní dopad na velikost dat). Vhodnější by bylo popsat, jak se velikost mění, ne jestli je to pozitivní nebo negativní.
- použití termínu "modulus" je na více místech nesprávné a matoucí

Kapitola 3:
Ačkoli je kapitola obsáhlá, čtivá a dobře členěná, mám občas problém pochopit, co chtěl autor říct:
- sekce 3.1 "Homomorfní šifrování by mohlo nalézt..." - znamená to, že se to používá, nebo ne? Pochopila jsem, že jde o případ, kdy uživatel nepoužívá svůj vlastní program na úpravu fotografií a chce použít webový, nikde to tam ale není zmíněno.
- oceňuji sekci 3.2.1 s vysvětlením aplikace na ZKP
- sekce 3.5 - problematika je zajímavá, ale potřebu homomorfního šifrování jsem pochopila až z obrázku, ne z textu

Highlighty práce:
- dobré a pochopitelné vysvětlení Learning with errors a příklady zašifrování bitu
- zajímavá část o aplikacích homomorfního šifrování

3. Nepísemná část, přílohy 80 /100 (B)

Praktickou část hodnotím známkou B - z mého pohledu po náročné teoretické části kvalitu práce trochu pozvedla, ale měla jsem problémy se spuštěním aplikace. Pokud si stáhnu přílohu a místo příkazů na instalaci závislostí a spuštění programu najdu odkaz na video, nepřijde mi to jako ideální výstup.

4. Hodnocení výsledků, jejich využitelnost 75 /100 (C)

Výsledky ve formě nastudování si problematiky, shrnutí přehledu a jednoduché aplikace hodnotím jako přiměřené k bakalářské práci. Hodnotím však známkou C, vzhledem k problémům výše.

Celkové hodnocení 75 /100 (C)

Celkově hodnotím práci jako relativně zdařilou. Pro známku C jsem se rozhodla z důvodu nesnadné orientace v teoretické části textu (popsáno výše) a z toho, že s praktická ukázka výsledek nevyvážila.
Jsem ale přesvědčená o tom, že téma studenta baví a myslím, že je na místě podpořit zájem o danou problematiku. Vzhledem k tomu, že problémy byly spíš s formulací a ne s faktickou nesprávností, neměla bych vůbec problém, kdyby se komise při dobré obhajobě rozhodla pro lepší známku.

Otázky k obhajobě

1. V úvodu práce uvádíte, že je homomorfní šifrování "revoluční technikou". V čem je to podle vás revoluční?
2. Co hodnotíte jako největší přínos vaší práce?

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.

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.