FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Mgr. Martin Jureček, Ph.D.
Student:	Bc. Hana Svobodová
Název práce:	Pokročilé algoritmy pro sdílení tajemství
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	30. května 2022

Hodnotící kritéria

1. Splnění zadání

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

Všetky body zo zadania práce považujem za splnené.

2. Písemná část práce 85 /100 (B)

Práca je dobre štrukturovaná, má odpovedajúci rozsah a pomerne bohatý zoznam literatúry. Text práce obsahuje niekoľko chýb:
- definícia 2.1 o (k,n)-prahovej schéme zdieľaného tajomstva nie je v súlade s definíciou z článku [1]
- definícia 2.2 obsahuje tri drobné chyby a definícia 2.3 ďalšie dve
- str. 8, 1. odsek: miesto s-s' má byť s+s'
- str. 12, vzťah (3.4): miesto g^x^t má byť g^xt
- str. 28, 1. odsek: "Tím vznikne polynom s náhodnými koeficienty stupně, ale ..." - má byť stupně 2t

Práca obsahuje množstvo dôkazov. U každého dôkazu je vhodné jasne vyznačiť tvrdenie, ktoré je následne dokázané (ako je to napr. u Vety 5.1). Úvod do kvantového počítania je pekne spracovaný. Väčšina schém je prehľadne uvedená v pseudokóde (napr. Pedersenova schéma z kap. 3.1.2 ale nie je v pseudokóde).

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

Nepísomná časť je dôkladne spracovaná, oceňujem množstvo komentárov v kóde. Nemám k tejto časti žiadne výhrady.

4. Hodnocení výsledků, jejich využitelnost 95 /100 (A)

Prínosom práce sú prehľadne spracované schémy pre vytvorenie zdieľaného tajomstva, pričom u každej schémy je uvedený dôkaz jej korektnosti alebo bezpečnostných vlastností. Uvedená práca môže poslúžiť ako príručka obsahujúca bezpečnostnú analýzu jednotlivých schém.

Celkové hodnocení 92 /100 (A)

Práca hlavne v 2. kapitole obsahovala mierne vyšší počet avšak drobných chýb. Inak je pomerne dobre a prehľadne spracovaná a autorka sa nevyhýbala ani matematickým dôkazom, ktoré boli súčasťou bezpečnostnej analýzy jednotlivých schém. Z týchto dôvodov hodnotím túto prácu známkou A.

Otázky k obhajobě

1. Ak uvažujeme Shamirovú schému, tak aký je vzťah medzi funkciou F_I z def. 2.2 a Lagrangeovým interpolačným polynómom popísaným vo vzťahu (2.4)?
2. str. 12, Pedersenová záväzková schéma: sú všetky prvky grupy G_q generátory a ak áno, tak prečo?
3. V závere sa píše, že knižnicu vsssLib je možné rozšíriť o ďalšie algoritmy a funkcionality. O aké konkrétne?

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.