FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Dr.-Ing. Martin Novotný
Student:	Bc. David Pokorný
Název práce:	Analýza postranních kanálů postkvantového podpisu Rainbow
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	27. 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

Předmětem diplomové práce je
1) nalezení a implementace útoku na referenční implementaci postkvantového schématu Rainbow, a
2) návrh a implementace protiopatření proti tomuto útoku.
To jsou dvě samostatné plnohodnotné diplomové práce. Autor splnil obě zadání.

2. Písemná část práce

95 / 100 (A)

Práce je členěna přehledně a logicky, autor systematicky postupuje k cíli. Pro zvládnutí práce si musel autor nastudovat poměrně rozsáhlé partie matematiky, se kterými čtenáře přehledně seznamuje. Autor všechny použité zdroje řádně cituje, seznam literatury obsahuje 23 zdrojů. Přestože je problematika náročná z matematického hlediska, autor dělá maximum pro to, aby text pochopil i nezasvěcený čtenář.
K textu mám jenom drobné výtky:
- Na některých místech textu bych uvítal více podrobností, například v odstavci 6.1 by mohl být popis měřícího pracoviště. Z textu nepřímo vyplývá, že autor v této části práce provedl měření výhradně s použitím přípravku ChipWhisperer-Lite (CW1173) 32-bit Basic Board, tedy použité měřící pracoviště je jiné nežli při měření v odstavci 6.3.
- V matematické části textu bych uvítal odkazy uvádějící, co se do čeho dosazuje. Například, rovnice 4.12 vznikla s použitím rovnice 4.2 (čímž se vyloučí možnost dosazení z rovnice 2.1) a rovnice 4.14 vznikla z rovnice 4.13 dosazením z rovnic 4.3 a 4.6 (což není explicitně uvedeno).
- Z překlepů bych upozornil zejména na rovnici 4.13, kde má (pravděpodobně) na druhém řádku být "inverze T s pruhem", nikoliv "T s pruhem".

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

Přílohy obsahují text práce, jednotlivé proměřované varianty (implementace) schématu Rainbow, měřící skripty, naměřená data a grafy z měření. Vše je přehledně členěno s příslušným popisem.

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

Výsledky z první části diplomové práce (návrh a realizace útoku) již byly publikovány na mezinárodní konferenci DATE 2021. Výsledky druhé části diplomové práce (návrh a realizace protiopatření) bude autor, předpokládám, rovněž publikovat.

Celkové hodnocení 100 /100 (A)

Autor de facto zpracoval dvě obtížná zadání dvou výzkumných diplomových prací. Obě zadání splnil bez výhrad; výsledky prvního zadání jsou již dokonce publikované na mezinárnodní konferenci DATE 2021. Proto si dovoluji komisi navrhnout, aby zvážila navržení předložené diplomové práce na ocenění cenou děkana.

Otázky k obhajobě

Na konci odstavce 6.4.3 uvádíte: "Jelikož neznáme zdroj úniku, pak je vhodné opravit implementační chyby popsané výše a znovu data přeměřit."

Zajímalo by mne, o jaké konkrétní implementační chyby se jedná, zda jste je již opravil a zda jste data znovu přeměřil.

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.

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.