FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	prof. Ing. Róbert Lórencz, CSc.
Student:	Bc. Ondřej Staníček
Název práce:	Útok postranním kanálem na PUF založený na kruhových oscilátorech
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	–

Hodnotící kritéria

1. Splnění zadání

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

Zadání bylo splněno bez výhrad.

2. Písemná část práce 100 / 100 (A)

Rozsah práce odpovídá jejímu obsahu. Práce obsahuje rozsáhlý úvod do problematiky ROPUF a přehled známých metod útoků pomocí postranních kanálů. Autor podrobně popisuje metody použité k provedení útoku na zadanou konstrukci ROPUF a její různé implementace, důkladně vyhodnocuje její zranitelnosti a následně navrhuje odpovídající obranná opatření proti těmto útokům.

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

Nepísemná část je v pořádku a plně funkční.

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

Výsledky práce jsou velmi přínosné a ukazují nové a zajímavé směry útoků pomocí postranních kanálů na ROPUF zadané konstrukce. Rovněž jsou navržený protiopatření proti těmto útokům. Práce byla prezentována na konferenci DSD 2024. Autor práce bude v doktorském studiu pokračování ve výzkumu daného tématu.

Celkové hodnocení

100 /100 (A)

Práce je přínosná pro studium odběrové analýzy vybraných ROPUF. Diskutuje také možnosti obrany proti útokům využívajícím tuto analýzu. Rozsahem i zpracováním tématu ji považuji za velmi zdařilou. Byl jsem součástí její publikace a prezentace na konferenci DSD 2024. Práce má potenciál dále rozvíjet tuto oblast výzkumu. Autor bude ve výzkumu pokračovat v rámci doktorského studia.

Otázky k obhajobě

Jaké jsou obecně možnosti obrany proti útokům na ROPUF (ne nutně pouze proti odběrové analýze)?
Existují typy čítačů, které by mohly kryptoanalýzu tohoto typu ztížit nebo ji dokonce zcela eliminovat?

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.