FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Vojtěch Miškovský, Ph.D.
Student:	Adam Rektořík
Název práce:	Vliv odstupu signálu od šumu na úspěšnost útoku postranním kanálem
Obor / specializace:	Počítačové inženýrství
Vytvořeno dne:	17. 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

Práce splňuje zadání bez výhrad.

2. Písemná část práce

60 / 100 (D)

Písemná zpráva má přiměřený rozsah, je informačně bohatá a neobsahuje zbytečné části. Analytická část i popis experimentů jsou v pořádku, nicméně zcela chybí úvod a závěr práce. Jinak je obsah logicky členěný, mám jen drobnou výhradu, že autor střídá pořadí mikrokontrolér/FPGA napříč kapitolami. V kapitole SNR bych pak uvítal popis výpočtů i matematickým zápisem. Po formální stránce obsahuje práce poměrně velké množství chyb, které se váží především k číslování a odkazování. Na některé plovoucí prvky, především obrázky a výpisy z kódu, není z textu vůbec odkazováno. Při odkazování pak často není uvedeno, na co autor odkazuje (sekci, obrázek,...), takže čtenář může jen hádat, na co je odkazováno. V některých kapitolách pak autor využívá podsekce, aniž by využíval sekce, takže například kapitola 4 obsahuje pouze podsekce 4.0.1 a 4.0.2. Jazykově je zpráva na poměrně vysoké úrovni, kterou ovšem sráží enormní množství překlepů. V bibliografii pak autorovi chybí jeden zdroj, na který v textu odkazuje (pravděpodobně manuál ChipWhisperer). Celkově písemná zpráva působí velmi narychlo sepsaně a autor tak bohužel formálními nedostatky velmi sráží jinak poměrně kvalitní práci.

3. Nepísemná část, přílohy 90 /100 (A)

Nepísemnou část považuji za kvalitní, zdrojové kódy jsou přehledné, většina je vhodně doplněna komentáři, chybí mi pouze komentáře u Verilog zdrojů. Provedené experimenty jsou dostatečně zdokumentované a tudíž snadno opakovatelné.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Výsledky práce považuji za užitečné pro výzkum v oblasti analýzy postranních kanálů. Pro větší průkaznost by bylo třeba provést experimenty na větším množství kryptografických algoritmů, což nebylo součástí zadání, nicméně díky kvalitě nepísemné části je možné experimenty snadno rozšířit. V práci mi ovšem chybí shrnutí a interpretace výsledků v závěru písemné části.

Celkové hodnocení 75 /100 (C)

Autor implementoval šifru Present na dvou různých platformách, navrhl různé způsoby ovlivňování odstupu signálu od šumu a následně vyhodnotil úspěšnost útoku postranním kanálem. Implementace i experimenty jsou kvalitní a autor splnil zadání práce. Výsledky práce jsou bohužel sráženy zásadními nedostatky písemné zprávy. Z tohoto důvodu ji hodnotím stupněm C.

Otázky k obhajobě

Čím si vysvětlujete tak výrazné rozdíly mezi výsledky na MCU a FPGA?
Chystáte se na tématu dále pracovat (např. směrem k diplomové práci) a nasadit experimenty na dalších algoritmech či platformách?

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.