FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	František Kovář
Oponent práce:	Ing. Filip Kodýtek
Název práce:	Use of physically unclonable function to secure wireless communication
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 15. 6. 2020

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	*1=zadání splněno,* ***2=zadání splněno s menšími výhradami,*** *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
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.

Komentář:

1. Study the topic of physically unclonable functions (PUFs).
 - Rešerše v rámci práce byla velmi stručná. Minimálně měl být alespon více do detailu popsán návrh PUFu, který byl využíván.

5. Perform automated testing of the system and its functionality in order to measure reliability parameters, such as false acceptance ratio and false rejection ratio.
 - V práci není zmíněno, jaka byla "false acceptance ratio", bylo vyhodnoceno jen procento úspešně proběhlých autentizací.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*70 (C)*

Popis kritéria:
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.

Komentář:

Kapitola 1 (Analysis) obsahuje pár tvrzení, které nejsou správné, příp. měl být citován zdroj, odkud tato informace pochází. Např.:

- PUF je odolný vůči fyzickým útokům
- ROPUF spadá do kategorie Strong PUF (přičemž nesplňuje definici Strong PUFu)
- Arbiter PUF má 64b challenge - možná jeho jedna konkrétní implementace

Dále v Kapitole 1 byly až příliš stručné popisy různých typů PUF, mohly zde být i nějaké obrázky. Alespoň ROPUF, který je v této práci využíván, tak měl být dostatečně popsán.
V sekci 1.5 nejasně napsaný rozdíl mezi symetrickou a asymetrickou šifrou.

Kapitola 2 má opět příliš stručný popis implementace ROPUF - zda byla imlementace komplětně celá převzata, nebo bylo něco upraveno, není zmíněno kolik je zde kruhových oscilátorů, ... Student zde popisuje využití repetičního kódu pro opravy chyb, ale není vysvětleno proč byla zvolena velikost bloku zrovna 9. Dále není jasné jaký význam, nebo co znamená server a client mode na security device (má to značit rozdíl mezi tím, kdo iniciuje spojení, nebo něco jiného?).

Kapitola 3 (Measurements) obsahuje výsledky z měření. Nejprve v tab. 3.1 vyhodnocuje stabilitu jednotlivých pozic bitů na 6 FPGA. Není ale zmíněno kolik měření bylo provedeno, za jakých podmínek (předpokládám, že jen za stabilních), a jak přesně se vyhodnocení provedlo. To samé platí pro tab 3.2, kde není zmíněno pro kolik FPGA a párů RO bylo vyhodnocení provedeno. Autor měl pro výběr vhodných bitů pro PUF využít již známé metriky, které jsou pro PUF používané. Dle výsledků v tab 3.5 se podařilo dosáhnout 96.7% úspěšnosti autentizace, ale není zmíněné, zda při daných konfiguracích nedochází k false acceptance (např. FPGA1 se autentizuje jako FPGA2).

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*90 (A)*

Popis kritéria:
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

Komentář:

Zdrojové kódy jsou přehledné, místy by si však zasloužily trochu podrobnější komentář. Odevzdané řešení je kompletní a lze použít pro další měření a navázat tak na aktuální práci.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*80 (B)*

Popis kritéria:
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.

Komentář:

Kladně hodnotím skutečnost, že student musel provést značné množství práce pro zprovoznění prototypu, aby mohl provést měření, která byla cílem této práce. Měřící aparát tedy může být opět využit pro případné další práce/výzkum/výuku. Ovšem samotná měření a jejich vyhodnocení mohla být provedena lépe, viz výše uvedené nedostatky.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*
5. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

Proč byla zvolena velikost bloku pro repetiční kód 9?
Jak bylo realizováno měření času generování odpovědi PUF?
Jaké by byly kroky pro zlepšení úspěšnosti autentizace?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*75 (C)*

Popis kritéria:
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.

Text hodnocení:

Student splnil zadání, až na drobné výtky (nepopsaný využitý návrh PUFu, chybějící vyhodnocení false acceptance rate).
Písemná část práce obsahuje řadu nedostatků, jako problematickou vnímám především kapitolu 3 zabývající se měřením a jeho následným vyhodnocením. Zde často chybí popis samotného měření, z jakých dat a jak bylo prováděno vyhodnocení a případné další odůvodnění (např. volba vyhodnocovacích parametrů - zde se student měl inspirovat z předcházející rešerše a využít).
Naopak velmi kladně hodnotím, že student musel provést spoustu práce, aby zprovoznil měřící aparát, který by mohl využít pro splnění cílů této práce.
Práci hodnotím známkou C.

Podpis oponenta práce: