FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Dr.-Ing. Martin Novotný
Student:	Tereza Horníčková
Název práce:	Odběrová analýza kryptografického procesoru CEC 1702
Obor / specializace:	Počítačové inženýrství
Vytvořeno dne:	31. 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

Předložená bakalářská práce reprezentuje téměř dva roky velkého úsilí, které započalo v srpnu 2020. Sestává ze dvou částí; úkolem první části bylo zprovoznit vývojový proces (design flow) procesoru CEC1702 a úkolem druhé části bylo zanalyzovat odolnost procesoru proti korelační odběrové analýze v momentě, kdy na něm běží šifra AES.
Obě části práce byly bez výhrad splněny. Rád bych zdůraznil, že zejména první část práce byla mimořádně obtížná a frustrující, vzhledem k neprofesionalitě firmy MikroElekronika Beograd, https://www.mikroe.com/, která je bohužel nejen dodavatelem vývojových přípravků Clicker 2 (nikdy nebyly funkční, ani když nám zaslali kusy s údajně správně naprogramovanými EFUSE bity), ale také vývojářem vývojového prostředí mikroC pro for ARM, které je poněkud svérázné (překladač z C není case-sensitive, nerespektuje prioritu stanovenou závorkami, apod.). Tyto odhalené chyby jsou zdokumentovány v předložené bakalářské práci. Bohužel, pro vývoj firmware pro CEC 1702 nelze (zatím) použít žádné jiné prostředí, pokud vývojář používá některé specifické rysy tohoto procesoru.
Druhá část práce se zabývá korelační odběrovou analýzou procesoru CEC 1702 s běžící šifrou AES. Jsou analyzovány dvě varianty firmware - varianta s čistě softwarovou implementací AES a varianta, která využívá hardwarový akcelerátor. Rovněž je provedena analýza procesoru STM32 se softwarovou variantou AES.

2. Písemná část práce

75 / 100 (C)

Pokud by text práce zdokumentoval celý rozsah odvedené práce, potom by svým rozsahem výrazně překročil horní doporučenou mez. Text se svým rozsahem drží doporučených mezí, přesto bych přivítal např. podrobnější zdokumentování nalezených chyb v překladači z C, či ukázky komunikace mezi řídícím počítačem a firmware.

3. Nepísemná část, přílohy 95 /100 (A)

Přiložené médium obsahuje jak vytvořený firmware a notebook v Mathematice, tak měřená a analyzovaná data u těch experimentů, kde velikost dat umožňuje jejich uložení na přiložené paměťové médium.

4. Hodnocení výsledků, jejich využitelnost 99 /100 (A)

Předložená práce je důležitá ve dvou směrech:
1) Podařilo se "rozchodit" design flow procesoru CEC 1702. Práce obsahuje rady, jak zapojit přípravek ChipWhisperer s deskou CEC1702 a jak psát program pro CEC1702, pokud se má kompilovat v prostředí mikroC pro for ARM. Pokud je nám známo, toto nebylo zatím nikde zdokumentováno.
2) Zabývá se korelační odběrovou analýzou procesoru CEC1702. Zatímco softwarová varianta AES podlehla útoku, zabudovaný hardwarový akcelerátor AES odolal jak CPA prvního řádu se 100 000 000 průběhů, tak CPA druhého řádu s 10 000 000 průběhů. Zdá se tedy, že je navržen tak, aby těmto útokům odolal. Ani toto zatím nikde nebylo publikováno.

5. Aktivita studenta

- [1] **výborná aktivita**
  [2] velmi dobrá aktivita
  [3] průměrná aktivita
  [4] slabší, ale ještě dostatečná aktivita
  [5] nedostatečná aktivita

Postup prací jsme konzultovali na pravidelných týdenních schůzkách.

6. Samostatnost studenta

- [1] **výborná samostatnost**
  [2] velmi dobrá samostatnost
  [3] průměrná samostatnost
  [4] slabší, ale ještě dostatečná samostatnost
  [5] nedostatečná samostatnost

Bez výhrad.

Celkové hodnocení 95 /100 (A)

Předložená bakalářská práce je novátorská ve dvou směrech:
1) Podařilo se "rozchodit" design flow procesoru CEC 1702. Práce obsahuje rady, jak zapojit přípravek ChipWhisperer s deskou CEC1702 a jak psát program pro CEC1702, pokud se má kompilovat v prostředí mikroC pro for ARM. Pokud je nám známo, toto nebylo zatím nikde zdokumentováno.
2) Zabývá se korelační odběrovou analýzou procesoru CEC1702. Zatímco softwarová varianta AES podlehla útoku, zabudovaný hardwarový akcelerátor AES odolal jak CPA prvního řádu se 100 000 000 průběhů, tak CPA druhého řádu s 10 000 000 průběhů. Zdá se

tedy, že je navržen tak, aby těmto útokům odolal. Ani toto zatím nikde nebylo publikováno.
Přivítal bych pouze, kdyby dosažené výsledky byly doprovozeny podrobnější dokumentací, ale v tom případě by práce pravděpodobně převýšila horní doporučenou mez.
Vzhledem k rozsahu a kvalitě odvedené práce si dovoluji komisi navrhnout, aby zvážila navržení předložené práce na cenu děkana.

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.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

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.