Posudek oponenta bakalářské práce

Student: Koleček František
Téma: Generování fyzicky neklonovatelné funkce (id 20868)
Oponent: Bidlo Michal, Ing., Ph.D., UPSY FIT VUT

1. Náročnost zadání **méně obtížné zadání**

Práce zkoumá možnost využití specifických fyzických vlastností zařízení pro účely tvorby tzv. neklonovatelné funkce. Jedná se o pokročilou problematiku využití elektronických systémů, jejíž náročnost závisí na použité technice a zařízení. Student zvolil kombinaci mikrokontroleru a paměti typu SRAM. Zvolený postup realizace v tomto případě považuji za méně obtížný - byl použit prakticky pouze postup vyčítání dat z paměti s doplněním některých dalších technik, následné analýzy a zpracování výsledků.

2. Splnění požadavků zadání **zadání splněno**

Zadání považuji za splněné, mohlo však být věnováno více úsilí k dosažení realizace, která by přinesla něco zajímavějšího. Dle mého názoru byla zvolena ta nejsnazší cesta.

3. Rozsah technické zprávy **je v obvyklém rozmezí**

4. Prezentační úroveň předložené práce **65 b. (D)**

Práce má logickou stavbu, kladně hodnotím bohaté a srozumitelné popisy množství různých technik použitelných pro realizaci neklonovatelných funkcí.

Méně srozumitelná mi přijde vlastní implementační část - např. není jednoznačně definován "index řádku" na obr. 4.4 (ani není tento pojem nikde vysvětlen v textu), dále obr. 2.5 nemá v textu adekvátní vysvětlení - na str. 27 je sice snaha o popis tohoto algoritmu, ale ten je odlišný od toho, co je na obrázku. Jedná se o klíčové techniky (hlavní přínos práce), proto bych očekával jejich precizní specifikaci.

5. Formální úprava technické zprávy **70 b. (C)**

Práce obsahuje větší množství překlepů a gramatických nedostatků, které sice nemají zásadní vliv na srozumitelnost, ale snižují požitek ze čtení a kvalitní práce by je obsahovat neměla. Dva příklady za všechny:

Str. 19:
"Dále by na základě znalostí získaných experimentací měl být navržena aplikace, která bude využívat zkoumaných fyzických vlastností za účely identifikace zařízení."

Str. 21:
"Díky domu, že pracuji se soubory vytvořené z paměti,..."

Formální stránku práce tedy hodnotím lehce podprůměrně.

6. Práce s literaturou **50 b. (E)**

Převzaté části jsou náležitě citovány. Na některých místech, kde se hodí spíše odkaz na web, však tato informace chybí, např. na str. 20 u knihovny Pillow nebo u konkrétního modelu použitého mikrokontroleru.

Závažným nedostatkem této části práce je nízký počet referencí (pouze 6, z nichž 3 odkazují na obecnou encyklopedii Wikipedia). U práce tohoto typu bych uvítal např. právě odkazy z oblasti kryptografie, odborné publikace z oboru technologie výroby pamětí atd.

Tuto část práce hodnotím tedy jako silně podprůměrnou.

7. Realizační výstup **50 b. (E)**

V rámci práce byla implementována jednoduchá metoda pro identifikaci zařízení (mikrokontroleru) na základě jeho nahodilých výrobních charakteristik (konkrétně v části vnitřní paměti SRAM), které byly využity pro fyzicky neklononvatelnou funkci zajišťující identifikaci zařízení.

Implementace nejdůležitější části na mikrokontroleru sestává z JEDINÉ funkce (cca 1,5 kB zdrojového textu v C) vyčítající obsah části paměti a jeho uložení do podoby matice bytů. Pomocné skripty realizují vizualizaci tohoto obsahu v grafické podobě, prosté srovnávání obsahů a jednoduchý algoritmus identifikace. Množství implementační práce považuji za podprůměrné, nevidím zde ani snahu o realizaci nějaké pokročilejší techniky.

Celkové uspořádání realizačního výstupu sestává z několika oddělených částí, postrádám zde uživatelský modul umožňující pohodlnou obsluhu bez nutnosti provádět řadu kroků ručně, které by bylo možné sladno automatizovat. Takový modul sice nebyl explicitně předmětem zadání, nicméně pro praktické využití bych jej zde považoval za nutnost. Stoupla by tím úroveň realizačního výstupu, který je jinak velice jednoduchý a působí spíše nedokončeným dojmem.

8. Využitelnost výsledků

Práce poskytuje pouze nezbytný základ pro seriózní uplatnění principu neklonovatelných funkcí. Po doplnění uživatelského modulu bych nicméně viděl dobrou využitelnost ve výuce vestavěných systémů (z důvodu jednoduchosti a snadné pochopitelnosti), kde by se tak daly prezentovat a názorně demonstrovat pokročilé vlastnosti elektronických zařízení.

9. Otázky k obhajobě

1. Na základě čeho jste navrhl algoritmus "druhé verze fyzicky neklonovatelné funkce" popsaný na str. 27, případně obrázkem 4.5? Je to Vaše dílo nebo pochází z literatury?
2. Jaký je Váš názor na případné provedení analýzy navržené metody v závislosti na externí teplotě nebo odchylkách napájecího napětí v povolených mezích? Budou mít podle Vás tyto faktory vliv na výsledky?

10. Souhrnné hodnocení **55 b. dostatečně (E)**

Práce řeší zajímavé a aktuální téma, její pojetí a realizaci však považuji za podprůměrné. Práce má zejména nedostatky v části referencí a v části implementace. S přihlédnutím k nízké náročnosti zvolené realizace navrhuji proto hodnocení známkou E.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 10. června 2020

Bidlo Michal, Ing., Ph.D.
oponent