POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Návrh generátorů pravých náhodných čísel vhodných pro integrované obvody**
Jméno autora:	**Ing. Vlastimil Kotě**
Typ práce:	Disertační
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra mikroelektroniky
Oponent práce:	Doc. Ing. Jiří Háze, Ph.D.
Pracoviště oponenta práce:	Ústav mikroelektroniky, FEKT, VUT v Brně

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání

Zvolené téma disertace je velmi aktuální vzhledem k rostoucím požadavkům na zabezpečení dat v současném světě, který je globálně propojen a kde je tzv. kybernetická bezpečnost jedním z kritických úkolů ochrany jak soukromých, tak státních či vojenských informací. Téma práce tedy reflektuje tuto poptávku a lze jej z hlediska náročnosti a ambicí autora řadit mezi náročnější.

Splnění zadání

Disertační práce v plném rozsahu splňuje všechna dílčí zadání bez jakýchkoli výhrad.

Zvolený postup řešení

Zvolený postup řešení disertační práce je správný, má logický vývoj a jasně postupuje od zadání, přes řešení až po závěr. Po úvodním seznámení s problematikou a rozborem současného stavu poznání vč. testovacích metod autor prezentuje hlavní jádro disertace a tím je nový princip (struktura) pro generátory náhodných čísel. Hlavními kritérii pro návrh byla bezpečnost generování náhodných čísel a možnost implementace v integrované podobě na čipu.

Autor disertace navrhnul nový TRNG (generátor pravých náhodných čísel) s časově multiplexovanými metastabilními zdroji náhodnosti v režimu pipelined tzn. řetězení. Díky navrženému řešení dosáhl autor pozoruhodných výsledků, které umožňují dosáhnout vyšší míry zabezpečení TRNG, jeho implementaci na čipu při současném dosažení nízké spotřeby cca 73 uW (a tedy i využití v bateriově napájených zařízeních) a zároveň vysokému datovému toku až 20 Mb/s. Navrženou strukturu pak autor více zobecnil se zaměřením na ještě vyšší bezpečnost generování sekvencí náhodných čísel s využitím von Nemannova korektoru a odhadu entropie. I tento obvod byl realizován na čipu ve 130 nm technologii CMOS od STMicroelectronics. Veškerý návrh je velmi dobře podložen i potřebným matematickým aparátem, což jen potvrzuje odbornou erudici doktoranda.

Dalším originálním výstupem je vývoj a využití nových behaviorálních modelů navržených TRNG, což významně urychluje simulace navržených struktur. Pokud by totiž probíhaly simulace navržených obvodů s běžnými součástkami, pak by trvaly i několik dnů.

V neposlední řadě je nutné také vyzdvihnout doplnění metodologie návrhu layoutu samotného čipu o krok, který autor nazval jako „předrozmístění" – Pre-placement. Princip této metody a výhody, které poskytuje, jsou značné. Zrychluje výrazně návrhy topologie čipu, významně pomáhá k automatizaci procesu návrhu topologie čipu a umožňuje dosáhnout i optimální plochy navrženého čipu.

Lze tedy konstatovat hned čtyři významné poznatky z hlediska disertability celé práce, jejíž výsledky lze využít v praxi ať už v bezpečnostních systémech pracujících v kyberprostoru, jež pracují s daty vč. těch citlivých, které je nutné chránit před zcizením a zneužitím, tak také v design centrech technologických firem, které zcela určitě mohou využít uvedené metody simulací a návrhu topologie čipu.

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

Odborná úroveň
Odborná úroveň práce splňuje náročné požadavky kladené na vypracování disertační práce. Autor pracuje s velkým množstvím zdrojů, které důkladně prostudoval a využil při vlastním výzkumu. Oceňuji, že práce má výrazný přesah do praxe a není to jen tzv. výzkum do šuplíku.

Formální a jazyková úroveň, rozsah práce
Práce je psaná v anglickém jazyce na 154 stranách textu a je rozdělena do celkem 8 kapitol vč. závěru. Je psaná přehledně, srozumitelně, pěknou čtivou angličtinou. Kapitoly na sebe logicky navazují. Drobné připomínky mám k rozdělování slov na konci řádku (zřejmě automatizované), kdy jsou některá slova rozdělena z hlediska gramatiky nesmyslně, a myslím si, že si tento nedostatek mohl autor pohlídat. Narazil jsem na velmi malé množství překlepů nebo chyb ve spellingu. Dále si myslím, že norma požaduje umísťování popisků tabulek nad tabulkami. Autor je má umístěné pod tabulkou. Poslední poznámkou k formální stránce práce mám u rovnic, kde by měla být použita čárka za rovnicí, pokud je tato součástí věty, která za rovnicí pokračuje.

Výběr zdrojů, korektnost citací
Student pracuje s velkým množstvím studijních podkladů, zejména článků a příspěvků v prestižních časopisech, na mezinárodních konferencích, ale také různé knihy nebo datasheety. Skladba těchto zdrojů je rozmanitá, vyvážená a z velké části ne starší jak 5-6 let. Literatura je řádně citována v celém textu disertační práce.

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Konstatuji na základě výše uvedených faktů, že student doktorského studia Ing. Vlastimil Kotě, zpracoval svou disertační práci na vysoké úrovni s minimem, spíše formálních, chyb. Práce obsahuje řadu původních autorových myšlenek a její výsledky mají značný přesah do praxe. **Na základě těchto zjištění doporučuji tuto disertační práci k obhajobě a udělení doktorandovi vědeckého titulu doktor – Ph.D.**

Otázky k obhajobě

1) V kap. 4.3.1. zmiňujete nutnost velmi přesného zdroje napájení. Je tedy navržený TRNG nějak výrazně citlivý na změnu napájecího napětí? Předpokládal bych naopak vysokou imunitu v tomto směru a tedy ani nutnost využití tohoto přesného zdroje.
2) Na str. 78 1. odstavec používáte přesný generátor hodinového signálu. Proč není implementován na čipu?
3) Dá se nějakým způsobem odbourat teplotní závislost generování sekvencí náhodných čísel jak je patrné z obr. 4.16? Jedná se zejména o vyšší teploty 85 °C.
4) V kap. 5.5 uvádíte, že je nutný další výzkum v oblasti bezpečnosti použití TRNG z hlediska odolnosti vůči záměrným škodlivým útokům. Kam se tento výzkum bude ubírat?
5) Zaujala mne vaše metoda pre-placement při návrhu topologie čipu. Jestliže seskupujete bloky, které mají stejné nebo podobné vlastnosti a tato seskupení pak rozmísťujete na čipu, neovlivní to vzdálenosti z hlediska propojování vodivými cestami? Nejsou tato propojení v konečném důsledku delší než při běžném návrhu topologie? Dá se váš nástroj pre-placement použít i na jiné technologie než jste použil vy ve své práci?
6) S ohledem na velmi zajímavé výsledky vaší práce, bych očekával, že bude vaší snahou je prezentovat v prestižních impaktovaných časopisech nebo na mezinárodních konferencích. Proč tedy „jen“ lokální zaměření (Radioengineering, EDS, Student, EMEA)?

Datum: 17.12.2018 Podpis: