POLITECHNIKA GDAŃSKA
WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

Katedra Systemów Mikroelektronicznych
prof. dr hab. inż. Stanisław Szczepański
Wydział Elektroniki, Telekomunikacji i Informatyki
Politechnika Gdańska

Recenzja rozprawy doktorskiej

mgr. inż. Michała Melosika

zatytułowanej: ***Rekonfigurowalny hybrydowy generator chaotyczny dla kryptografii sprzętowej***

---

1. Problem badawczy i jego znaczenie

Przedstawiona do recenzji rozprawa doktorska mgr. inż. Michała Melosika dotyczy opracowania nowej klasy generatora chaotycznego o strukturze hybrydowej (programowo-sprzętowej), cechującego się zwiększoną odpornością na ataki sprzętowe dokonywane poprzez tzw. trojany sprzętowe. Zgodnie z podaną w pracy definicją **za trojan sprzętowy uważa się:** *dodatkowy obwód lub zmianę (parametrów, połączeń) wprowadzoną do układu z wrogim zamiarem, która nie może zostać wykryta w ramach podstawowego procesu testowania.*

W przeprowadzonych badaniach Autor pracy trafnie zastosował metodę modelowania generatora hybrydowego w języku VHDL-AMS, pozwalającą na jednoczesną symulację części analogowej i cyfrowej. W realizacji sprzętowej modułu analogowego wykorzystał profesjonalny zestaw matryc programowalnych typu FPAA (Field Programmable Analog Array). W rozważaniach teoretycznych Autor dochodzi do ważnego wniosku, że konstrukcja modułowa zwiększa poziom bezpieczeństwa modelu hybrydowego poprzez niezależne użycie części analogowej i cyfrowej. W kolejnej części pracy, na tle szerokiego przeglądu literatury światowej,

POLITECHNIKA GDAŃSKA
Wydział Elektroniki,
Telekomunikacji i Informatyki
ul. G. Narutowicza 11/12
80-233 Gdańsk
www.eti.pg.gda.pl

Sekretariat katedry:
tel:. +48 58 347 18 45
fax: +48 58 347 23 78
e-mail: ksmi@ue.eti.pg.gda.pl

dotyczącej systemów kryptografii sprzętowej Doktorant wnikliwie przedstawił praktyczne możliwości zastosowań technologii programowalnych układów cyfrowych FPGA (Field Programmable Gate Array) oraz specjalizowanych układów scalonych typu ASIC (Application Specific Integrated Circuit). Wiele też uwagi poświęcił zagadnieniom analizy z wykorzystaniem nowych modeli trojanów sprzętowych, jak również problematyce testów stosowanych do wykrywania tego typu zagrożeń i aktywności w praktycznych realizacjach heterogenicznych systemów mikroelektronicznych, np. w urządzeniach mobilnych z systemami wbudowanymi. Praca ma charakter interdyscyplinarny i odnosi się do wielu istotnych problemów naukowych, zarówno teoretycznych jak i aplikacyjnych z zakresu współczesnej informatyki, elektroniki, fizyki, telekomunikacji i innych dyscyplin oraz specjalności technicznych.

2. Wkład autora

Rozprawa doktorska mgr. inż. Michała Melosika w przeważającej części jest teoretyczno-koncepcyjna, zawiera też istotne wyniki z przeprowadzonych badań symulacyjnych i w mniejszym stopniu z badań eksperymentalnych. Składa się ona z 7 rozdziałów, 2 odrębnych spisów rysunków i tabel oraz 84 pozycji bibliografii. Praca zaczyna się od zwięzłego wstępu, w którym Doktorant ogólnie charakteryzuje projektowanie kryptograficznych systemów wbudowanych z uwzględnieniem powiązań między informatyką i elektroniką. Ogólnie też przedstawia klasyfikację metod bezpieczeństwa i zagrożeń w systemach wbudowanych. Można również uznać, że w kolejnych 2 podpunktach tego rozdziału w stopniu wystarczającym sformułowane zostały teza (w pracy teza nie została określona wprost) oraz cel i zakres pracy, odnoszące się do poprawy bezpieczeństwa systemów wbudowanych w warstwie sprzętowej.

W rozdziale drugim Autor podał podstawowe wymagania dotyczące bezpieczeństwa generatorów losowych ze szczególnym uwzględnieniem generatorów wartości zalążkowych. Podano charakterystyki wybranych komercyjnych modułów kryptograficznych. Rozważane były też problemy ograniczeń technologicznych w realizacjach generatorów losowych i zalążkowych.

W rozdziale trzecim przybliżono znaczenie korekcji von Neumana w zwiększeniu różnorodności występowania bitów zalążkowych. Podane zostały podstawy teoretyczne testu 0-1 oraz scharakteryzowano nową metodę rozwiązania problemu nadpróbkowania opartą

na kryterium częstotliwościowym. W kolejnych badaniach kryterium to zostało użyte przez Autora pracy w porównaniu z metodą informacji wzajemnej.

Rozdział czwarty obejmuje opis poziomów bezpieczeństwa sprzętowego i klasyfikacje trojanów. Przeprowadzono też szczegółową analizę nowych modeli trojanów sprzętowych. Opracowane modele zostały zastosowane do przeprowadzenia nieopisanych do tej pory w literaturze specjalistycznej ataków na znane generatory chaotyczne.

W rozdziale piątym (kluczowym) przedstawiono opracowanie koncepcji nowego hybrydowego generatora chaotycznego o strukturze mieszanej (programowo-sprzętowej). Generator jest nowym rozwiązaniem dla bezpiecznego generowania binarnych sekwencji zalążkowych. W ramach rozdziału opisano sposób tworzenia hybrydowej sekwencji chaotycznej. Odporność na działanie trojanów, scharakteryzowanych wcześniej w rozdziale czwartym, została potwierdzona badaniami symulacyjnymi z wykorzystaniem testu 0-1. Autor pracy zaproponował metodę modelowania generatora hybrydowego w języku VHDL-AMS pozwalającą na jednoczesną symulację części analogowej i cyfrowej. W sprzętowej realizacji modułu analogowego wykorzystano zestaw matryc FPAA.

W ramach rozdziału szóstego badania obejmowały ocenę poziomu bezpieczeństwa sprzętowego hybrydowego generatora chaotycznego. Autor podkreśla, że ocena taka jest ważnym kryterium bezpieczeństwa i do tej pory nie była rozważana w odniesieniu do znanych obwodów chaotycznych. W rozdziale rozważono problem ograniczeń w rejestracji danych do weryfikacji poprawnego działania generatorów zalążkowych. Jednocześnie przeprowadzono analizę poziomu losowości hybrydowej sekwencji chaotycznej z użyciem pakietu *ent*. Analiza ta została rozszerzona o nową metodę porównawczą z kwantowym losowym źródłem odniesienia.

W rozdziale siódmym Autor podsumował wyniki swojej pracy oraz przedstawił oryginalne osiągnięcia w badaniach nad bezpieczeństwem sprzętowym kryptografii chaotycznej.

Zasadnicze zadania badawcze obejmujące istotne zagadnienia teoretyczne, koncepcyjne i symulacyjne zrealizowane zostały w czterech grupach tematycznych, które dotyczą:

- Adaptacji metod do oceny dynamiki chaotycznej generowanej sekwencji binarnej.
- Zdefiniowania problemów bezpieczeństwa w wybranych sprzętowych generatorach chaotycznych.
- Opracowania koncepcji struktury hybrydowej generatora chaotycznego.

- Analizy porównawczej bezpieczeństwa hybrydowego generatora chaotycznego z generatorem kwantowym.

W mojej ocenie recenzowana rozprawa doktorska jest ważnym, autorskim opracowaniem, a osiągnięcia naukowe z przeprowadzonych badań zasługują na uznanie i wysoką ocenę. Na szczególne podkreślenie zasługuje fakt, że najważniejsze wyniki opublikowane zostały w 8 współautorskich artykułach naukowych w tym 5 prac w czasopismach z renomowanej listy JCR (Journal Citation Reports). Między innymi, prace Doktoranta zostały opublikowane w takich czasopismach jak: *Elektronics Letters*, *Bulletin of the Polish Academy of Sciences Technical Sciences*, *Expert Systems with Applications* oraz *International Journal of Numerical Modelling: Electronic Networks, Devices and Fields*. Jestem też przekonany, że opublikowane wyniki badań mają istotne znaczenie praktyczne dla rozwoju współczesnych systemów mikroelektronicznych zarówno implementowanych sprzętowo jak i programowo-sprzętowych.

Do oryginalnych osiągnięć pracy należy zaliczyć:

- Adaptację testu 0-1do wykrywania aktywności trojanów w obwodach chaotycznych.
- Przeprowadzenie analizy podatności obwodów chaotycznych na działanie trojanów sprzętowych i opracowanie nowych modeli trojanów w odniesieniu do ataku sprzętowego na generatory chaotyczne.
- Opracowanie hybrydowego generatora chaotycznego.
- Wyniki z analizy porównawczej poziomu losowości generatora hybrydowego z losowym generatorem kwantowym.

3. Poprawność opracowania

Recenzowana praca została napisana starannie, znalazłem tylko nieliczne błędy literowe i kilka mniej istotnych nieścisłości językowych, które pomijam w mojej opinii. Do niedociągnięć w pracy zaliczam brak odrębnego akapitu w tekście z treścią jawnie postawionej tezy lub zestawu tez dla niniejszej rozprawy. Można też zauważyć, że w przeprowadzonych pracach wyraźnie został ograniczony zakres badań o charakterze eksperymentalnym, (np. z użyciem fizycznych układów FPGA lub ASIC). W kwestii modułowej implementacji sprzętowej systemów kryptograficznych można byłoby również rozważyć wykorzystanie zaawansowanych technologii wertykalnych 3D. Dodatkowe wyniki z tego typu badań, w moim przekonaniu miałyby istotne

znaczenie porównawcze, co zwiększyłyby też potencjalne walory aplikacyjne niniejszego opracowania. Na stronie 52 Doktorant w tekście pomyłkowo zaliczył tranzystory do grupy elementów pasywnych.

4. Wiedza kandydata

W poszczególnych rozdziałach swojej pracy Doktorant profesjonalnie rozważa wiele istotnych aspektów teoretycznych i praktycznych dotyczących ważnych zagadnień współczesnych systemów kryptografii sprzętowej i programowo-sprzętowej, systemów wbudowanych, matryc FPAA i FPGA, techniki mikroprocesorowej oraz układów scalonych typu ASIC i SoC (System on Chip). W przeprowadzonych badaniach umiejętnie wykorzystał szeroką wiedzę z kilku pokrewnych dyscyplin i specjalności, w szczególności z informatyki, mikroelektroniki oraz inżynierii komputerowej. W przeglądowej części rozprawy potwierdził bardzo dobre rozeznanie w krajowej i międzynarodowej literaturze specjalistycznej przedmiotu. Uważam też, że w swojej pracy doktorskiej kompetentnie wykorzystał reprezentatywny zestaw bibliografii z 84 pozycjami odnoszącymi się do różnych dyscyplin i specjalności.

5. Podsumowanie

Biorąc pod uwagę opinie zaprezentowane w poprzednich punktach i wymagania zdefiniowane przez artykuł 13 Ustawy z dnia 14 marca 2003 r. o stopniach i tytule naukowym (z późniejszymi zmianami) moja ocena rozprawy doktorskiej mgr. inż. Michała Melosika pod względem trzech podstawowych kryteriów jest następująca:

A. Czy rozprawa zawiera oryginalne rozwiązanie problemu naukowego?
Odpowiedź: **zdecydowanie TAK**.

B. Czy po przeczytaniu rozprawy zgadzasz się, że kandydat posiada ogólną wiedzę teoretyczną w dyscyplinie Informatyka?
Odpowiedź: **zdecydowanie TAK**.

C. Czy kandydat posiada umiejętność samodzielnego prowadzenia pracy naukowej?
Odpowiedź: **raczej TAK**.

Ponadto, biorąc pod uwagę bardzo dobry poziom naukowy rozprawy oraz współudział w opublikowaniu 8 artykułów z zakresu tematycznego rozprawy (w tym 5 prac w czasopismach umieszczonych na liście JCR) będę wnioskował, w przypadku bardzo dobrego przebiegu publicznej obrony, o wyróżnienie rozprawy doktorskiej.

Gdańsk, dn. 29. 05. 2017 r.

Stanisław Szczepański