Dr hab. inż. Jan Sadecki, prof. PO
Instytut Informatyki
Wydział Elektrotechniki, Automatyki
i Informatyki, Politechnika Opolska
e-mail: j.sadecki@po.opole.pl

Opole, 29 maja 2017 r.

Recenzja rozprawy doktorskiej

mgra inż. Michała Melosika

zatytułowanej:

„Rekonfigurowalny hybrydowy generator chaotyczny dla kryptografii sprzętowej"

1. Problem badawczy i jego znaczenie

Rozprawa doktorska mgra inż. Michała Melosika dotyczy w ogólności problematyki chaotycznej kryptografii sprzętowej, a w szczególności zagadnień skutecznego zapobiegania zagrożeniom pojawiającym się w ostatnich latach ze strony tzw. trojanów sprzętowych w systemach wbudowanych. Tematyka rozprawy ukierunkowana jest w szczególności na opracowanie koncepcji oraz modelu rekonfigurowalnego hybrydowego generatora chaotycznego, wykazującego zwiększony poziom bezpieczeństwa, udokumentowany w pracy przeprowadzoną przez Doktoranta analizą porównawczą w odniesieniu do własności wybranego generatora kwantowego.

Przedstawiona do oceny rozprawa doktorska ma, moim zdaniem, charakter teoretyczno-koncepcyjny i znajduje się w głównym nurcie zagadnień objętych dyscypliną Informatyka, a w szczególności obszarem zainteresowania tzw. inżynierii komputerowej leżącej na styku z dyscypliną Elektronika, reprezentowaną przez warstwę sprzętową modułów bezpieczeństwa.

Tematykę rozprawy uważam za aktualną i nowoczesną. Spektrum problemów, które pojawiły się w trakcie wykonywania związanych z pracą badań i rozważań, jak również aktualność tematyki oraz jej duża ważność praktyczna gwarantują, że zainicjowane w pracy badania bezpośrednio związane z bezpieczeństwem kroptograficznym układów wbudowanych mogą być kontynuowane w przyszłości i być podstawą przyszłych działań wdrożeniowych.

2. Wkład autora

Oceniając pracę pragnę podkreślić, iż została ona wykonana na wysokim poziomie i jest bardzo wartościowa z punktu widzenia pogłębienia wiedzy w zakresie chaotycznej kryptografii sprzętowej oraz w nowej, bardzo aktualnej problematyce trojanów sprzętowych w systemach wbudowanych. Wnosi ona także oryginalny wkład naukowy i potwierdza wysokie kwalifikacje Autora rozprawy. Należy również podkreślić duże praktyczne znaczenie opracowanych rozwiązań, stwarzające istotne potencjalne możliwości ich zastosowania.

Do najważniejszych, oryginalnych osiągnięć uzyskanych w rozprawie można zaliczyć:

1. Dokonanie adaptacji testu 0-1 do wykrywania aktywności trojanów w obwodach chaotycznych oraz przeprowadzenie analizy tego testu pod kątem detekcji chaosu w układach ciągłych jak też wyjaśnienia przypadków nadpróbkowania.
2. Przeprowadzenie dogłębnej analizy dotyczącej podatności obwodów chaotycznych na działanie trojanów sprzętowych.
3. Zaproponowanie koncepcji oraz opracowanie modelu rekonfigurowalnego hybrydowego generatora chaotycznego, wykazującego zwiększony poziom bezpieczeństwa ograniczający zagrożenia pojawiające się ze strony ataków trojanami sprzętowymi. Model ten został opracowany jako generator wartości zalążkowych zabezpieczający generatory pseudolosowe przed reinicjacją taka sama wartością.
4. Przeprowadzenie analizy porównawczej poziomu losowości opracowanego generatora hybrydowego z losowym generatorem kwantowym.

Uzyskane i zaprezentowane w rozprawie oryginalne osiągnięcia Doktoranta mogą stanowić bazę dla potencjalnych przyszłościowych prac wdrożeniowych. Opracowanie ogólnej teorii i koncepcji hybrydowego generatora chaotycznego, co można uznać za spektakularne osiągnięcie Doktoranta, pozwala na wykorzystanie uzyskanych wyników badań do dalszych prac nad bezpieczeństwem współczesnych systemów wbudowanych.

Potwierdzeniem powyższych uwag w zakresie oryginalności, ważności i aktualności prezentowanych w rozprawie rezultatów może być znaczący dorobek publikacyjny Doktoranta. Wyniki swoich badań mgr inż. Michał Melosik przedstawił w 8. artykułach naukowych znajdujących się na liście JCR, 4. artykułach w czasopismach spoza listy JCR, 9. opublikowanych wystąpieniach konferencyjnych oraz w jednym opublikowanym rozdziale w monografii, co daje w sumie 22 opublikowane prace, w tym 8 w większości znaczących publikacji ściśle związanych z tematyką rozprawy doktorskiej. Doktorant brał ponadto udział w kilku grantach, przy czym w jednym z nich był kierownikiem.

3. Poprawność

Autor wykazał umiejętność poprawnego i przekonywującego przedstawiania uzyskanych przez siebie wyników. Styl prezentacji jest dojrzały, zwięzły i przejrzysty, także w zakresie formalistyki matematycznej. Formalna, redakcyjna strona rozprawy jest poprawna; oceny tej nie podważają nieliczne usterki typograficzne.

Stwierdzam, iż rozprawa jest napisana bardzo starannie, układ pracy jest precyzyjny i logiczny, strona graficzna jest wzorowa. Wnioski końcowe uzyskane w pracy są poprawne i interesujące.

Wyniki rozważań zawarte w rozprawie upoważniają do stwierdzenia, iż założone cele pracy zostały w pełni zrealizowane.

Przedstawiona rozprawa dowodzi, że Doktorant umiejętnie korzysta z najnowszej literatury w obranej dziedzinie wiedzy, podchodzi do niej krytycznie, a ponadto potrafi twórczo rozwijać osiągnięcia innych autorów.

Doktorant wykazał się bardzo dobrą znajomością nowoczesnych metod i narzędzi badawczych. Uważam, że praca stanowi samodzielne rozwiązanie przez Autora szeregu zagadnień naukowych

4. Wiedza kandydata

Motywacja dla podjęcia tematu rozprawy wynikła z bardzo dobrze przeprowadzonej przez Autora analizy literatury przedmiotu. Dzięki oczytaniu Autora odzwierciedlony został w wyczerpujący sposób aktualny stan wiedzy w zakresie Informatyki, w problematyce chaotycznej kryptografii sprzętowej, a w szczególności w zakresie zagadnień skutecznego zapobiegania zagrożeniom ze strony tzw. trojanów sprzętowych w systemach wbudowanych. Najistotniejszy z tego punktu widzenia jest tutaj pierwszy rozdział rozprawy (podrozdziały 1.1, 1.2), chociaż liczne komentarze i odwołania do materiałów bibliograficznych, doprecyzowujące aktualną bazę wiedzy niezbędną w omawianych zagadnieniach, mają miejsce praktycznie w każdym z głównych rozdziałów pracy.

Przeprowadzona analiza literatury przedmiotu (wykaz cytowanych pozycji bibliograficznych zawiera 84, w większości aktualne i właściwie dobrane pozycje), świadczy, moim zdaniem, o głębokiej wiedzy Autora, zaś sformułowane w sposób jasny i przekonywujący wnioski przywiodły Autora do sprecyzowania w pełni zrealizowanych celów rozprawy doktorskiej, które wychodzą naprzeciw rzeczywistemu zapotrzebowaniu w obszarze szeroko pojętego bezpieczeństwa kryptograficznego systemów wbudowanych.

O szerokiej, reprezentującej wysoki poziom wiedzy Doktoranta w obszarze poruszanej tematyki przedmiotu świadczy również przywołany już wyżej znaczący dorobek publikacyjny Autora rozprawy.

5. Inne uwagi[1]

W rozprawie doktorskiej nie zauważyłem znaczących błędów i uchybień merytorycznych, które należałoby podnieść. W trakcie zapoznawania się z treścią pracy nasunęło mi się jednak kilka pytań i uwag dyskusyjnych, w tym uwag natury obliczeniowej. Prosiłbym Doktoranta o ewentualne ustosunkowanie się do trzech wyszczególnionych poniżej pytań i uwag dyskusyjnych.

1. W rozdziale 3.2.1 Doktorant przytacza dwa sposoby prezentacji wyników testu 0-1 do detekcji chaosu. Pierwszy z nich („ilościowy") oparty jest o wartość liczby rzeczywistej K (przyjmującej wartości z przedziału [0,1]). Drugi natomiast („graficzny") oparty jest o wykres wykonany na płaszczyźnie (p,q), gdzie wartości te wyznaczane są wg. zależności (3.1). Pytanie moje jest następujące: Jaka jest złożoność obliczeniowa (czasochłonność) powyżej określonych sposobów wykrywania dynamiki chaotycznej bądź dynamiki regularnej dokonywanego wg. każdego z tych sposobów. Ponadto, czy, w obliczu dostępnych dzisiaj bardzo zaawansowanych narzędzi obliczeniowych oraz sprzętowych wykorzystywanych do przetwarzania obrazów (np. technologia CUDA), może być

[1] Opcjonalnie

uzasadnione (jeżeli tak, to w jakich przypadkach) wprowadzenie automatyzmu w wyszukiwaniu sekwencji regularnych na płaszczyźnie (p,q)?

2. Na wstępie podpunktu 5.2 Doktorant zawarł następujące sformułowanie: „W modelu hybrydowym nowa sekwencja chaotyczna tworzona jest z dwóch binarnych sekwencji chaotycznych generowanych niezależnie przez moduł analogowy i cyfrowy. Mieszanie wektorów D i C odbywa się przez zastosowanie operacji XOR". Pytanie moje dotyczy problemu ogólniejszego, a mianowicie celowego zwielokrotniania pewnych jednostek czy też modułów (np. obliczeniowych, sterujących, ...) działających w określonych systemach rzeczywistych celem poprawy np. bezpieczeństwa czy też niezawodności działania całego systemu (np. już wiele lat temu P. Enslow w swojej książce: „Systemy cyfrowe wieloprocesorowe" wspominał o tego typu rozwiązaniu stosownym w instalacjach kosmicznych). Problemem bardzo istotnym w tego typu rozwiązaniach było sformułowanie kryterium, jak spośród wielu rozwiązań wybrać to „właściwe". Można by tu zauważyć na pierwszy rzut oka pewną analogię z propozycją Doktoranta, jednak problem rozważany w dysertacji ma nieco inną naturę. Pytanie moje nawiązuje jednak do powyższego, a mianowicie, czy zdaniem Doktoranta można sobie wyobrazić sytuację uwzględnienia w zaproponowanej przez niego koncepcji generatora hybrydowego jego „mutacji" opartej nie o dwie sekwencje binarne lecz np. o trzy lub więcej binarnych sekwencji chaotycznych, generowanych wg. możliwie różnych sposobów (układów, algorytmów, ...). Kiedy hipotetycznie zdaniem Doktoranta takie rozwiązanie mogłoby być uzasadnione i czy można sobie wyobrazić sytuację, że rozwiązanie takie mogłoby wpłynąć na poprawę bezpieczeństwa.
3. Sprzęt oraz oprogramowanie systemów komputerowych rozwija się obecnie bardzo szybko osiągając coraz większy stopień miniaturyzacji przy jednoczesnym wzroście mocy obliczeniowej, w odniesieniu nawet do najprostszych i powszechnie stosowanych układów informatyki czy też automatyki. Procesory wielordzeniowe są już standardem, a liczba dostępnych w ich strukturze rdzeni stale rośnie. W konsekwencji możliwe staje się rozwiazywanie nawet stosunkowo złożonych zagadnień w „akceptowalnym" czasie m.in. poprzez zastosowanie idei przetwarzania równoległego. Jak ta tendencja może wpłynąć na możliwości oraz kierunki rozwoju technologii bezpieczeństwa (kryptograficznego) w urządzeniach wbudowanych – w odniesieniu np. do autorskich rozwiązań proponowanych w rozprawie doktorskiej

Praca została napisana poprawnym i zrozumiałym stylem. Podkreślam staranność Autora we właściwym zapisywaniu wzorów matematycznych oraz bardzo dobrą stronę graficzną pracy.

W pracy znalazłem zaledwie kila błędów edytorskich, jak np.:

- str.13, 10 wiersz od góry; jest: „... zostanie ...", chyba lepiej brzmi sformułowanie: „... będzie ...",
- str. 14, 4 wiersz od dołu; jest: „... zostać ...", chyba lepiej brzmi sformułowanie: „... być ...",
- str. 15, 8 wiersz od góry; podwójnie użyte słowo „... dwóch ...",
- str.18, 6 wiersz od góry; jest: „... porówna ...", powinno być: „... porównana ...",
- str.21, 6 wiersz od góry; jest: „... ze ...", powinno być: „... że ...",

- str.37, 12 wiersz od dołu; zbędne słowo: „... do ...",
- str. 40, 12 wiersz od dołu; jest: „... mniejszego ...", powinno być: „... krótszego ...",
- str.45, 1 wiersz od dołu; dwa razy użyte słowo: „... przeprowadzone ...",
- str.61, 12 wiersz od góry; niejasna sekwencja słów: „... w dwóch obwodów ...",
- str. 73, 9 wiersz od góry; podwójnie użyte słowo „... układy ...",
- str. 76, 18 wiersz od dołu; podwójnie użyte słowo „... hybrydowego ...",

Błędy te nie wpływają jednak na bardzo dobrą ostateczną ocenę pracy.

6. Podsumowanie

Biorąc pod uwagę opinie zaprezentowane w poprzednich punktach i wymagania zdefiniowane przez artykuł 13 Ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym (z późniejszymi zmianami) [2] moja ocena rozprawy pod względem trzech podstawowych kryteriów jest następująca:

A. Czy rozprawa zawiera oryginalne rozwiązanie problem naukowego? (wybierz jedną opcję stawiając znak **X**)

[X]	[ ]	[ ]	[ ]	[ ]
Zdecydowanie TAK	*Raczej TAK*	*Trudno powiedzieć*	*Raczej NIE*	*Zdecydowanie NIE*

B. Czy po przeczytaniu rozprawy zgadzasz się, że kandydat posiada ogólną wiedzę teoretyczną w dyscyplinie Informatyka lub Automatyka i Robotyka?

[X]	[ ]	[ ]	[ ]	[ ]
Zdecydowanie TAK	*Raczej TAK*	*Trudno powiedzieć*	*Raczej NIE*	*Zdecydowanie NIE*

C. Czy kandydat posiada umiejętność samodzielnego prowadzenia pracy naukowej?

[X]	[ ]	[ ]	[ ]	[ ]
Zdecydowanie TAK	*Raczej TAK*	*Trudno powiedzieć*	*Raczej NIE*	*Zdecydowanie NIE*

Ponadto, biorąc pod uwagę wysoki poziom merytoryczny rozprawy, nowoczesność i aktualność podjętej tematyki, bardzo ciekawe, tak z punktu widzenia teoretycznego jak i praktycznego, wyniki badań, precyzyjnie sformułowane wnioski końcowe oraz bardzo dobrą stronę graficzną pracy rekomenduję wyróżnienie rozprawy doktorskiej.

Jan Sadecki
Podpis

[2] http://www.nauka.gov.pl/g2/oryginal/2013_05/b26ba540a5785d48bee41aec63403b2c.pdf