dr hab. inż. Remigiusz Wiśniewski, prof. UZ
Instytut Sterowania i Systemów Informatycznych
Uniwersytet Zielonogórski

Zielona Góra, 06.05.2025

Recenzja rozprawy doktorskiej mgra inż. Szymona Sarny

System kryptograficzny implementowany w pSoC

Część jawna

Podstawą opracowania recenzji jest uchwała nr 95/2024 Rady Dyscypliny Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne Politechniki Śląskiej z dnia 19 listopada 2024 r.

Ze względu na charakter rozprawy, która zawiera informacje prawnie chronione oraz zgodnie z zarządzeniem nr 206/2021 Rektora Politechniki Śląskiej, recenzja została podzielona na „część jawną" (zawierającą informacje nieobjęte tajemnicą prawnie chronioną) oraz „część tajną" (zawierającą informacje lub odwołującą się do informacji prawnie chronionych).

1. Przedstawienie informacji o ocenianej rozprawie doktorskiej

Praca doktorska Pana mgra inż. Szymona Sarny p.t. „System kryptograficzny implementowany w pSoC" dotyczy opracowania, realizacji oraz praktycznej implementacji systemu kryptograficznego w formie koprocesora. W szczególności, doktorant skupił się przede wszystkim na usprawnieniu koprocesora CryptOne w celu podniesienia efektywności oraz poziomu bezpieczeństwa systemu kryptograficznego. Aby to uzyskać, w ramach rozprawy doktorskiej opracowano szereg metod i technik nakierowanych na podniesienie efektywności oraz bezpieczeństwa systemu kryptograficznego - zarówno na poziomie sprzętowym, programowym, jak i aplikacyjnym. Opracowane i zrealizowane koncepcje zostały bardzo gruntownie zweryfikowane eksperymentalnie, a następnie wdrożone w przedsiębiorstwie współpracującym w ramach programu „doktorat wdrożeniowy".

Uważam, że temat recenzowanej rozprawy doktorskiej Pana mgra inż. Szymona Sarny jest aktualny, interesujący i ważny technicznie. Teza oraz cel pracy zostały sformułowane precyzyjnie, a stopień złożoności, znaczenie naukowe i zakres zadań odpowiadają ustawowym i zwyczajowym wymogom stawianym rozprawie doktorskiej.

2. Ocena merytoryczna rozprawy

Rozprawa stanowi tematycznie spójną całość. Składa się z 8 rozdziałów oraz bibliografii. Zasadniczą część rozprawy stanowią rozdziały 3, 4, 5 oraz 6 i 7, w których przedstawiono opracowane koncepcje – zarówno od strony naukowo-badawczej, jak i wdrożeniowej.

Rozdział 1 zawiera wprowadzenie do tematyki doktoratu. Przedstawiono w nim podstawowe zagadnienia związane z algorytmami szyfrującymi, a także omówiono aspekty bezpieczeństwa systemów kryptograficznych.

Rozdział 2 uzasadnia celowość podjęcia tematu, formułuje cel, zakres oraz tezę pracy. Należy podkreślić, że zarówno cel, jak i tezę określono precyzyjnie i jednoznacznie. Czytelnik nie ma wątpliwości, co Autor chce uzyskać i jakie techniki zastosować.

Rozdział 3 koncentruje się na generatorach liczb losowych. Autor przedstawia dwie najistotniejsze grupy generatorów (pseudolosowe oraz prawdziwie losowe), koncentrując się przede wszystkim na generatorach prawdziwie losowych. Należy w tym miejscu podkreślić rzetelny przegląd stanu wiedzy, który jest podstawą do opracowanej i zrealizowanej przez doktoranta własnej implementacji tego typu generatora.

Rozdział 4 dotyczy protokołów z kluczem jednorazowym. Tu doktorant skupia się przede wszystkim na technikach opartych o algorytm RSA (i pochodnych). [Dalszą treść opisu utajniono i zawarto w „części tajnej" niniejszej recenzji]

Rozdział 5 dotyczy usprawnień wprowadzonych przez doktoranta w celu zwiększenia wydajności i bezpieczeństwa systemu kryptograficznego implementowanego w formie koprocesora. [Dalszą treść opisu utajniono i zawarto w „części „tajnej niniejszej recenzji]

Rozdział 6 szczegółowo omawia aspekty bezpieczeństwa oraz przeprowadzone testy eksperymentalne. [Dalszą treść opisu utajniono i zawarto w „części tajnej" niniejszej recenzji]

Rozdział 7 podsumowuje opracowane koncepcje na tle wdrożonego systemu kryptograficznego, z kolei rozdział 8 konkluduje całą rozprawę, w nim też zawarto wnioski.

Do najważniejszych, oryginalnych elementów rozprawy zaliczam:

- Opracowanie oraz realizacja autorskich metod i technik nakierowanych na podniesienie efektywności oraz bezpieczeństwa systemu kryptograficznego implementowanego w formie koprocesora.
- Zwiększenie efektywności systemu kryptograficznego na poziomie sprzętowym oraz programowym.
- Zwiększenie poziomu bezpieczeństwa systemu kryptograficznego na poziomie programowym oraz aplikacyjnym.
- Implementacja oraz wdrożenie opracowanych koncepcji w przedsiębiorstwie współpracującym w ramach realizacji programu „doktorat wdrożeniowy".
- Przeprowadzenie szeregu badań eksperymentalnych potwierdzających praktyczną skuteczność opracowanych i zrealizowanych rozwiązań.

Podsumowując ten fragment recenzji jednoznacznie stwierdzam, że założony cel pracy został osiągnięty.

3. Uwagi krytyczne, wątpliwości, pytania

Podczas lektury rozprawy doktorskiej pojawiły się uwagi, pytania oraz wątpliwości, które zamieściłem zbiorczo w tym rozdziale. Ze względu na utajnienie fragmentów rozprawy, w tej sekcji zawarłem jedynie komentarze dotyczące aspektów ogólnych, jednocześnie unikając elementów mogących naruszać kwestie tajności. Niniejsza sekcja ma charakter dyskusyjny i dotyczy moich pytań oraz wątpliwości, które pojawiły się w trakcie sporządzania recenzji rozprawy. Jednocześnie chciałbym wyraźnie zaznaczyć, że przedstawione uwagi i sugestie absolutnie nie umniejszają wartości rozprawy doktorskiej.

1. Pierwsza uwaga ogólna: rozprawa doktorska jest generalnie napisana poprawnie, nie dostrzeżono poważniejszych błędów językowych. Największym plusem rozprawy jest wyjątkowo rozległa i bogata wiedza doktoranta w poruszanej tematyce i to zarówno od strony naukowo-badawczej, jak i praktycznej. Natomiast sporym problemem jest odpowiednie „przelanie" wiedzy na „papier". O ile początkowe rozdziały rozprawy czyta się z prawdziwą satysfakcją, to niestety im dalej, tym gorzej. Być może wynika to z faktu trudności wytłumaczenia zagadnień poruszanych w rozdziałach stricte technicznych, niemniej w moim odczuciu zabrakło typowo naukowych przemyśleń i konkluzji. Przede wszystkim brakuje rzetelnego określenia ograniczeń proponowanego rozwiązania – czy są takowe? A jeśli tak, to jakie? Słabością są również zaledwie dwie publikacje naukowe, które powstały w trakcie realizacji doktoratu (jedna w czasopiśmie z listy JCR, druga konferencyjna), choć przypuszczam, że wynika to przede wszystkim ze względu na wdrożeniowy charakter rozprawy, a być może ma też związek z klauzulami poufności. Niemniej uważam, że większa liczba publikacji uwiarygodniłaby wartość naukową opracowanych rozwiązań.

2. [Treść utajniono i zawarto w „części tajnej" niniejszej recenzji].

3. Doktorant w pracy często posługuje się terminem „weryfikacja" w kontekście sprawdzenia, czy zrealizowany produkt jest prawidłowy, np. str. 17, ostatni akapit: „Proces projektowania układów cyfrowych jest rozbudowany, ale w uproszczeniu można przyjąć, że po opisaniu układu w języku opisu sprzętu oraz weryfikacji funkcjonalnej w symulacji dobrą praktyką jest zweryfikowanie działania projektu w układzie FPGA". Tego typu stwierdzeń w pracy jest więcej. Wydaje mi się, że należy w tym przypadku użyć pojęcia „walidacja" nie „weryfikacja" (zwłaszcza w odniesieniu do sprawdzenia funkcjonalności systemu poprzez symulację).

4. Twierdzenie 1: czy jest to twierdzenie autorskie? Jeśli tak, dlaczego autor nie zawarł odpowiedniego dowodu? Jeśli jednak twierdzenie pochodzi ze źródeł zewnętrznych – dlaczego nie przytoczono odpowiednich źródeł (cytowań)?

5. [Treść utajniono i zawarto w „części tajnej" niniejszej recenzji].

4. Ocena końcowa rozprawy

Podsumowując jednoznacznie stwierdzam, że rozprawa doktorska Pana mgra inż. Szymona Sarny stanowi oryginalne rozwiązanie problemu naukowego i spełnia warunki określone w art. 187 ustawy z dnia 20 lipca 2018 r. - *Prawo o szkolnictwie wyższym i nauce.* Autorskie osiągnięcia przedstawione w rozprawie wnoszą istotny wkład w rozwój dyscypliny Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne, wobec czego wnoszę o przyjęcie rozprawy doktorskiej i dopuszczenie jej do publicznej obrony.