dr hab. inż. Paweł Russek, prof. AGH
Instytut Elektroniki
Akademia Górniczo-Hutnicza w Krakowie

Recenzja rozprawy doktorskiej mgr. Inż. Szymona Sarny
pt. „System kryptograficzny implementowany w pSoC"
napisanej pod opieką naukową dr. hab. inż. Roberta Czerwiński, prof. PŚ

1. Podstawa opracowania recenzji

Recenzję przygotowano na prośbę dr hab. inż. Adama Gałuszki, przewodniczącego Rady Dyscypliny Automatyki, Elektroniki, Elektrotechniki i Technologii Kosmicznych Politechniki Śląskiej, na podstawie uchwały nr. 95/2024 tejże Rady.

Recenzję przygotowano zgodnie z wymaganiami ustawy „Prawo o szkolnictwie wyższym i nauce" z dnia 20 lipca 2018 r., w szczególności wytycznymi art. 187.

Mocą uchwały nr. 93/2024 Rady Dziedziny AEEiTK PŚ, rozprawie doktorskiej mgr. inż. Szymona Sarny pt: „System kryptograficzny implementowany w pSoC" nadano status utajnionej. Zgodnie z zarządzeniem nr. 206/2021 Rektora Politechniki Śląskiej nakłada to na recenzenta obowiązek wyodrębnienia części recenzji dotyczącej informacji objętych tajemnicą. Uwagi dotyczące utajnionych treści pracy zostały umieszczone w rozdziale 7.

2. Tytuł, cel i teza pracy.

Rozprawa doktorska przedstawia badania zmierzające do ulepszenia elementów elektronicznego systemu kryptograficznego rozwijanego na bazie koprocesora CryptOne, którego własność intelektualna jest w posiadaniu firmy Digital Core Design.

Celem pracy jest usprawnienie i polepszenie parametrów systemu kryptograficznego w zakresie efektywności i bezpieczeństwa. Poprawę efektywności doktorant osiąga poprzez rozwój architektury procesorów dedykowanych dla wybranych algorytmów kryptograficznych. Poprawa efektywność rozumiana jest jako zwiększenie wydajność obliczeniowej i skrócenie czasu realizacji algorytmów kryptograficznych oraz zmniejszenie wymaganych zasobów sprzętowych.

W zakresie poprawy bezpieczeństwa praca skupia się na atakach na systemy kryptograficzne prowadzonych kanałem pobocznym. Ataki takie umożliwiają złamanie systemu kryptograficznego metodą np. pomiaru czasu działania algorytmu, pobieranej mocy chwilowej, czy analizy promieniowania.

Istotnym elementem opisywanych badań jest także opracowanie autorskich protokołów kryptograficznych działających w oparciu o klucze jednorazowe. Opracowano algorytm szyfrowania typu OTP (ang. One-Time-Password), który jest odporny na ataki kanałem pobocznym i jest pozbawiony wad i ograniczeń rozwiązań opisywanych w literaturze.

Odrębnym zagadaniem przedstawionym w doktoracie jest badanie możliwość realizacji generatora liczb prawdziwie losowych. Generatory liczb pseudolosowych odgrywają podstawową rolę podczas generowania kluczy kryptograficznych i od ich jakości w dużej mierze zależy

bezpieczeństwo systemu szyfrującego. Generatory liczb losowych są istotne także z punktu widzenia odporności systemu kryptograficznego na ataki kanałem pobocznym.

Tytuł rozprawy tj. „System kryptograficzny implementowany w pSoC" nie do końca precyzyjnie oddaje zawartość i tematykę pracy. Chodzi o zastosowaniem skrótu pSoc, który w treści pracy autor prawidłowo rozwija jako angielskojęzyczny termin *programmable System-on-Chip*. W rozumieniu recenzenta termin ten odnosi się do układów zawierających rdzeń procesora wraz z peryferiami (SoC) oraz programowalne zasoby logiczne z rekonfigurowalną siecią połączeń. Przykładem PSoC są na przykład układy Zynq firmy AMD (Xilinx). Na początku rozdziału 2 doktorant napisał, że układ pSoC jest najczęściej implementowany w układach FPGA, otwierając sobie tym samym pole do szerszej interpretacji, ale zdaniem recenzenta takie rozumienie pojęcia pSoC nie jest powszechnie przyjęte w środowisku. Niezależnie jednak od szczegółowego rozumienia skrótu pSoC, w żadnej merytorycznej części pracy doktorant nie powołuje się bezpośrednio na układy pSoC wykorzystane przy realizacji badań.

Z drugiej strony, lektura pracy przekonuje, że swoim zakresem i ambicjami rozprawa wykracza poza układy pSoC i FPGA, przedstawiając wyniki, które mają ogólniejszy charakter i dotyczą także technologii półprzewodnikowych układów cyfrowych ASIC. Przykładowo, podając ilość potrzebnych zasobów logicznych, doktorant posługuje się metryką FF+LUT, czyli sumą potrzebnych przerzutników i elementów Look-Up-Table, Nie jest to miara typowo stosowana przez projektantów FPGA. W FPGA właściwsze jest posługiwanie się liczbą bloków logicznych, ponieważ liczba FF+LUT w układach FPGA może przełożyć się na liczbę bloków logicznych w zakresie od 100 do 200 procent, w zależności od stopnia upakowania pary LUT+FF w pojedynczym bloku lub w dwóch różnych blokach. Miara FF+LUT wskazuje raczej na ASIC jako docelową platformę dla opracowywanych rozwiązań. Dodatkowo w wielu miejscach pracy, autor wspomina o układach ASIC jako potencjalnie docelowej platformie. Na przykład, w części dotyczącej generatora liczb pseudolosowych autor wspomina o braku możliwości weryfikacji rozwiązania w technologii ASIC.

Uwaga dotycząca tytułu jest także istotna merytorycznie, ponieważ w pracy zaciera się granica pomiędzy stosowaniem opracowywanych rozwiązań w układach FPGA i w technologii ASIC. Nie umniejsza to wartości końcowych wyników rozprawy, ale dla recenzenta docelowa technologia wydaje się mieć istotne znaczenie, ponieważ choć pewne oryginalne rozwiązania i osiągnięcia układowe mogą przynieść korzyści w dowolnej technologii półprzewodnikowej, to optymalizacja dla układów FPGA ma swoją specyfikę i specjalne wymagania. Rozwiązania opracowane dla FPGA są ściśle związane z tą technologią i często tracą zalety lub nawet nie mogą być bezpośrednio przenośne do ASIC. Jasne i czytelne określenie docelowej technologii znacząco ułatwiłoby jednoznaczną ocenę zaproponowanych rozwiązań, zwłaszcza w części dotyczącej akceleratorów obliczeń.

Teza badawcza jaką stawia autora rozprawy brzmi: „Poprzez odpowiednio prowadzony proces projektowy w obszarze sprzętowo-programowo-aplikacyjnym możliwe jest istotne podniesienie bezpieczeństwa i efektywności systemu kryptograficznego". Bardzo dobrze odpowiada ona celowi i tematyce pracy i została przez doktoranta udowodniona. Tak postawiona teza pozostawia jednak pewien niedosyt, ponieważ wydaje się zbyt mało twórcza i odważna. Teza nie prowokuje do stawiania pytań, nowych przemyśleń, dyskusji i rozważań. Choć teza nie decyduje o wartości treści zawartych w rozprawie, to jest ważny element dysertacji doktorskiej. W tym zakresie autorowi zabrakło, zdaniem recenzenta, ciekawszego pomysłu.

We współczesnym cyfrowym świecie, w czasie ciągle rosnącego praktycznego znaczenia bezpieczeństwa danych oraz wzrostu społecznej świadomości i chęci każdego użytkownika

Internetu poprawy osobistego bezpieczeństwa, znaczenie podjętej tematyki badawczej wydaje się oczywiste.

3. Metoda badawcza

Podejmowane badania mają głównie charakter wdrożeniowy, zmierzający do wykorzystania modeli teoretycznych i rozwiązań prototypowych do opracowania rozwiązania praktycznego, w tym wypadku cyfrowego systemu elektronicznego do realizacji algorytmów kryptograficznych.

Praca ma również cechy i charakter badań stosowanych, których celem jest łączenie, ulepszanie i modyfikowanie przez autora znanych i opisanych w literaturze rozwiązań w celu poprawy ich parametrów i praktycznego zastosowania. Na bazie swojego doświadczenia praktycznego, znajomości zagadnień bezpieczeństwa systemów, a także przeprowadzonych eksperymentów praktycznych, autor jest w stanie proponować nowe rozwiązania, które są pozbawione wad wykluczających lub ograniczających ich użycie w praktyce.

Zastosowana przez autora rozprawy metoda badawcza jest zdaniem recenzenta właściwa. Analiza dostępnych w literaturze rozwiązań, a następnie ich twórcze rozwijanie poprzez łączenie metod i rozwiązań z różnych dziedzin jest podstawą badań stosowanych i wdrożeniowych. W praktyce istnieje bardzo niejednoznaczna granica pomiędzy pracą badawczo-rozwojową, a aktywność inżynierską. Działalność polegająca na projektowaniu, konstrukcji, modyfikacji i utrzymaniu efektywnych kosztowo rozwiązań dla rozwiazywania praktycznych problemów to domena pracy inżynierów. W opinii recenzenta, złożona tematyka, wymagany poziom wnioskowania analitycznego, źródła literaturowe jakimi posługuje się autor i w końcu rezultaty przedstawionej pracy nie pozostawia wątpliwości co do jej naukowego charakteru. Dodatkowo erudycja, poziom zaawansowania i warsztat badawczy doktoranta nie pozostawiają wątpliwości, że mamy do czynienie z pracą wykonaną przez badacza, a przy okazji także przez bardzo dobrego inżyniera.

4. Struktury rozprawy

Poza rozdziałami stanowiącymi wstęp (Rozdział 1) i opis celu i tezy rozprawy (Rozdział 2), pracę podzielono na cztery odrębne części merytoryczne, które są od siebie w zasadzie niezależne. Rozdział 3 dotyczy prac nad generatorem liczb prawdziwie losowych; rozdział 4 dotyczy rozbudowy i poprawy protokołów korzystającego z haseł jednorazowych; rozdział 5 opisuje prace dotyczące optymalizacji układu mnożącego dla arytmetyki modularnej; rozdział 6 dotyczy prac nad odpornością rozwijanych rozwiązań na ataki kanałami pobocznymi; rozdział 7 podsumowuje rezultaty pracy w postaci wyników wydajności i wymaganych zasobów sprzętowych uzyskanego praktycznego rozwiązania procesora kryptograficznego.

Początkowe sekcje rozdziałów 3, 4, 5, 6 i 7 stanowią istotny wstęp teoretyczny do poruszane w tych rozdziałach zagadnień. Zawierają ogólne omówienie problemów oraz przegląd istotnych dla przedstawianych rozwiązań źródeł literaturowych. Te części pracy są ważnym elementem rozprawy. Nie tylko tworzą ciekawą narrację i tło badań, ale także stanowią podstawę przekonania recenzenta o szerokiej ogólnej wiedzy teoretyczną doktoranta w dziedzinie praktycznie wykorzystywanych algorytmów, metod ich realizacji sprzętowej i sposobów zapewnienia bezpieczeństwa systemów.

Kolejne sekcje rozdziałów przedstawiają opisy i treści, które są kluczowe dla merytorycznej oceny wartości pracy i unikalnego wkładu doktoranta. Części te zostały utajnione ze względu na

informacje, będące tajemnicą przedsiębiorstwa Digital Core Design. Są to kolejno: podrozdziały 3.3 i 3.4 zawierające wyniki implementacji generatora liczb losowych; podrozdziały 4.5, 4.6 i 4.7 zawierające opis rozbudowy i zasady działania poprawionego protokołu wykorzystującego hasła jednorazowe; podrozdziały 5.6 i 5.7 opisujące implementację i integrację z procesorem CryptOne nowej architektury układu mnożącego; podrozdziały 6.3 i 6.5 w których omówiono wdrożone metody zabezpieczeń przed atakami kanałami pobocznymi oraz cały rozdział 7 w którym podsumowano wdrożenie opracowanych rozwiązań w praktycznym systemie kryptograficznym.

5. Materiały źródłowe i dorobek publikacyjny

W tekście rozprawy autor powołuje się na ponad 100 pozycji literaturowych. Bibliografia zawiera artykułu naukowe i konferencyjne, standardy przemysłowe, ale także popularne artykuły opublikowane w sieci Internet. Są w niej nawet materiały zamieszczone w serwisie YouTube.

Trzy pozycje literaturowe zamieszczone w doktoracie tj. praca magisterska, artykuł konferencyjny (konferencja American Institute of Physics) i artykuł w czasopiśmie Electronics (otwarte czasopismo MDPI o otwartym dostępie IF=2,6), to pozycje stanowiące dorobek publikacyjny doktoranta.

Dorobek publikacyjny doktoranta odgrywa kluczową rolę w ocenie jego kompetencji naukowych, zdolności do prowadzenia samodzielnych badań oraz wkładu w rozwój danej dziedziny wiedzy. Publikacje naukowe są nie tylko dowodem na umiejętność krytycznego myślenia, formułowania hipotez i prowadzenia badań, ale także na zdolność do skutecznego komunikowania wyników i wniosków z tych badań. Spełnienie tych wymagań jest niezbędne do uzyskania stopnia doktora oraz dalszego rozwijania kariery naukowej.

Dorobek publikacyjny doktoranta uznać należy za niewielki, ale w kontekście pracy jest wystarczający do spełnianie wymagań zwyczajowo stawianych kandydatom do uzyskania stopnia doktora. Zrozumiała i oczywista jest trudność publikowania uzyskiwanych wyników w przypadku prowadzenia badań o charakterze wdrożeniowym dla firmy dbającej o poufność stosowanych rozwiązań. Dodatkowo praktyczny i wdrożeniowy charakter prowadzonych z pewnością nie ułatwiał autorowi osiągnięcia wysokiego wskaźnika publikacyjnego.

6. Zawartość i ocena rozprawy w części jawnej

6.1 Rozdział 3 rozprawy

W części opisowej rozdziału trzeciego omówiono znaczenie i wykorzystanie generatorów liczb losowych w systemach cyfrowych. Wskazano na istotną różnicę pomiędzy generatorami pseudolosowym i prawdziwie losowymi. Podano przykłady algorytmów które są wykorzystywane go generacji liczb pseudolosowych. Następnie przedstawiono możliwe źródła losowości dla generatorów prawdziwie losowych w systemach cyfrowych. Wskazano na znaczenie jakie w przypadku generatorów liczb losowych ma określenie i podanie modelu stochastycznego źródła i podkreślono znaczenie dużej wydajność generatorów (liczba generowanych bitów na sekundę).

W rozdziale 3.1 skupiono się na omówieniu potencjalnych źródeł binarnych ciągów prawdziwie losowych w układach FPGA. W rozdziale 3.2 omówiono zaczerpnięte z literatury rozwiązania problemu generowania ciągów losowych w synchronicznych układach sekwencyjnych.

Omawiane rozwiązania są rozwinięciem pomysłu z publikacji (R.C. Fairfield i inni, 1985)[1], polegającego na wykorzystaniu błędu fazy źródeł zegarowych. Przedstawiono także opisaną w pracy (M. Majzoobi i inni, 2011)[2] metodę uzyskiwania losowości stanów cyfrowych poprzez celowe wprowadzanie przerzutników w stany metastabilne.

W podrozdziale 3.3 przestawiono autorską architekturę generatora liczb prawdziwie losowych. W podrozdziale 3.4 przestawiono wyniki jej praktycznej realizacji. Oba podrozdziały utajniono.

6.2 Rozdział 4 rozprawy

Na początku rozdziału czwartego wskazano na zalety systemów z kluczami jednorazowymi (ang. One-Time Pad – OTP). Jako przykład systemu w pełni opierającego się na OTP przywołano rozwiązanie Gilberta Vernama z 1926 roku. Jak podkreślono, choć systemy „prawdziwie" oparte na hasłach jednorazowych są niepraktyczne, to jednak pewne ich cechy mają zastosowane w rozwiązaniach takich jak HOTP (ang. HMAC-based One-Time Password), TOTP (ang. Time-based One-Time Password), czy Yubico OTP.

Rozdział czwarty w całości dotyczy rozwinięcia i poprawienia pomysłu szyfrowania za pomocą haseł jednorazowych o nazwie RSA-OTP zaproponowanego w pracy (J. Jabłoński i M. Wójtowicz, 2014)[3]. Praca ta dotyczy algorytmu o nazwie RSA-OTP działającego w oparciu o algorytm RSA w którym para kluczy RSA jest utajniona i podlega cyklicznym zmianom. Autor zauważa, że przestawiony RSA-OTP trudno uznać za szyfrowanie przy użyciu haseł jednorazowych jednak uznał to rozwiązanie za inspirujące i postanowił go rozwinąć w celu usunięcia istniejących wad.

W dalszej części rozdziału doktorant przedstawia podstawy szyfrowania RSA, metody generacji klucza RSA zgodne ze standardami bezpieczeństwa FIPS i NIST oraz metodę OAEP (ang. Optimal Asymmetric Encryption Padding), która jest praktycznie stosowana w RSA w celu eliminacji jego podatności na kryptoanalizę. Tym samym doktorant wykazuje się wiedzą w zakresie praktycznych zasad i standardów bezpiecznego stosowania popularnego algorytmu szyfrowania RSA.

Ze względu na niedostępność pracy Jabłońskiego i Wójtowicza online przydatny jest podrozdział 4.3 pracy w którym omówiono podstawowe założenia algorytmu RSA-OTP.

Za bardzo wartościowy należy uznać podrozdział 4.4 pracy w którym autor analizuje bezpieczeństwo RSA-OTP, a następnie je podważa proponując autorską metodę ataku która jak wykazuje znacząco obniża teoretyczne bezpieczeństwo tego algorytmu. W rozdziale tym autor udowadnia swoją wiedzę z zakresu teorii liczb, znajomość matematycznych metod przełamywania zabezpieczeń i zdolność praktycznego ich zastosowania. Jak tłumaczy doktorant największe wątpliwości w algorytmie budzi założenie o jawnej wymianie informacji, o przyrostowej zmianie bezwzględnej wartości klucza szyfrującego RSA. Wykorzystując fakt jawności Δn przedstawiony zostaje algorytm ataku na RSA-OTP. Warto zaznaczyć, że przedstawiony schemat ataku ten jest jedynym osiągnięciem doktoranta opisanym w pracy, które nie zostało utajnione.

---

[1] Robert C Fairfield, Robert L Mortenson i KB Coulthart. „An LSI random number generator (RNG)". W: Advances in Cryptology: Proceedings of CRYPTO 84 4., Springer. 1985, s. 203–230.

[2] Mehrdad Majzoobi, Farinaz Koushanfar i Srinivas Devadas. „FPGA-based true random number generation using circuit metastability with adaptive feedback control", Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13. Springer. 2011, s. 17–32.

[3] J Jabłoński i M Wójtowicz. „Bezwarunkowo bezpieczny system kryptograficzny". Logistyka 5 (2014), s. 611–616.

Zastrzeżenia formalne dotyczące rozdziału 4.4 polegają na tym, że na stronie 37 autor umieszcza twierdzenie, którego pozostawia bez dowodu. Dowód może nie jest bardzo skomplikowany, ale formalnie jakiś komentarz powinien się w tej kwestii pojawić.

Pozostała cześć rozdziału zawiera poprawiony i rozbudowany przez autora protokół RSA-OTP i została zastrzeżona z powodu konieczności zapewnienia tajemnicy przedsiębiorstwa.

6.3 Rozdział 5 rozprawy

Rozdział piąty dotyczy realizacji układu mnożącego modulo n, gdzie dodatkowym wyzwaniem projektowym oprócz wydajności i oszczędności w użyciu zasobów sprzętowych jest zapewnienie odporności na ataki kanałem pobocznym np. poprzez ataki czasowe.

W podrozdziale 5.1 omawiana jest istotna dla algorytmów kryptograficznych arytmetyka modularna. Rozdział rozpoczyna się od podania znanych w literaturze algorytmów redukcji modulo. Cały podrozdział 5.2 autor poświęca ważnemu dla realizacji układów kryptograficznych RSA zagadnieniu redukcji Montgomerego, a podrozdział 5.3 przedstawia algorytm redukcji Barreta.

W podrozdziale 5.5 doktorant realizuje przegląd znanych z literatury architektur układów mnożących ze szczególnym naciskiem na algorytmów Radix-n, w tym także w wariantach uwzględniających kodowanie metodą Bootha. W rozdziale tym doktorant wspomina także o istotnych w realizacji mnożenia architekturach układów dodających: sumatorze ze skrośną propagacją przeniesienia (ang. Ripple Carry Ripple Adder – CRA) oraz o sumatorze przechowującym przeniesienia (ang. Carry Save Adder - CSA).

Pozostała cześć rozdziału piątego zawiera szczegóły autorskiej implementacji układu mnożącego i została utajniona.

6.4 Rozdział 6 rozprawy

W rozdziale szóstym doktorant zajmuje się zagadnieniem ataków tzw. kanałem pobocznym. Autor przestawia zasadę ataków i znane przypadki tych ataków opartych na analizie czasu trwania algorytmu, mocy rozpraszanej przez urządzenie (metoda prosta SPA i różnicowa DPA) i analizie promieniowania elektromagnetycznego.

Zagadnienie badania ataków kanałem pobocznym trudno jest umieścić w ramach rygoru metody naukowej, ponieważ jak słusznie zauważa autor "adekwatnym sposobem komunikacji w przypadku implementacji kryptograficznych jest podnoszenie odporności przeciwko atakom kanałem pobocznym, ponieważ w praktyce kolejne zabezpieczenia podnoszą „koszty" ataków, ale nie sprawiają, że są one niemożliwe do przeprowadzenia". Brak adekwatnego rygoru naukowego powoduje, że trudno jednoznacznie ocenić i porównać ilościowo metody przedstawiane w tej części rozprawy. Ta część pracy ma w wielu fragmentach charakter publicystyczny opisujący różne szczególne przypadki znanych ataków. Przykłady pozwalają co prawda wyciągać wnioski ogólne, ale nie dają uniwersalnych przepisów na uniknięcie ataku kanałem pobocznym. Wytarte klawisze czy dźwięk wciskanych klawiszy klawiatury są przykładem ataku kanałem pobocznym który wymyka się zastosowaniu metod naukowych. Autor dzieli jednak metody ataków na metody pasywne, aktywne (ingerujące w działanie układu). Wśród metod pasywnych autor analizuje metodę czasową, rozpraszanie mocy i analizę promieniowania. Do metod aktywnych autor zalicza ingerencję z zasilanie, częstotliwość taktowania i oddziaływanie elektromagnetyczne. Autor analizuje także inwazyjność układu. Podano przykład usuwania obudowy klucza zabezpieczającego acetonem, czy analiza struktury układu scalonego poprzez usuwanie

Część tekstu wycięta ze względu na tajny charakter rozprawy
Olga Nazar

7.1 Rozdział 3 rozprawy

W podrozdziale 3.3 autor przestawił pomysł na architekturę generatora liczb prawdziwie losowych. Do praktycznej realizacji autor zdecydował się na wykorzystanie układów FPGA Cyclone V firmy Intel i środowiska Quartus. Z punktu widzenia przyszłego wdrożenia rozwiązania wybór układu wydaje się nie być najlepszy, ponieważ układy te choć ciągle dostępne produkowane są zastępowane przez nowsze rodziny FPGA. Oczywiście wybór platformy nie przekreśla badawczej wartości tej części pracy i nie wiadomo czy może mieć wpływ na jej walor wdrożeniowy w kontekście wykorzystania wyników w systemie koprocesora CryptOne. Nie jest jasne, czy platformą dla systemu CryptOne może być rodzina nisko budżetowych i niskoenergetycznych układów Cyclone.

Jako przyczynę wyboru Cyclone V autor podaje zastosowanie środowiska programowego Intel Quartus, nie tłumaczy jednak, dlaczego użycie tego środowiska było istotne, ani dlaczego nie zastosowano innych układów obsługiwanych przez Quartus. Być może przyczyn zastosowania Cyclone V należy szukać w źródłach literaturowych na których swoją pracę opiera doktorant. Przedstawione w pracy wyniki bazują bowiem na wynikach pomiaru błędu fazowego zegara wygenerowanego przez oscylator pierścieniowy zrealizowany w układach Cyclone V, które podano w artykule (Oto Petura i inni, 2016)[4].

Implementacja generatora liczb losowych opiera się na rozwinięciu znanej z pracy (R.C. Fairfield i inni, 1985)[5] metodzie wykorzystania błędu fazy sygnału zegarowego o bardzo długim okresie. Jako źródło zegara w Cyclone V doktorant zbudował niestabilny częstotliwościowo generator zegarowy na bazie oscylatora pierścieniowego utworzony z bramek logicznych NOT.

[4] (Oto Petura, Ugo Mureddu, Nathalie Bochard, Viktor Fischer I Lilian Bossuet. „A survey of AIS-20/31 compliant TRNG cores suitable for FPGA devices", 26th international conference on field programmable logic and applications (FPL), IEEE, 2016, s. 1–10.).

[5] Robert C Fairfield, Robert L Mortenson i KB Coulthart. „An LSI random numer generator (RNG)", *Advances in Cryptology: Proceedings of CRYPTO 84 4*.Springer. 1985, s. 203-230.

Należy docenić to, że autor poradził sobie z chaotycznym rozmieszczaniem przez Quartus bramek oscylatora w układzie FPGA poprzez zastosowanie ręcznego przypisania lokalizacji bramek. Chaotyczne rozmieszczenie powodowało brak kontroli nad generowaną częstotliwością zegara w strukturze układu rekonfigurowalnego. Dodatkowo pomocne w obejściu optymalizacji logicznej narzędzi do syntezy, które usuwały oscylatory pierścieniowe jako logikę nadmiarową okazało się wstawienie w ciąg bramek NOT bramki AND. Niestety autor nie podaje mechanizmu w jaki taka bramka "oszukuje" optymalizację logiczną. Nie podaje również w jaki sposób doszedł do takiego właśnie rozwiązania problemu. Zrozumienie mechanizmu wydaje się kluczowe dla przenośności rozwiązania do innych struktur FPGA. Podniesienie tego zagadnienia podyktowana jest ciekawością recenzenta, dla którego dodanie bramki AND nie powinno stanowić przeszkody dla realizacji optymalizacji logicznej długiego łańcucha bramek.

Ostatecznie doktorant przetestował praktycznie generatora liczb prawdziwie losowych według pomysłu zaproponowanego w pracy (K. Wold i C.H. Tan, 2009)[6] Architekturę tą cechuje poprawiona wydajność w stosunku do oryginalnego pomysłu R.C. Fairfielda i innych, oraz to, że dla tej architektury jej twórcy podają model stochastyczny co stanowi podstawę teoretycznych rozważań doktoranta. Nie bez znaczenie w tym zakresie okazały się wyniki pomiarów błędu fazy sygnału zegarowego w Cyclone V podane w pracy (Oto Petura i inni, 2016), które pozwoliły na określenie odpowiednich parametrów implementacji tego generatora.

Jednak, wątpliwości recenzenta budzi wiarygodność podanej przez Oto Petura i innych wartości błędu fazy, którą określono jako 3 ps. Jak zauważył doktorant, „wartość [błędu fazy] może być rzędu pojedynczych pikosekund, a jej zmierzenie wymaga specjalistycznego sprzętu pomiarowego". Tymczasem w pracy, na którą powołuje się autor stwierdzono jedynie, że do pomiaru błędu fazy użyto oscyloskopu Lecroy WaveRunner 640ZI o paśmie 4 GHz i częstotliwości próbkowania 40 GS/s. Problematyczne jest, czy pomiar błędu fazy o wartości 3 ps w ogóle kwalifikuje się do pomiarów oscyloskopowych. Warto także dodać, że rozdzielczość czasowa użytego oscyloskopu WaveRunner według karty katalogowej wynosi 20 ps. Być może zastosowano dodatkowe „sztuczki" i założenia, których niestety w artykule nie opisano. W związku z powyższym należy odnosić się do wartości 3 ps z dużą ostrożnością.

Oczywiście doktorant przeprowadził eksperyment, zebrał pomiary i przeanalizował wyniki przy pomocy testów statystycznych otrzymując satysfakcjonujące wyniki. Zdaniem recenzenta, architektura zastosowanego generatora liczb powoduje, że poddanie w wątpliwość wartości założonego błędu fazy rzutuje na to, czy zrealizowany generator to generator liczb prawdziwie losowych czy tylko pseudolosowych. Inaczej mówiąc może się tylko wydawać, że liczby są prawdziwie losowe, bo liczby pseudolosowe często przechodzą testy statystyczne.

Być może udałoby się zweryfikować wartości założonego błędu fazy jakaś metodą pośrednią. Sprawdzenie pewnych założeń dot. parametrów fizycznych platformy Cyclone z pewnością łatwiejsze byłoby dla pierwowzoru generatora z pracy (Fairfield i inni, 1985), dla którego łatwiej byłoby zaobserwować nieprawidłowości w uzyskanych generowanych. Czy zatem przeprowadzono eksperymenty wykluczające pseudolosowy charakter rejestrowanych w eksperymencie danych?

Jest też, o czym wspomina sam doktorant trudny do oszacowania wpływ zjawiska metastabilności, który powoduje, że zastosowany model stochastyczny nie do końca odpowiada rzeczywistym właściwościom generatora liczb.

---

[6] Knut Wold i Chik How Tan. „Analysis and enhancement of random number generator in FPGA based on oscillator rings", International journal of reconfigurable computing 2009.1 (2009), s. 501672.

Część tekstu wycięta ze względu na tajny charakter rozprawy
Olga Nazar

8. Podsumowanie (syntetyczna ocena i konkluzja końcowa)

Celem doktoratu pan Szymona Sarny było opracowanie i wdrożenie cyfrowego systemu kryptograficznego, w taki sposób, aby zwiększyć jego efektywność i bezpieczeństwo na trzech poziomach: sprzętowym, programowym i aplikacyjnym.

Na poziomie sprzętowym skupiono się na optymalizacji układu mnożącego dla algorytmów RSA. Układ mnożący stanowi rozszerzenie instrukcji koprocesora CryptOne. Na poziomie programowym głównym zadaniem była poprawa bezpieczeństwa i zapewnienia integralności protokołów kryptograficznych, a na poziomie bezpieczeństwa programowego - implementacja i weryfikacja mechanizmów chroniących przed atakami kanałem pobocznym. Projekt zawierał również opracowanie oryginalnego generator liczb losowych w FPGA i odpowiednie dla niego stanowisko pomiarowe.

Przeprowadzone badania potwierdziły skuteczność wszystkich działań, udowadniając tezę pracy doktorskiej o znaczącym podniesieniu bezpieczeństwa i efektywności systemu kryptograficznego. Całość prac, pomimo wdrożeniowego i komercyjnego charakteru, objęła również szeroki zakres zadań badawczych, modelowania i testowania. Elementy pracy opierają się na znanych rozwiązaniach, lecz ich połączenie, adaptacja do konkretnej architektury i technologii systemu cyfrowego i wynikające z tego usprawnienia stanowią o oryginalności całej pracy

Wartościową cechą sprzętowej części jest przedstawianie wyników dla wielu różnych układów rekonfigurowalnych FPGA. Doktorant korzysta zarówno z układów firmy Xilinx (aktualnie

firma AMD) jak i Altera (aktualnie firma Intel). Dodatkowo posługuje się różnymi narzędziami EDA tych firm, w zależności od zastosowanej rodziny układów FPGA. Na potrzeby porównania opracowanych rozwiązań z rozwiązaniami prezentowanymi w literaturze, przeprowadza implementację swoich projektów w układach FPGA tożsamych z zastosowanymi w cytowanej literaturze.

Na podstawie przedstawionego doktoratu należy stwierdzić, że doktorant, mgr inż. Szymon Sarna, dysponuje rozległą i pogłębioną wiedzą w zakresie kryptografii, inżynierii sprzętowej i softwarowej, a także bezpieczeństwa systemów kryptograficznych. Należy docenić złożoność i wieloaspektowość podjętej tematyki. Doktorant rozumienie mechanizm zagrożeń i działanie mechanizmów obronnych. Implementacja i weryfikacja mechanizmów zabezpieczających przed atakami kanałem pobocznym oraz analiza podatności wskazują na głębokie zrozumienie problematyki bezpieczeństwa kryptograficznego. Kluczowe umiejętności badawcze, które były wykorzystywane to:

- proponowanie, realizacja i praktyczna weryfikacja nowych architektur procesorów dedykowanych,
- testowanie urządzeń cyfrowych,
- modelowanie zjawisk zachodzących w układach elektronicznych,
- analiza danych i protokołów transmisji danych,
- analiza podatności i realizacja próbnych ataków.

Doktorant realistycznie podchodzi do trudności np. do złożoności problemu ochrony przed atakami kanałem pobocznym, co świadczy o świadomości istnienia ograniczeń i wyzwań technologicznych.

Recenzja zawiera oczywiście pewne wątpliwości. Są to jednak w zasadzie uwagi o charakterze formalnym, porządkowym lub uzupełniającym. Większość postawionych w recenzji pytań wskazuje na elementy pracy wymagające uzupełnienia lub wyjaśnienia. Oczywiste jest, że w opisie zrealizowanych badań doktorant nie mógł zawrzeć wszystkich możliwych informacji. Dlatego pytania recenzenta często wypływają z jego osobistej ciekawości dotyczącej szczegółowych aspektów badań. Należy podkreślić, że uwagi w żaden sposób nie umniejszają wartości rezultatów uzyskanych przez autora. Są raczej istotnym elementem dyskusji naukowej.

Oryginalność, znaczenie naukowe i aplikacyjne pracy, a także wysoki poziom kompetencji badawczych doktoranta oraz praktyczne zastosowanie wyników badań świadczą o tym, że mgr inż. Szymon Sarna spełnił wymagania konieczne do nadania mu stopnia doktora.

Przedstawiona praca doktorska pana mgr. Inż. Szymona Sarny spełnia kryteria stawiane kandydatom w ustawie z dnia 20 lipca 2018 roku - Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2023 r. poz. 742 z późn. zm.). W związku z tym, wnioskuję o dopuszczenie pana mgr. Inż. Szymona Sarny do dalszych etapów postępowania.