Dr hab. inż. Roman Stanisław Deniziak, prof. PŚk
Katedra Systemów Informatycznych
Politechnika Świętokrzyska
ul. 1000-lecia Państwa Polskiego 7
25-314 Kielce

Kielce, 25.04.2025

Recenzja rozprawy doktorskiej dla Rady Naukowej Dyscypliny Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne Politechniki Śląskiej

Tytuł rozprawy: System kryptograficzny implementowany w pSoC

Autor rozprawy: mgr inż. Szymon Sarna

Promotor rozprawy: dr hab. inż. Robert Czerwiński, prof. PŚ

1. Cel, zakres, charakter i teza rozprawy

Tematyka pracy doktorskiej dotyczy problemów z zakresu bezpieczeństwa systemów cyfrowych, a w szczególności obejmuje zagadnienia dotyczące wydajności i bezpieczeństwa systemów kryptograficznych wykonanych w technice System-on-Chip. Punktem wyjścia do badań był system kryptograficzny CryptOne firmy Digital Core Design. Analizując architekturę i możliwości badanego systemu Doktorant wyróżnił cztery obszary, w ramach których możliwe byłoby ulepszenie architektury, zarówno pod kątem wydajności jak i podniesienia bezpieczeństwa. Są to: moduł sprzętowy realizujący operację mnożenia modulo, generator liczb losowych, protokół z kluczami jednorazowymi, zabezpieczenia przed atakami kanałami pobocznymi.

Praca obejmuje zarówno analizę i ocenę istniejących rozwiązań z zakresu wyżej wymienionych zagadnień jak i oryginalne propozycje rozwiązań opracowanych przez Autora. Rozprawa doktorska przedstawia także wyniki wykonanych badań i porównanie opracowanych rozwiązań z istniejącymi. Jednak głównym celem było wdrożenie opracowanych rozwiązań poprzez zaimplementowanie ich w system kryptograficzny CryptoOne. Zatem praca ma charakter badawczo-projektowy. Zakres pracy dotyczy podniesienia bezpieczeństwa i efektywności systemu kryptograficznego oraz wykonania badań mających na celu weryfikację bezpieczeństwa badanych rozwiązań, co zostało sformułowane w postaci następującej tezy rozprawy:

„Poprzez odpowiednio prowadzony proces projektowy w obszarze sprzętowo-programowo-aplikacyjnym możliwe jest istotne podniesienie bezpieczeństwa i efektywności systemu kryptograficznego”.

O ile ogólny sens tezy można wywnioskować na podstawie opisanego celu pracy, to jednak tak sformułowana teza jest niejednoznaczna i mało precyzyjna. Zastrzeżenia budzi przede wszystkim brak wskazania punktu odniesienia (wskazanie konkretnego typu/klasy systemu kryptograficznego), bez czego teza może sugerować możliwość podnoszenia w nieskończoność poziomu bezpieczeństwa i efektywności. Innym zastrzeżeniem jest użycie pojęcia „proces projektowy w obszarze sprzętowo-programowo…". Może to się mylnie kojarzyć z pojęciem „kosyntezy sprzętowo-programowej", co jest zupełnie innym podejściem do optymalizacji wydajności systemów, niż podejście stosowane w pracy.

2. Zawartość rozprawy

Rozprawa doktorska składa się z 8 rozdziałów, bibliografii oraz spisow skrótów, rysunków i tabel. Pierwszy rozdział zawiera wstęp stanowiący wprowadzenie do tematyki rozprawy. W rozdziale 2 Autor przedstawił cel, zakres i tezę pracy. Rozdział 3 dotyczy problemów projektowania sprzętowych generatorów liczb losowych. W rozdziale tym Doktorant przedstawia też własny projekt takiego generatora implementowanego w układach FPGA. Rozdział 4 obejmuje zagadnienia protokołów z kluczami jednorazowymi. W szczególności opisany jest protokół RSA-OTP w tym opis modyfikacji tego protokołu zwiększającej jego bezpieczeństwo. W rozdziale 5 zaprezentowano rozwiązania z zakresu algorytmów dzielenia modulo oraz implementacji sprzętowej tych algorytmów. Przedstawiono tu również implementację układów mnożących opracowaną przez Doktoranta. Rozdział 6 zawiera opis zagadnień związanych z atakami kanałem pobocznym. Doktorant przedstawił tu również wyniki własnych badań i opis zaproponowanych rozwiązań. W rozdziale 7 opisano kompletny system kryptograficzny z wdrożonymi rozwiązaniami opracowanymi przez Doktoranta, a w rozdziale 8 przedstawiono podsumowanie i wnioski.

Zaproponowany układ rozprawy jest logiczny. Na wstępie Autor określił problem badawczy i przedstawił cel pracy. Następnie w kolejnych rozdziałach przedstawił poszczególne problemy badawcze, najpierw opisał aktualnie stosowane rozwiązania a następnie opisał wynik własnych prac. Na zakończenie podsumował uzyskane wyniki w postaci opisu kompletnego systemu oraz wniosków wraz z wykazaniem udowodnienia tezy rozprawy.

3. Analiza źródeł

Bibliografia przedstawiona w autoreferacie zawiera 107 pozycji, obejmujących głównie artykuły w czasopismach zagranicznych i referaty z konferencji międzynarodowych, z czego trzy pozycje to publikacje współautorskie Doktoranta. Znacząca część (około 30) bibliografii stanowią też materiały i dokumentacje techniczne dostępne na stronach internetowych.

Tylko około 30% pozycji literatury są to publikacje z ostatnich 10 lat. W dużej mierze wynika to z faktu, że Doktorant często odwołuje się do klasycznych rozwiązań z przed wielu lat, ale wydaje się, że uwzględnienie kilku najnowszych pozycji, w szczególności prac przeglądowych, np.:

- Hou, Xiaolu, and Jakub Breier. *Cryptography and Embedded Systems Security.* Springer, 2024,
- Kaleem, Muhammad, et al. "Navigating Side-Channel Attacks: A Comprehensive Overview of Cryptographic System Vulnerabilities." *Journal of Computing & Biomedical Informatics* 7.02 (2024),

pozwoliłoby na uzupełnienie bibliografii i być może zaktualizowanie przeglądu istniejących rozwiązań.

Doktorant na początku każdego rozdziału prezentującego wyniki swoich badań z danego zakresu przedstawia dosyć obszernie przegląd prac dotyczących danej tematyki. W tym zakresie bibliografia jest obszerna i wystarczająca. Jedynie we wstępie, gdzie autor powołuje się na wiele podstawowych pojęć i metod z zakresu kryptografii brakuje odniesienia do piśmiennictwa opisującego te zagadnienia.

4. Metodyka badań

Metodyka badań w ogólnym zarysie jest poprawna jednak sprawia wrażenie nieco chaotycznej. Punktem wyjścia jest tutaj system kryptograficzny CryptOne, którego ulepszenie było celem badań. Ulepszenie miało na celu poprawę wydajności przy jak najmniejszym wzroście kosztu oraz poprawę bezpieczeństwa. Jednak Autor nie wychodzi od analizy systemu kryptograficznego będącego przedmiotem badań ale od ogólnych problemów związanych z bezpieczeństwem i wydajnością systemów kryptograficznych, aby w kolejnych etapach określić główne kierunki badań. W efekcie odnosi się wrażenie, że zaproponowane kierunki badań obejmujące: implementację generatora liczb losowych, opracowanie protokołu z kluczami jednorazowymi, architektury modułów sprzętowych realizujących operację mnożenia modulo oraz zabezpieczenia przed atakami kanałami pobocznymi, dotyczą arbitralnie wybranych problemów a nie wynikają z obranej metodyki badawczej i celu badań. Dopiero w końcowej części pracy następuje zbieżność kierunków badawczych poprzez wdrożenie uzyskanych wyników w docelowym systemie kryptograficznych, chociaż tutaj też nastąpiły też pewne niespójności z wcześniej prezentowanymi badaniami.

W zakresie wybranych przez Autora kierunków badań przyjęta metodyka jest w pełni zgodna z ogólnymi zasadami prowadzenia badań naukowych. Doktorant najpierw dosyć szczegółowo przeanalizował istniejące rozwiązania i kierunki badawcze, skupiając się na problemach związanych z tematyką pracy. Następnie przeprowadził badania i opracował własne rozwiązania. Na zakończenie wykonał analizę i ocenę opracowanych rozwiązań poprzez wykonanie eksperymentów badawczych i porównanie uzyskanych wyników z wynikami uzyskanymi dla rozwiązań znanych z literatury.

5. Oryginalność uzyskanych wyników

Ze względu na, w znacznym stopniu, projektowy charakter pracy, głównym efektem pracy jest projekt i implementacja, w formie pSoC, systemu kryptograficznego. Opracowane rozwiązanie bazuje na istniejącym systemie CryptOne ale poprzez wprowadzenie istotnych,

innowacyjnych modyfikacji, zwiększających efektywność i bezpieczeństwo systemu, opracowano oryginalne rozwiązanie. Do najważniejszych oryginalnych osiągnięć Autora należą:

1. Zwiększenie efektywności systemu kryptograficznego na poziomie sprzętowym: w tym zakresie opracowano nowa architekturę układu mnożącego o podstawie 4, zwiększona zakres wspieranych konfiguracji koprocesora zwiększających wydajność dla algorytmów RSA 2048 i 4096 bitów, rozszerzono zakres instrukcji koprocesora, opracowano sprzętowy akcelerator (HMAC)-SHA2, zintegrowano opracowane moduły sprzętowe z koprocesorem.
2. Zwiększenie wydajności systemu kryptograficznego na poziomie programowym poprzez optymalizację implementacji algorytmów kryptograficznych i dostosowanie ich do zmodyfikowanej architektury systemu.
3. Podniesienie bezpieczeństwa systemu kryptograficznego na poziomie programowym poprzez opracowanie i implementację mechanizmów zabezpieczających przed atakami kanałem pobocznym
4. Podniesienie bezpieczeństwa systemu kryptograficznego na poziomie aplikacyjnym poprzez opracowanie koncepcji protokołu z kluczami jednorazowymi.

Szczegółowe uwagi dotyczące uzyskanych wyników są przedstawione w niejawnej części recenzji.

W odniesieniu do aktualnego stanu wiedzy wyniki badań uzyskane przez Autora są innowacyjne. Wyżej wymienione osiągnięcia zostały wdrożone w formie fizycznego systemu kryptograficznego.

6. Uwagi krytyczne, wady i słabe strony rozprawy

Oprócz wcześniej przedstawionych uwag dotyczących sformułowania tezy pracy, bibliografii i metodyki badań, wydaje się, że niektóre zagadnienia powinny być dokładniej przedyskutowane, wymagają wyjaśnienia lub uzupełnienia. Dotyczy to następujących problemów:

1. W tezie rozprawy wskazano, że poprawę bezpieczeństwa i efektywności można uzyskać poprzez „odpowiednio prowadzony proces projektowy". Można by zatem oczekiwać, że efektem pracy będzie propozycja metodyki projektowania, która pozwalałaby na zwiększenie ww. cech systemu kryptograficznego. W pracy Doktorant przedstawił jedynie wyniki końcowe w postaci opisu projektów poszczególnych elementów systemu. Zatem pojawia się pytanie co Autor uznaje za „odpowiednio prowadzony proces projektowy", który doprowadził do uzyskania systemu o lepszych parametrach jakościowych?
2. W pracy Doktorant skupił się na 4 zagadnieniach: generatorze liczb losowych, układzie mnożenia modulo, protokole z kluczami jednorazowymi oraz atakami kanałem bocznym. Powstaje pytanie skąd wynika taki zestaw badanych elementów systemu? Czy inne elementy/cechy systemu już nie da się zmodyfikować aby ulepszyć bezpieczeństwo czy wydajność systemu? Może warto by było wykonać analizę

architektury/własności systemu pod kątem wydajności i bezpieczeństwa aby zidentyfikować te elementy, które szczególnie warto ulepszyć?

3. W podsumowaniu Doktorant wymienia pewne modyfikacje koprocesora, które wcześniej nie zostały opisane. Niektóre z nich np. rozszerzenie zakresu instrukcji koprocesora, implementacja sprzętowa SHA2 itp. mogą mieć znaczny wpływ na własności rozwiązania końcowego (np. na efektywność). Zatem powstaje pytanie czy te modyfikacje są elementem procesu projektowego określonego w tezie pracy? a jeśli tak to dlaczego ich nie opisano i w jakim stopniu wpłynęły na poprawę efektywności systemu kryptograficznego?

Pozostałe uwagi dotyczą utajnionej części rozprawy i zostały umieszczone w niejawnej części recenzji.

Ponadto rozprawa zawiera wiele drobnych błędów językowych i nieścisłości merytorycznych. Szczegółowe uwagi:

1. Str. 5 – „jednorazowy" => „jednorazowych",
2. Str. 16 – odwołanie do wzoru (3.2) zamiast do (3.1).
3. Str. 34 – linie 6,7 oraz 8,9 są identyczne w Alg. 4.1.
4. Str. 37 – dla Tw. 1 nie podano dowodu. Czy jest to twierdzenie Autora?
5. Str. 55 – „Dla obliczeń wykonywanych przez człowieka" – to jest użyte w znaczeniu obliczeń wykonywanych w systemie dziesiętnym, ale człowiek może też liczyć w innych systemach, zatem nie jest to precyzyjne.
6. Str. 58 – „reguła" => „regułą",
7. Str. 59 - w algorytmie 5.10 „do" powinno być wyróżnione czcionką bold,
8. Str.59 – w algorytmie 5.11 brakuje określenia k jako parametru wejściowego,
9. Str. 60 – „prze 3" => "przez 3",
10. Str. 61 – błąd w równaniu (5.6),
11. Str. 63 – Rys.5.3 występuje 2 razy C2 a brakuje C1,
12. Str. 79 – „operacji operacji" => „operacji", „milinów" => „milionów",
13. Str. 83 – „obniżeniu wydajność" => "obniżeniu wydajności",
14. Str. 84 – „wraz zestawem" => „wraz z zestawem",
15. Str. 85 – „ze względu potencjalnie" => „ze względu na potencjalnie",
16. Str.86 – co istotnego do rozprawy naukowej wnoszą zdjęcia aparatury pomiarowej? Wydaje się, że bardziej istotne byłyby schemat stanowiska pomiarowego czy parametry techniczne tej aparatury.
17. Str. 87 – Nie jest określone co przedstawiają rysunki 6.5, 6.6 i dalsze. Po pierwsze, z opisu osi Y wynikałoby, że oś ta przedstawia przebieg prądu a nie zmiany mocy. Po drugie, opis skali (którego brakuje), pomimo że nie jest istotny dla zrozumienia opisywanych zagadnień to jednak dawałby wyobrażenie o skali zjawiska, co już jest istotne np. z punktu widzenia techniki pomiarowej.

Wyżej wymienione uwagi nie podważają wartości uzyskanych wyników badań i poprawności opracowanych rozwiązań. Ale omówienie tych zagadnień pozwoliłoby na lepszą

ocenę uzyskanych wyników badań, lepsze zrozumienie zastosowanej metodyki badań i podkreśliłoby innowacyjność uzyskanych wyników

7. Znaczenie uzyskanych wyników

Głównym wynikiem pracy jest opracowanie nowej wersji systemu kryptograficznego, będącej znaczną modyfikacją wcześniej opracowanego systemu CryptOne. Modyfikacja miała na celu zarówno zwiększenie wydajności przy jak najmniejszym wzroście kosztu implementacji jak i zwiększenie poziomu bezpieczeństwa. Coraz bardziej wyrafinowane metody łamania zabezpieczeń wymagają opracowywania skuteczniejszych zabezpieczeń a jednocześnie należy pamiętać o wzrastających wymaganiach dotyczących parametrów jakościowych stosowanych rozwiązań.

Biorąc pod uwagę szybki wzrost zagrożeń związanych z cyberprzestępczością konieczny jest rozwój coraz bardziej skutecznych i wydajnych mechanizmów ochrony. Jednym z istotnych elementów takich zabezpieczeń są systemy kryptograficzne. W tym kontekście uzyskane wyniki mają ogromne znaczenie praktyczne, szczególnie że opracowane rozwiązane jest gotowe do wdrożenia w rzeczywistych systemach.

8. Ocena końcowa rozprawy

Podsumowując, uważam że rozprawa doktorska mgra inż. Szymona Sarny przedstawia oryginalne rozwiązanie zaprezentowanego w niej zagadnienia naukowego i konstrukcyjnego. Autor podjął w niej problem, który ma istotne znaczenie w dziedzinie nauk inżynieryjno-technicznych w zakresie dyscypliny naukowej Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne. Trafnie określił założenia dotyczące jego analizy i uzyskane wyniki potwierdził wykonanymi eksperymentami. Wykazał się dobrą znajomością ogólnej wiedzy teoretycznej i praktycznej z zakresu tematyki pracy, a także umiejętnością samodzielnego prowadzenia pracy naukowej. Stwierdzam, że recenzowana praca spełnia wymogi stawiane rozprawom doktorskim w Ustawie z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U. poz. 1668, art. 187) i niniejszym wnoszę o dopuszczenie jej do publicznej obrony.