Warszawa, 3 października 2022 r.

dr hab. inż. Grzegorz Borowik, prof. Uniwersytetu SWPS
Katedra Informatyki
Wydział Projektowania
SWPS Uniwersytet Humanistycznospołeczny

Recenzja rozprawy doktorskiej pt. Metody zautomatyzowanego poszukiwania charakterystyk różnicowych w odniesieniu do kryptoanalizy szyfrów blokowych

Autor rozprawy:
mgr inż. Władysław Józef Dudzic

Promotor:
dr hab. inż. Andrzej Paszkiewicz, prof. WAT

Promotor pomocniczy:
dr inż. Krzysztof Kanciak

Niniejsza recenzja została sporządzona na prośbę Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej w przedłożonym przez dra hab. inż. Zbigniewa Tarapatę, prof. WAT piśmie (uchwała 18/RDN ITiT/2022) i dotyczy rozprawy doktorskiej w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja.

Dokonując oceny rozprawy doktorskiej mgra inż. Władysława Józefa Dudzica uwzględniłem obligatoryjne wymogi formalno-prawne stawiane dysertacjom, determinowane przepisami ustawy z dnia 14 marca 2003 roku o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki – Dz.U. 2003 Nr 65 poz. 595 z późn. zm. W recenzji dokonałem oceny doboru problematyki badawczej i tematu pracy, postawionego celu badawczego, hipotez pracy oraz wykorzystanych metod badawczych, struktury i treści pracy. Wykonałem ocenę merytoryczną i formalną pracy na bazie swojej wiedzy i dostępnych publikacji. Postawiłem konkluzję końcową.

Motywacją do podjęcia prac przez Autora rozprawy była automatyczna ocena bezpieczeństwa algorytmu kryptograficznego z wykorzystaniem kryptoanalizy różnicowej. Celem pracy było opracowanie wydajnej, automatycznej i generycznej metody poszukiwania optymalnych charakterystyk różnicowych – pod kątem maksymalnej wartości prawdopodobieństwa lub minimalnej liczby aktywnych skrzynek podstawieniowych – i charakterystyk różnicowych obciętych na zadaną liczbę rund szyfru blokowego. Autor pracy nie sformułował tezy rozprawy. W pracy podano tylko cel i zakres. Uważam, że dla oceny rozprawy doktorskiej kluczowe znaczenie ma jej teza, ponieważ prowadzone przez doktoranta prace mające na celu przygotowanie rozprawy doktorskiej powinny zmierzać w kierunku udowodnienia postawionej tezy. Za pomocą tezy, autor dysertacji, identyfikuje również nowy lub istniejący problem naukowy oraz proponuje jego nowatorskie rozwiązanie.

Przedstawione w recenzowanej rozprawie wyniki, przez ich potencjalne zastosowanie w praktyce, są ściśle związane z bezpieczeństwem informacji. Wyniki znajdują ważne zastosowanie w poszukiwaniu charakterystyk różnicowych. Uwzględniając powyższe wyrażam przekonanie, że wybór tematu rozprawy doktorskiej mgr. inż. Władysława J. Dudzica uznać należy za ważny technicznie i aktualny, a stopień trudności i zakres podjętego zadania, jego znaczenie naukowe oraz przydatność praktyczna odpowiadają ustawowym i zwyczajowo przyjętym kryteriom jakie zwykło się wiązać z rozprawą doktorską.

Tematyka rozprawy doktorskiej mieści się w nurcie badań z zakresu bezpieczeństwa i kryptoanalizy. Charakter rozprawy można uznać za syntetyczno-eksperymentalny, wyraźnie ukierunkowany w stronę praktycznego zastosowania.

Wykaz literatury obejmuje 66 pozycji (są to pozycje z okresu 1949–2021, z czego większość to publikacje z ostatniego dziesięciolecia, ale zamieszczenie pozycji starszych jest jak najbardziej uzasadnione), w tym jedna pozycja autorska oraz 2 pozycje współautorskie mgr. inż. Władysława J. Dudzica. Wnioski z przeglądu stanu wiedzy oraz aktualnych badań w uznanych ośrodkach naukowych przedstawiono w sposób jasny i przekonujący. Autor w sposób właściwy odniósł się do dotychczasowego dorobku literaturowego i oceny stanu wiedzy w zakresie istotnych problemów zgodnych z tematyką pracy.

W trakcie prowadzonych badań Autor:

- opracował automatyczną metodę wyznaczania charakterystyk różnicowych opartą na grafach AIG, aktywującą minimalną liczbę skrzynek podstawieniowych w szyfrach blokowych;
- potwierdził wydajność opracowanej metody z użyciem testów przeprowadzonych na popularnych szyfrach blokowych;
- opracował automatyczną metodę poszukiwania obciętych charakterystyk różnicowych opartą na grafach AIG;
- zaimplementował narzędzia do poszukiwania charakterystyk różnicowych;
- w ramach przeprowadzonych obliczeń wyznaczył nieznane, optymalne charakterystyki różnicowe oraz charakterystyki różnicowe obcięte dla zredukowanych w liczbie rund wybranych szyfrów blokowych;
- przeprowadził badania i doświadczenia, potwierdzające użyteczność SMT i SAT-solverów w procesach związanych z kryptoanalizą i oceną bezpieczeństwa algorytmów kryptograficznych;
- stworzył efektywne narzędzie wspomagające projektowanie nowych szyfrów pod kątem ich odporności na ataki różnicowe.

Wymienione elementy rozprawy stanowią samodzielny i oryginalny dorobek Autora.

Rozprawa stanowi spójną tematycznie całość. Następstwo rozdziałów i podrozdziałów oraz ich zawartość należy uznać za właściwe. Omawiane zagadnienia zostały uzupełnione przez wybrane skrypty w języku Cryptol. Zawartość poszczególnych rozdziałów i rozwój zawartych w nich myśli świadczy o dojrzałości naukowej Doktoranta, dobrym przygotowaniu do samodzielnego prowadzenia badań naukowych, jak również świadczy o popartych wyczuciem dużych umiejętnościach inżynierskich.

W zasadzie nie dostrzegam istotnych wad rozprawy, a gdyby chcieć wymienić „drobne", to wskazałbym na:

- na str. 31 pracy Autor koncentruje uwagę na minimalizacji funkcji boolowskiej. Używa stwierdzenia „minimalny nakład obliczeniowy" przez co rozumie małą liczbę bramek logicznych. Należy zauważyć, że minimalizacja funkcji boolowskich może nie tylko pozytywnie wpłynąć na redukcję liczby elementów logicznych, ale również na czas propagacji przez układ – o czym Autor już nie napisał. Należy również zaznaczyć, że wiele układów kryptograficznych było i jest implementowanych w układach cyfrowych innych niż układy bramkowe, np. w układach FPGA. Te nie zostały rozważone przez Autora pracy.

- na str. 46 Autor stwierdza: „Obecnie nie jest znany algorytm, który skutecznie rozwiązałby każdy problem SAT i uważa się, że taki algorytm nie istnieje." Nie można się zgodzić z drugą częścią tej tezy.

- na str. 87 Autor napisał, że liczba klauzul rośnie liniowo dla każdego z badanych algorytmów wraz z liczbą rund, co podsumował rysunkiem 6.5 na str. 88. Rysunek przedstawia zaś zależność liczby rund do logarytmu naturalnego z liczby klauzul, co nie jest zależnością liniową. Autor nie pokazał również na jakiej podstawie wnioskuje o liniowości tej zależności. Ilustracja nie jest w żadnym stopniu dowodem tej zależności, a skala logarytmiczna wpływa niekorzystnie na „rozdzielczość" wartości prezentowanych na osi rzędnych.

- w pracy występuje wiele powtarzających się zagadnień (również w prezentowanym przez Autora tekście). Wynika to, co prawda, ze specyfiki zaproponowanego/zaproponowanych rozwiązań, jednak dla poprawy czytelności Autor mógł rozważyć usunięcie bądź przeredagowanie tych części pracy.

- można odnieść wrażenie, że słowo „optymalny" jest przez Autora pracy nadużywane. Słowo optymalny oznacza, że osiągnęliśmy optimum, czyli najkorzystniejsze rozwiązanie lub najlepsze możliwe warunki w danej sytuacji. Jeżeli coś jest optymalne, to znaczy, że jest najlepsze, najkorzystniejsze, najdogodniejsze w tych właśnie warunkach i już lepsze być nie może. Przez *nadużywanie* mam tutaj na myśli sytuacje, w których Autor pracy korzysta z metod probabilistycznych, które z założenia dają rozwiązanie przybliżone do rozwiązania optymalnego, a które jest zwykle możliwe do osiągnięcia z wykorzystaniem metody systematycznej. Dlatego sugerowałbym rozważenie zamiany słowa „optymalny" na „skuteczny" lub „wydajny".

Praca zawiera kilka błędów stylistycznych i redakcyjnych, które nie wpływają na jakość i wartość merytoryczną rozprawy:

- str. 10, „może nie być **bezwarunkowe** bezpieczny"
- str. 30, „Najczęściej wykorzystywana jest szeroko rozumiana **minimalizacji** funkcji boolowskiej, …"
- str. 38, „W ataku **różnicowych** możemy wykorzystać…"
- str. 39, pojęcia – charakterystyki różnicowe obcięte oraz niemożliwe – pojęcia są używane wcześniej, a dopiero na stronie 39 Autor przytacza ich anglojęzyczne odpowiedniki
- str. 55, „**na rysunku** nr 5.2." – powinno być „w tablicy…"

Autor dysertacji używa potocyzmów i ma tendencję do antropomorfizowania:

- str. 12, „Obecnie wszystkie ogólnodostępne narzędzia oparte są na metodach, w których równania opisujące propagację charakterystyki różnicowej są predefiniowane dla każdego algorytmu przy wykorzystaniu **trików** zaproponowanych przez ich autorów."
- str. 46, „… wykorzystuje się algorytm CDCL, który **inspiruje się** algorytmem…"
- str. 68, „… algorytmy … **radziły sobie**…"
- str. 75, „… oraz **innym zabiegom** pozwalającym maksymalnie zredukować jego rozmiar."

Przeprowadzone przez Doktoranta prace mają charakter badań na przecięciu dziedzin: matematyki, telekomunikacji i informatyki. Wyniki badań znajdują duże zastosowanie w implementacjach przemysłowych związanych z bezpieczeństwem informacji i kryptografii. Jak wykazał Autor rozprawy, badania dotyczące opracowywania efektywnych metod poszukiwania charakterystyk różnicowych są prowadzone w wielu zespołach naukowo-badawczych na świecie, w szczególności w ostatnim dwudziestoleciu. Pozwala to tym bardziej wysoko ocenić rezultaty uzyskane przez Doktoranta, który w wyniku realizacji rozprawy doktorskiej zaproponował oryginalne, efektywne i automatyczne metody poszukiwania charakterystyk różnicowych oraz stworzył użyteczne narzędzia komputerowego wspomagania tego zadania. Mając na uwadze, że otrzymane przez Doktoranta wyniki w sposób znaczący mogą przyczynić się do poprawy wielu algorytmów ochrony informacji oraz istotnie poprawiają rezultaty osiągnięte i opublikowane w literaturze światowej, zachęcam Autora rozprawy do publikacji tych wyników w czasopismach o szerokim zasięgu.

Rozprawę mgr. inż. Władysława Dudzica oceniam jako spełniającą wymogi stawiane dysertacjom. Autor rozprawy wykazał się dogłębną wiedzą z zakresu zagadnień, które uczynił przedmiotem dociekań naukowych. Rozwiązał nietrywialne, aktualne i ważne technicznie problemy naukowe, użyteczne praktycznie i wszystko dobrze udokumentował. Wykazał się przy tym inicjatywą twórczą, umiejętnościami rozwiązywania złożonych problemów, bardzo dobrym opanowaniem warsztatu badawczego i przygotowaniem do samodzielnego prowadzenia badań naukowych. Uważam, że przedstawiona do recenzji praca mgr. inż. Władysława J. Dudzica pt.: „Metody zautomatyzowanego poszukiwania charakterystyk różnicowych w odniesieniu do kryptoanalizy szyfrów blokowych" spełnia wymagania postanowień aktualnie obowiązującej „Ustawy o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki". Dlatego wnoszę o przyjęcie recenzowanej pracy jako rozprawy doktorskiej i dopuszczenie jej Autora do dalszych etapów przewodu doktorskiego.