Prof. dr hab. inż. Zbigniew Kotulski,
Instytut Telekomunikacji Politechniki Warszawskiej

Warszawa, 31 maja 2022 r.

RECENZJA ROZPRAWY DOKTORSKIEJ
DLA RADY DYSCYPLINY NAUKOWEJ
INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA
WOJSKOWEJ AKADEMII TECHNICZNEJ W WARSZAWIE

Tytuł rozprawy: Metody zautomatyzowanego poszukiwania charakterystyk różnicowych w odniesieniu do kryptoanalizy szyfrów blokowych

Autor rozprawy: Władysław Józef Dudzic, Wydział Cybernetyki Wojskowej Akademii Technicznej w Warszawie

Niniejsza recenzja została opracowana na odpowiedzi na pismo Przewodniczącego Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja WAT, profesora WAT dr. hab. inż. Zbigniewa Tarapaty, realizującego uchwałę Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja WAT nr 18/RDN ITiT/2022 z dnia 12 kwietnia 2022 r. w sprawie wyznaczenia recenzentów rozprawy doktorskiej mgr. inż. Władysława Józefa Dudzica.

Wstęp

Praca jest napisana w języku polskim i liczy 106 stron. Treść pracy podzielona jest na siedem rozdziałów i bibliografię. Rozdział 1 (str. 9-13) zawiera wiadomości wstępne dotyczące tematyki rozprawy, sformułowanie celu i zakresu rozprawy oraz omówienie stanu badań w zakresie tematyki rozprawy na podstawie literatury. W rozdziale 2 (strony 15-35) przedstawiono podstawowe definicje dotyczące szyfrów blokowych, schematy budowy szyfrów i wybrane własności szyfrów, w tym charakterystyki różnicowe. Rozdział 3 (str. 37-44) zawiera opis trzech najważniejszych metod kryptoanalizy: różnicową, liniową i ataki algebraiczne, a także ataki na algorytmu o ograniczonej liczbie rund. W rozdziale 4 (str. 45-49) przedstawiono, na podstawie literatury, trzy metody optymalizacji z więzami, które zostały wykorzystane w dalszych częściach rozprawy. Kolejne dwa rozdziały zawierają oryginalne wyniki obliczeniowe i teoretyczne uzyskane przez Doktoranta. Rozdział 5 (str. 51-63) przedstawia komputerowe metody ustalania dwóch wielkości charakteryzujących szyfry blokowe: parametr Differential Branch Number charakteryzujący minimalną liczbę aktywnych elementów na wejściu i wyjściu operacji używanych w szyfrach oraz minimalną liczbę aktywnych skrzynek

podstawieniowych w procesie szyfrowania. Rozdział 6 (str. 65-95) zawiera główne oryginalne wyniki badań, czyli opracowane przez Doktoranta metody zautomatyzowanego poszukiwania różniczek i charakterystyk różnicowych wraz z przykładami obliczeniowymi. Rozdział 7 (str. 97-100) to podsumowanie rozprawy ze wskazaniem uzyskanych wyników oryginalnych oraz nakreśleniem perspektyw kontynuacji badań.

Bibliografia liczy 66 pozycji, w tym 1 pracę autorstwa i 2 współautorstwa pana mgr. inż. Władysława Dudzica. W pracy brak jest spisów rysunków, tablic i algorytmów. Po podliczeniu stwierdzam, że zawiera ona 30 rysunków, 29 tabel i 6 kodów źródłowych algorytmów napisanych w języku Python.

Dalszą część recenzji przygotowałem według punktów wzorowanych na zestawie pytań zalecanych w recenzjach wykonywanych dla WEiTI PW.

Omówienie rozprawy

Jakie zagadnienie naukowe jest rozpatrzone w pracy (teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?

Cel rozprawy został jasno i precyzyjnie sformułowany, chociaż nie jest to sformułowanie w formie tradycyjnie rozumianej tezy doktorskiej. Celem jest opracowanie wydajnej, automatycznej i generycznej metody poszukiwania optymalnych charakterystyk różnicowych, a także charakterystyk różnicowych obciętych do zadanej liczby rund szyfru blokowego. Charakterystyki te powinny być zoptymalizowane ze względu na maksymalizację wartości prawdopodobieństwa lub minimalizację liczby aktywnych skrzynek podstawieniowych.

Celem rozprawy jest opracowanie algorytmu obliczeniowego i potwierdzenie jego walorów za pomocą eksperymentów obliczeniowych, zatem charakter pracy jest w dominującej mierze eksperymentalny, z elementami modelowania matematycznego.

Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł / w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle /świadczący o dostatecznej wiedzy autora. Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?

Studia literaturowe przeprowadzone w rozprawie doktorskiej zostały potraktowane bardzo wąsko. Poza kilku podstawowymi publikacjami z zakresu kryptografii i kryptoanalizy, w rozprawie zacytowano i omówiono jedynie te publikacje, które są ściśle związane z jej tematem, wykorzystywanymi metodami matematycznymi i rozwijanymi algorytmami. W tym węższym zakresie literatura jest

właściwie dobrana i odpowiednio zacytowana. Wnioski z literatury są odpowiednio sformułowane i właściwie udokumentowane.

Odrębną sprawą jest sposób przedstawienia publikacji w spisie literatury. Autor prawdopodobnie wykorzystywał do sporządzenia bibliografii system bibtex i nie sprawdził wyniku wygenerowanej bibliografii, stąd liczne usterki w wydrukowanym wykazie. Np. w pozycji [1] brak jest tytułu czasopisma, w poz. [2] brak numeru tomu, zeszytu i numerów stron, w poz. [3] Auguste Kerckhoffs występuje jako K. Auguste, co sprawia, że autor znalazł się w niewłaściwym miejscu listy w kolejności alfabetycznej, itd. Ogólnie brak jest także podania numerów DOI publikacji, co obecnie jest standardem w publikacjach naukowych.

Czy autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?

Podjęty problem badawczy jest aktualny i niezwykle ważny ze względu na trwające intensywne prace nad nowymi szyframi blokowymi (konkurs na lekką kryptografię) oraz potrzeby wynikające z rozwoju technologii wykorzystywanych w kryptoanalizie. Autor rozprawy swoje badania oparł na analogicznych rezultatach znanych z literatury, rozwinął je, ulepszył oraz wprowadził element automatyzacji konstrukcji wraz z odpowiednim oprogramowaniem realizującym praktycznie opracowaną metodę. Porównanie wyników ilościowych z wynikami uzyskanymi za pomocą oprogramowania publicznie dostępnego potwierdza słuszność zrealizowanego rozwiązania.

Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?

Autor rozprawy doktorskiej przeprowadził oryginalne badania teoretyczne i obliczeniowe, poprzedzone analizą stanu sztuki i wymagań związanych z planowaną aplikacją nowego rozwiązania. Za najważniejsze oryginalne osiągnięcia rozprawy uważam:

- propozycję wykorzystania grafów AIG do opisu szyfrów blokowych i opracowanie automatycznych metod wyznaczania charakterystyk różnicowych aktywujących minimalną liczbę skrzynek podstawieniowych w szyfrach blokowych (rozdz. 5.2.2), optymalnych charakterystyk różnicowych (rozdz. 6.3.1) oraz obciętych charakterystyk różnicowych (rozdz. 6.3.2);
- przygotowanie oprogramowania realizującego opracowane automatyczne metody wyszukiwania i optymalizacji, mogącego stanowić podstawę kontynuacji prac badawczych w zakresie kryptoanalizy różnicowej;
- przeprowadzenie obliczeń wykazujących skuteczność zaproponowanych metod

oraz znalezienie nieznanych dotychczas w publikacjach optymalnych charakterystyk różnicowych dla wybranych szyfrów blokowych o zredukowanej liczbie rund.

Niewątpliwą zaletą rozprawy jest fakt, że Autor przeprowadził pełen cykl badań charakterystyczny dla nauk technicznych: od pomysłu i analizy teoretycznej, poprzez modelowanie matematyczne i implementację rozwiązania do praktycznej realizacji systemu i eksperymentalnej weryfikacji, z udostępnieniem uzyskanych wyników eksperymentów w Internecie.

Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników /zwięzłość, jasność, poprawność redakcyjna rozprawy/?

Rozprawa jest w części merytorycznej dobrze zredagowana, napisana poprawnym językiem matematycznym i poprawną polszczyzną. Przedstawienie problemu rozwiązywanego w rozprawie jest precyzyjnie sformułowane, poprzedzone niezbędnym wprowadzeniem zawierającym definicje, fakty matematyczne i pokrewne wyniki uzyskane przez innych autorów. W kilku miejscach Autor niepotrzebnie zmienił orientację wykresów i tabel na stronie, co utrudnia czytanie rozprawy (rys. 5.3, 5.4, 6.7, 6.8, 6,9, 6.10, tabela 2.9). Poważne zastrzeżenia budzi brak staranności w zredagowaniu bibliografii, o czym już pisałem.

Kilka zauważonych usterek redakcyjnych dotyczących tekstu rozprawy przedstawiam poniżej.

Str. 23, jest: w **przypadku gdy** parametr Differential,
powinno być: w **przypadku, gdy** parametr Differential

Str. 26 jest: **niemożlwych**
powinno być: **niemożliwych**

Str. 37 i 38 jest: **zdeszyfrowania**
powinno być: **odszyfrowania**

Str. 44 jest: **nie koniecznie**
powinno być: **niekoniecznie**

Str. 47 jest: NP-**zupełnym dlatego**
powinno być: NP-**zupełnym, dlatego**

Str. 47 jest: w **przypadku gdy** stosunek
powinno być: w **przypadku, gdy** stosunek

Str. 52, 84 jest: **podstawioniowych**
powinno być: **podstawieniowych**

Str. 53 jest: etapie w **przypadku gdy**
powinno być: etapie w **przypadku, gdy**

Str. 53 AES za **pomoca** zadania MILP
powinno być: AES za **pomocą** zadania MILP

Str. 56 jest: jest **różnież** duża wydajność.

powinno być: jest **również** duża wydajność.

Str. 56 jest: w **rodziale** 5.2.1

powinno być: w **rozdziale** 5.2.1

Str. 56 jest: różnicowej, **ktora** aktywuje

powinno być: różnicowej, **która** aktywuje

Str. 57, 72, 74, 76 jest: Skrypt języka Cryptol **opisujacy** propagację

powinno być: Skrypt języka Cryptol **opisujący** propagację

Str. 61 jest: czasochłonnym w **przypadku gdy** algorytm blokowy

powinno być: czasochłonnym w **przypadku, gdy** algorytm blokowy

Str. 87 jest: Warto jednak **podkreslić**, że rozmiar

powinno być: Warto jednak **podkreślić**, że rozmiar

Str. 89 jest: Udało się **rownież** potwierdzić

powinno być: Udało się **również** potwierdzić

Str. 95 jest: Widać **wyrażnie**, że szyfry blokowe

powinno być: Widać **wyraźnie**, że szyfry blokowe

Str. 95 jest: wymaga **intensywanego** wysiłku

powinno być: wymaga **intensywnego** wysiłku

Str. 98 jest: trendy konstrukcyjne **odwracją** się właśnie

powinno być: trendy konstrukcyjne **odwracają** się właśnie

Str. 99 jest: przy jednoczesnym zachowaniu jego **funkcjonalości**.

powinno być: przy jednoczesnym zachowaniu jego **funkcjonalności**.

Str. 99 jest: tzw. relacjach **boolowskiech**

powinno być: tzw. relacjach **boolowskich**

Jakie są słabe strony rozprawy i jej główne wady?

Praca jest ogólnie dobrze napisana, uzyskane wyniki są wartościowe a wykonane prace badawcze nie zawierają błędów merytorycznych. Jeśli chodzi o oczekiwania dotyczące rozprawy to przydałaby się szerzej opracowana część monograficzna dotycząca szyfrów blokowych. Na przykład, w charakteryzacji własności szyfrów pominięto algorytmy generowania kluczy rundowych, które mają istotny wpływ na bezpieczeństwo szyfrowania. Przydałby się też szerszy opis metod kryptoanalizy, chociażby uwzględnienie kryptoanalizy liniowo-różnicowej. Niedosyt budzi też stosunkowo niewielka liczba przebadanych szyfrów, czyli 8: AES, KLEIN, MIDORI, PRESENT, SPECK, SIMON, PYJAMASK oraz SATURNIN. Program, do którego wyników porównywane są rezultaty uzyskane w niniejszej rozprawie, czyli CryptoSMT, analizuje 16 szyfrów blokowych: Simon, Speck, Skinny, Present, Midori, LBlock, Sparx, Twine, Noekeon, Prince, Mantis, Speckey, Rectangle, Cham, CRAFT, TRIFLE, Nasuwa się pytanie: na ile prosta jest automatyzacja metody uzyskanej w rozprawie i czy przebadanie dodatkowych szyfrów byłoby dużym problemem. I czy możliwe jest znajdowanie różnic dla innych klas algorytmów, tak jak w programie CryptoSMT, czyli funkcji skrótu, szyfrów strumieniowych, algorytmów

uwierzytelnionego szyfrowania i MAC. Uwagi te mają charakter dyskusyjny i w żadnym stopniu nie podważają nowych i oryginalnych wyników badawczych uzyskanych w recenzowanej rozprawie.

Jaka jest przydatność rozprawy dla nauk technicznych?

W rozprawie doktorskiej zaimplementowano narzędzia do poszukiwania charakterystyk różnicowych (optymalnych pod kątem wartości prawdopodobieństwa oraz minimalnej liczby aktywnych skrzynek podstawieniowych) i charakterystyk różnicowych obciętych. Tego typu oprogramowanie, po odpowiednim dostosowaniu do użytku przez osoby nie będące jego autorami (instrukcje obsługi, przyjazne interface, itd.) mogłoby się stać ważnym narzędziem wspomagającym opracowywanie nowych algorytmów kryptograficznych. Również wyniki już uzyskane przez Doktoranta przy wykorzystaniu tego oprogramowania, udostępnione w publicznym repozytorium (https://gitlab.com/Witek1809/Ariadna-Results) stanowią ważny wkład do rozwoju szyfrów blokowych jako dane referencyjne dla innych badaczy. Jak widać, przydatność uzyskanych w rozprawie wyników dla rozwoju kryptografii nie budzi wątpliwości.

Podsumowanie i ocena rozprawy

W swojej rozprawie doktorskiej pan magister inżynier Władysław Dudzic jasno sformułował i poprawnie zrealizował zagadnienie badawcze z zakresu kryptoanalizy szyfrów blokowych, wykorzystując do tego celu nowoczesne metody matematyczne i obliczeniowe. Uzyskany przez niego rezultat jest nowy i oryginalny, przydatny zarówno w badaniach bezpieczeństwa znanych szyfrów blokowych, jak też projektowania nowych algorytmów. Rozprawę doktorską pana magistra inżyniera Władysława Dudzica oceniam pozytywnie. Uważam, że spełnia ona wymagania stawiane przez *USTAWĘ z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki*, Dz.U. z 2003 r. Nr 65, poz. 595 z późniejszymi zmianami, rozprawom doktorskim w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie naukowej: informatyka techniczna i telekomunikacja i wnioskuję o jej dopuszczenie do publicznej obrony.

Kotulski

Prof. dr hab. inż. Zbigniew Kotulski