Warszawa, 14.11.2022

dr hab. inż. Arkadiusz Orłowski, prof. SGGW

Katedra Sztucznej Inteligencji
Instytut Informatyki Technicznej
Szkoła Główna Gospodarstwa Wiejskiego
ul. Nowoursynowska 159
02-787 Warszawa

RECENZJA ROZPRAWY DOKTORSKIEJ

Tytuł rozprawy:	**Metody zautomatyzowanego poszukiwania charakterystyk różnicowych w odniesieniu do kryptoanalizy szyfrów blokowych**
Autor rozprawy:	mgr inż. Władysław Dudzic
Promotor:	dr hab. inż. Andrzej Paszkiewicz
Promotor pomocniczy:	dr inż. Krzysztof Kanciak

Recenzowana rozprawa liczy 106 stron. Składa się na nią siedem rozdziałów merytorycznych (w tym czterostronicowe Podsumowanie) oraz liczący 102 pozycje spis literatury przedmiotu. Dodatkowo, na początku rozprawy umieszczono Spis treści, Listę skrótów, Streszczenie i anglojęzyczny Abstract.

Cztery pierwsze rozdziały recenzowanej rozprawy stanowią pożyteczne wprowadzenie do dalszej części pracy. Mają one w związku z tym głównie charakter kompilacyjny i przeglądowy, aczkolwiek zawierają też autorskie obserwacje i komentarze.

Rozdział pierwszy zawiera krótkie wprowadzenie do problematyki szyfrów blokowych, w tym do metod ich konstrukcji i analizy bezpieczeństwa. Następnie sformułowano cel pracy, którym jest **„opracowanie wydajnej, automatycznej i generycznej (mającej zastosowanie przy każdej konstrukcji analizowanego algorytmu) metody poszukiwania optymalnych charakterystyk różnicowych (pod kątem maksymalnej wartości prawdopodobieństwa lub minimalnej liczby aktywnych skrzynek podstawieniowych) i charakterystyk różnicowych obciętych (o prawdopodobieństwie większym niż szum) na zadaną liczbę rund szyfru blokowego”**. Przedstawiono też i omówionu jej zakres. Rozdział ten kończy się skrótowym i syntetycznym zarysem stanu badań w dziedzinie kryptoanalizy szyfrów blokowych i przeglądem literatury przedmiotu, co stanowi dobry punkt wyjścia do dalszej części pracy. Poza celem głównym w rozprawie nie sformułowano w sposób jawny hipotez badawczych (ani celów szczegółowych), ale można przyjąć, że chodzi właśnie o możliwość stworzenia nowych i udoskonalenia istniejących metod pozwalających na automatyczne wykrywanie optymalnych charakterystyk różnicowych („zwykłych” i obciętych) z wystarczającą efektywnością. Wydaje się, że w rozdziale tym autor lekko nadużył metody *cut-and-paste*. Na przykład (ważny skądinąd) fragment „pod kątem maksymalnej wartości prawdopodobieństwa lub minimalnej liczby aktywnych skrzynek podstawieniowych” pojawia się w dokładnie takim samym brzmieniu trzykrotnie.

Rozdział drugi jest zwartym, ale interesującym i zasadniczo kompletnym (jak na 21 wykorzystanych stron) wprowadzeniem w problematykę szyfrów blokowych, istotnie ułatwiającym śledzenie w prowadzonych przez autora w dalszych częściach rozprawy badań i analiz. Po podaniu podstawowych definicji oraz najważniejszych metod konstrukcji (sieci SPN, sieci Feistela, struktura Lai-Massey’a) oraz bardzo krótkiego omówienia operacji ARX, strategii szerokiej ścieżki i dwuzdaniowego komentarza (tworzącego podrozdział 2.5) dotyczącego bezpieczeństwa, następuje bardzo ważny, choć wciąż pomocniczy podrozdział 2.6., liczący nieco ponad czternaście stron. Pojawiają się tu wszystkie istotne pojęcia wykorzystywane w dalszej części pracy, poczynając od losowości szyfrogramu, klasycznych Shannon’owskich koncepcji konfuzji i dyfuzji, definicji parametru DBN (*Differential Branch Number*), poprzez pojęcie profili różnicowych, aktywnych skrzynek podstawieniowych w

sieciach SPN aż po problematykę reprezentacji szyfru blokowego za pomocą układów równań nad ciałem binarnym. W ostatnim podrozdziale 2.6.7 podrozdziału 2.6 pięć stron poświecono koncepcji grafów AIG i opisowi ich do reprezentacji szyfrów blokowych. Nie powinno to jednak dziwić, gdyż jest to podstawowa struktura wykorzystywana w rozprawie. Trzeba przyznać, że autor bardzo szczegółowo i przekonywująco przedstawia zalety grafów AIG zarówno do reprezentacji samych szyfrów blokowych, jak też do reprezentacji struktury logicznej opisującej propagację charakterystyk różnicowych. Poza typowymi zaletami, autor zwraca uwagę na możliwość wykonania tzw. redukcji funkcjonalnej (minimalizacja grafu ze względu na liczbę wierzchołków) oraz istnienie wielu narzędzi ułatwiających automatyzację istotnych elementów opisu przekształceń kryptologicznych. Definicja grafu AIG podana w pierwszym paragrafie podrozdziału 2.6.7 jest praktycznie dosłownym tłumaczeniem definicji podanej w anglojęzycznej Wikipedii. Zachęcam autora do przygotowania pełnego hasła dla Wikipedii w języku polskim.

Rozdział trzeci również został opracowany na podstawie istniejącej literatury przedmiotu i zawiera krótkie wprowadzenie w podstawowe metody kryptoanalizy szyfrów blokowych. Po przypomnieniu standardowej terminologii dotyczącej podstawowych typów ataków kryptograficznych, omówiono najważniejsze cechy kryptoanalizy różnicowej (w tym uogólnienia „standardu” na kryptoanalizę wykorzystującą tzw. charakterystyki różnicowe obcięte i niemożliwe) oraz bardzo skrótowo opisano kryptoanalizę liniową i kryptoanalizę algebraiczą. Rozdział zamyka krótki opis specyfiki ataków typu 0R i nR.

Kolejnym niewielkim objętościowo, ale przydatnym rozdziałem pomocniczym, jest rozdział czwarty, w którym scharakteryzowano wykorzystywane później przez autora problemy typu CSP. Wyróżniono problemy SAT, SMT i MIP. W punkcie 4.1 wspomniano także o problemie ASP, ale nie został on później omówiony. Tzw. SAT *solvery* wykorzystuje się coraz częściej do kryptoanalizy szyfrów blokowych, strumieniowych i funkcji skrótu. Autor zwraca uwagę na słabe strony wielu algorytmów służących do rozwiązywania problemów SAT, omawia krótko hipotezę dotyczącą własności losowo generowanych problemów SAT, oraz wprowadza interesujące pojęcie gęstości problemu SAT. Do rozwiązywania problemów SMT, autor rekomenduje SMT *solver* Z3 firmy Microsoft. Omawiając krótko problemy MIP, autor zwraca uwagę na ich szczególny przypadek - MILP, gdzie wszystkie ograniczenia wyrażone są za pomocą funkcji liniowych. Jest on coraz częściej wykorzystywany w kontekście

kryptologicznym do wyznaczania minimalnej liczby aktywnych skrzynek podstawieniowych w szyfrach budowanych na bazie sieci SPN.

Rozdział piaty, dotyczący metod zautomatyzowanego wyznaczania wybranych własności szyfrów blokowych, zawiera krytyczny przegląd istniejących metod, wzbogacony wynikami badań własnych autora rozprawy. Rozdział zaczyna się od przypomnienia omawianego już wcześniej w podrozdziale 2.6.3 ważnego parametru DBN. Warto wspomnieć, że autor zaimplementował na potrzeby rozprawy narzędzie, które na bazie grafu AIG automatycznie wyznacza minimalną wartość tego parametru dla zadanego przekształcenia liniowego. Sam graf AIG również tworzony jest automatycznie na podstawie implementacji operacji kryptograficznych w języku funkcyjnym Cryptol. Następnie szczegółowo omawiany jest bardzo istotny w rozwijanym podejściu problem znajdowania minimalnej liczby aktywnych skrzynek podstawieniowych w sieciach SPN. Jest to ważny element procesu analizy odporności szyfru blokowego na atak różnicowy, który przydaje się także przy wyznaczaniu dobrych charakterystyk różnicowych. Przedstawiono dwa podejścia do rozwiązania tego typu problemów. Pierwsze, wykorzystujące problem MILP, zilustrowano na przykładzie AES. Drugie podejście jest podejściem autorskim, które bazuje na grafie AIG i modelu SAT. Podejście to zostało zilustrowane na przykładach pięciu ważnych szyfrów blokowych (AES, PRESENT, MIDORI, KLEIN i PYJAMASK). Autor słusznie zauważa, że pierwsze podejście dobrze sprawdza się w przypadku szyfrów przetwarzających bajty lub słowa heksadecymalne (ogólnie, w przypadku szyfrów zorientowanych na przetwarzanie słów o rozmiarach kilkubitowych). Ma ono jednak kilka wad. Z punktu widzenia autora najistotniejszy wydaje się fakt, że w tym podejściu wyznaczenie minimalnej liczby skrzynek nie oznacza automatycznie znajomości konkretnej charakterystyki różnicowej, która aktywuje tę właśnie liczbę skrzynek. Wady tej wydaje się nie mieć podejście opracowane przez autora rozprawy. Trzy zasadnicze etapy metody autorskiej to opisanie propagacji aktywności skrzynek za pomocą grafu AIG, konwersja grafu AIG do modelu SAT, i wreszcie wyznaczenie odpowiedniego wartościowania modelu SAT. Autor uważa, że „wydajność metody jest w pełni akceptowalna na potrzeby obliczeń”, chociaż zauważa, że „czas potrzebny na wyznaczanie poprawnego wartościowania modelu jest znacznie większy niż w przypadku metody wykorzystującej model MILP”. Oczywiście wartością dodaną jest uzyskanie w przypadku metody autorskiej konkretnej, przykładowej charakterystyki różnicowej, aktywującej wyznaczoną minimalną liczbę skrzynek podstawieniowych. Jako przykład opisu propagacji aktywnych skrzynek dla szyfru PRESENT podano skrypt w języku Cryptol. W formie tabelarycznej przedstawiono też zbiorcze wyniki

dla wszystkich pięciu wyżej wspomnianych szyfrów. Zaobserwowano, że wydajność metody jest najgorsza dla szyfru PYJAMASK. Potwierdza to wcześniejszą uwagę autora, że określenie minimalnej liczby skrzynek podstawieniowych jest najbardziej czasochłonne w przypadku szyfrów bardziej zorientowanych na przetwarzanie pojedynczych bitów niż słów wielobitowych.

Zasadniczą częścią recenzowanej rozprawy doktorskiej jest rozdział szósty. Jest on objętościowo największy i zawiera główne wyniki autora. Jako pierwsze omawiane jest podejście wykorzystujące zmodyfikowany algorytm podziału i ograniczeń. Autor wyraźnie zaznacza, że przyjmuje się tu ważne założenie, które mówi, że „jeżeli w zbiorze perspektywicznych różniczek znajdą się dwie różniczki o tej samej postaci, są one scalane do jednej (prawdopodobieństwa charakterystyk różnicowych są sumowane, ponieważ zakładamy, że zdarzenia te będą niezależne)". Nie jest dla mnie całkowicie jasne czy wyniki autora potwierdzają, a jeśli tak to w jakim stopniu, słuszność założenia o niezależności zdarzeń. Jeśli chodzi o wydajność tego podejścia, to jest ona niestety niezadawalająca. W szczególności podejście to jest niepraktyczne dla algorytmów z ośmiobitową skrzynką podstawieniową. Autor zauważa także inną potencjalna wadę, która kojarzy mi się z wadą niektórych algorytmów zachłannych, a mianowicie fakt, że „w związku z redukcją źle rokujących następników nie mamy również pewności czy w niektórych przypadkach algorytm nie odrzuci ścieżki, która w etapie końcowym dawałaby optymalne rozwiązanie". Co prawda autor twierdzi, że „w szyfrach opartych na sieci SPN prawdopodobieństwo takiego zdarzenia nie wydaje się jednak znaczące". Znowu nie jest jasne czy są to tylko przeczucia lub intuicje autora, czy też ma to jakieś uzasadnienie lub potwierdzenie statystyczne. Drugie analizowane podejście bazuje na modelu SMT. Autor zaimplementował tu wspomniany wcześniej SMT *solver* Z3. Po wstępnych testach, z algorytmów optymalizacyjnych dostępnych w Z3 wybrano algorytm SYMBA. Dla ułatwienia analizy przedstawiono kod źródłowy odpowiedniej konfiguracji *solvera* wykonanej z poziomu języka Python. Również w tym przypadku uzyskana wydajność nie pozwala na praktyczny atak na pełne wersje badanych szyfrów, pokazano bowiem, że czas działania rośnie wykładniczo ze wzrostem liczby rund. Ostatecznie autor opisuje najbardziej obiecujące podejście, bazujące na grafie AIG i modelu SAT. Przy opisie trzech etapów tego podejścia autor posłużył się zmodyfikowaną metodą *cut-and-paste*, przepisując odpowiedni tekst ze strony 57, zamieniając SR i SE na PR i PE a zmienną x na odpowiednie logarytmy zadanego prawdopodobieństwa p. Załączono bardzo przydatne, zdaniem recenzenta, skrypty w języku Cryptol, opisujące propagację charakterystyk różnicowych w algorytmach PRESENT i

SIMON oraz propagację charakterystyki różnicowej obciętej dla AES (zredukowany do trzech rund). W ważnym podrozdziale 6.3.3 przedstawiono wyniki badań z zastosowaniem tego podejścia dla trzech w miarę typowych szyfrów blokowych (AES, MIDORI i KLEIN) oraz dla kilku szyfrów blokowych reprezentujących tzw. lekką kryptografię (PRESENT, SPECK, SIMON, PYJAMASK i SATURNIN). Metodę poszukiwania charakterystyk różnicowych obciętych przetestowano na przykładzie szyfrów AES, MIDORI, KLEIN i PRESENT. Otrzymane wyniki uważam za ciekawe i obiecujące, aczkolwiek widać silną zależność od liczby rund i/lub rozmiaru bloków. Mam nadzieję, że te badania będą kontynuowane. Jeśli chodzi o efektywność trzeciego podejścia, to wydajność zaimplementowanego przez autora narzędzia wydaje się być sporo lepsza od dostępnego „na rynku" oprogramowania, np. od CryptoSMT. Jak wiadomo, konwersja grafu AIG do modelu SAT odbywa się za pośrednictwem postaci ANF. Natomiast do konwersji ANF do CNF autor wykorzystywał zmodyfikowane oprogramowanie *open source*. Zauważa on przy tym słusznie, że „inne metody konwersji mogą wpłynąć na skuteczność rozwiązywania modeli SAT określonych poprzez zbiór klauzul formacie CNF". Wyraził też nadzieję, że „w przyszłości w ramach usprawnienia zaimplementowanego narzędzia wykonane zostanie badanie pozwalające wybrać optymalny sposób konwersji". Oczywiście gorąco popieram pomysł zbadania efektywności innych algorytmów konwersji z postaci ANF do postaci CNF. Jak wiadomo postać CNF nie jest jednoznaczna a algorytmy przejścia z ANF do CNF bynajmniej nie są trywialne. Dlatego warto, moim zdaniem, zbadać ten problem, z intencją znalezienia lepszego rozwiązania. Byłbym natomiast ostrożny ze sformułowaniem „optymalny sposób konwersji", ponieważ nie ma pewności, że dla tego zadania optymalny algorytm konwersji w ogóle istnieje. Ciekawa jest też hipoteza sformułowana pod koniec rozdziału szóstego, że sam „rozmiar problemu SAT nie determinuje jednoznacznie czasu wymaganego na rozwiązanie zadania". Autor zaobserwował, że złożoność obliczeniowa zależy od kilku czynników. W szczególności „podczas testów brano pod uwagę m.in. rozmiar i gęstość modelu SAT oraz średni rozmiar klauzuli CNF". Zasadniczo zgadzam się z tym stwierdzeniem, chociaż nie wiem, czy z tego samego powodu co autor rozprawy. `W każdym razie gorąco popieram pomysł bardziej dokładnego sprawdzenia tego w przyszłości.

Rozdział siódmy, ostatni w rozprawie, zawiera podsumowanie osiągniętych przez autora wyników oraz sugestie dotyczące kierunków dalszych badań. Na prawie czterech stronach autor podzielił się swoimi refleksjami i przypuszczeniami co do dalszego rozwoju tej tematyki badawczej. Autor podkreśla, że choć w rozprawie skupił się na kryptoanalizie różnicowej

szyfrów blokowych, to przedstawione podejście może by wykorzystane do automatyzacji procesów związanych z kryptoanalizą liniowa i algebraiczną. Zasugerował, że zastosowany w rozprawie opis propagacji charakterystyk różnicowych z wykorzystaniem grafu AIG można również bez większego problemu zastosować do propagacji charakterystyk liniowych. Powołując się na artykuł [2], którego jest współautorem, pokazał, jak zrobić to w przypadku kryptoanalizy algebraicznej. W pełni zgadzam się z autorem, że opracowane podejście może być łatwo i (co ważniejsze) skutecznie uogólnione na przypadek szyfrów strumieniowych. Obroniona w listopadzie 2022 w Instytucie Informatyki Technicznej SGGW w Warszawie rozprawa doktorska p. Sylwii Stachowiak „SAT-kryptoanaliza wybranych algorytmów kryptografii symetrycznej" podaje prosty przykład takiego uogólnienia. Sam autor również cytuje wcześniejsze prace sugerujące taką możliwość. Bardzo ciekawa jest też sugestia zastosowania rozwijanych metod do poszukiwania charakterystyk różnicowych funkcji skrótu. Zdaniem autora rozprawy „zabieg ten powinien być stosunkowo prosty". Zgadzam się, że powinno to być jak najbardziej możliwe, ale moja intuicja nie jest wystarczająca, aby ocenić, czy jest to rzeczywiście tak proste zadanie, jak sugeruje autor. Ciekawa jest również idea konwersji układu równań w postaci ANF do problemu QUBO a następnie wykorzystanie komputera kwantowego (zakładam, że chodzi o komputer *D-Wave Advantage*, bo innych realistycznych opcji jak na razie nie widzę). Idea ta poparta jest obiecującymi wynikami zaprezentowanymi w artykule [19], dotyczącym możliwego zastosowania kwantowego wyżarzania do ataków algebraicznych na wybrane szyfry blokowe (w artykule tym opisano między innymi transformację pełnego AES-128 do problemu QUBO).

Rozprawę zamyka sześciostronicowa bibliografia, zawierająca 66 pozycji literatury przedmiotu. Uważam, że choć zawiera ona najistotniejsze pozycje, to staranność jej wykonania pozostawia bardzo wiele do życzenia. Celem bibliografii jest przecież umożliwienie czytelnikowi (w tym przypadku recenzentowi) szybką i jednoznaczną identyfikację wykorzystanych źródeł zewnętrznych. Są od lat przyjęte standardy właściwego cytowania, których autor rozprawy niestety nie przestrzega. W szczególności powinny być podane wszystkie istotne szczegóły bibliograficzne, co bardzo ułatwia potencjalnemu czytelnikowi szybkie dotarcie do źródeł. Ekstremalnym przypadkiem nonszalancji w cytowaniu jest pozycja [6] zwierająca wyłącznie autora i tytuł oraz pozycje [34] i [36], gdzie dodatkowo pojawił się rok wydania. Jest to najsłabiej zredagowana część rozprawy, a sytuację, w tym aspekcie, ratują tylko efektywne algorytmy wyszukiwania internetowego opracowane przez Google. Szczerze mówiąc trudno mi zrozumieć taką niefrasobliwość, tym bardziej, że przygotowanie

zadawalającej bibliografii dla autora dobrze przecież znającego literaturę przedmiotu powinno być trywialne.

Przejdę teraz do bardziej szczegółowych choć drobnych uwag krytycznych, które nasunęły mi się w trakcie lektury rozprawy. Są one uporządkowane „chronologicznie" czyli w kolejności pojawiania się w tekście rozprawy. W większości nie są to istotne uwagi merytoryczne a raczej bardziej trywialne poprawki dotyczące literówek, błędów gramatycznych czy innych nieścisłości drobniejszego kalibru.

Str. 11-12. Błąd składniowy we fragmencie „Każda zaproponowana do tej metoda pory działa w czasie wykładniczym."

Str. 12. Literówka w przypisie: "...weryfikacja rozwiązania można zostać wykonana w czasie wielomianowym".

Str. 15. Autor pisze: "...jest bijekcją, to znaczy, że jest odwracalna w obie strony...". Nie bardzo rozumiem, jakie „obie strony" autor ma na myśli. Chodzi przecież o elementarny fakt, że każda bijekcja ma funkcję odwrotną, która też jest bijekcją.

Str. 22. Błąd w nazwisku "Claude Shannone".

Str. 30. Dwie literówki we fragmencie "Zaprezentowanie algorytmu kryptograficznego jako układu równań nad ciałem binarnym umożliwia wykorzystanie szeregu technik związanych z logika binarną. Najczęściej wykorzystywana jest szeroko rozumiana minimalizacji funkcji boolowskiej".

Str. 33. Mało precyzyjne sformułowanie "znacznie zmniejsza rozmiar grafu". Znacznie, czyli jak? W dalszej części tekstu autor pokazuje przykłady dla wybranych szyfrów, ale nie jest jasne ani jak ogólna jest ta uwaga ani jak to naprawdę wpływa na obliczenia?

Str. 33. Literówka we fragmencie "minimalizacji ulega również układu równań nad ciałem binarnym".

Str. 38. Brak spójności we fragmencie "przez Eli’ego Bihama i Adi’ego Shamir". Albo piszemy „Eli’ego Bihama i Adi’ego Shamira” albo „Eli’ego Biham i Adi’ego Shamir”. Ponadto nie rozumiem, dlaczego oba nazwiska pisane są tu kursywą a np. Lars Knudsen na następnej stronie już nie.

Str. 40-41. Na str. 40 pojawia się "Rijndael" a na następnej stronie (w podpisie rysunku 3.3) „AES”. Rozumiem, że jest to skrót myślowy, ale niestety dość niefortunny. Zauważyłem zresztą, że autor dość często używa tych określeń praktycznie jako synonimów. Oczywiście autor wie doskonale, że Rijdael i AES to nie są synonimy. Rijndael jest algorytmem (a właściwie rodziną algorytmów) a AES standardem FIPS-197. Zwykle takie utożsamienie nie prowadzi do nieporozumień, ale w takiej pracy jak recenzowana rozprawa, gdzie bada się efektywność metod kryptoanalitycznych np. w funkcji rund czy wielkości bloków szyfru, klarowne rozróżnienie może być istotne.

Str. 44. Błąd ortograficzny "nie koniecznie".

Str. 45. Dziwne sformułowanie "zbiór dziedzin odpowiadającym zmiennym”. Chyba zgrabniej jest mówić o wartościach zmiennych należących do dziedzin.

Str. 46. Co autor rozumie w tym kontekście przez „skuteczne rozwiązanie” we fragmencie "skutecznie rozwiązałby każdy problem SAT".

Str. 46. Czy teza wyrażona we fragmencie "Współcześnie do rozwiązywania problemów SAT najczęściej wykorzystuje się algorytm CDCL" to intuicja lub obserwacja autora, czy może ktoś zrobił jakieś statystyki?

Str. 48. Literówka we fragmencie "opracowywanie algorytmów i narzędzie do weryfikacji mogących działać".

Str. 54. Rozumiem, że we fragmencie "możemy zatem zapisać równania liniowe dla pierwszej rundy", chodzi tak naprawdę o nierówności.

Wracając do rzeczy istotnych chciałbym podkreślić, że rozprawa jest interesująca i przeanalizowałem ją z dużą przyjemnością. Pomijając wspomniane wcześniej niedociągnięcia, które moim zdaniem nie obniżają jej wartości naukowej, stanowi ona niewątpliwie ważny przyczynek do rozwoju zautomatyzowanych metod ułatwiających kryptoanalizę szyfrów blokowych. Uważam, że tkwi w niej także duży potencjał rozwojowy. Mocną stroną rozprawy, o czym już wcześniej wspominałem, są także obszerne fragmenty działających (sprawdzałem!) kodów, prezentowane w rozdziałach piątym i szóstym. Pomogły one recenzentowi lepiej zrozumieć specyfikę i konkretne aspekty omawianych zagadnień.

Tematykę rozprawy, można bez wątpienia zaliczyć do dyscypliny naukowej informatyka techniczna i telekomunikacja w dziedzinie nauk inżynieryjno-technicznych a przedstawione rozwiązania analizowanych w rozprawie problemów badawczych pozwalają uznać, że mgr inż. Władysław Dudzic jest właściwie przygotowany zarówno do dalszej pracy naukowej jak też do skutecznego wykorzystania zdobytej wiedzy w praktyce.

Podsumowując, uważam, że rozprawa doktorska magistra inżyniera Władysława Dudzica stanowi interesujący wkład w rozwój problematyki kryptoanalizy współcześnie używanych szyfrów blokowych, zwłaszcza w zakresie kryptoanalizy różnicowej. Tematyka podjęta w rozprawie jest ważna i aktualna zarówno w aspekcie praktycznym jak i czysto teoretycznym. Biorąc pod uwagę dynamiczny rozwój szyfrów blokowych oraz ich powszechność, także w biznesie, nie mam wątpliwości, że problematyka ta będzie w najbliższych latach intensywnie rozwijana, dając autorowi szansę na dalsze doskonalenie zaproponowanych rozwiązań. Pozytywnie oceniając poziom naukowy recenzowanej rozprawy doktorskiej i stwierdzając spełnienie wymogów ustawowych, wnoszę o dopuszczenie jej autora do kolejnych etapów przewodu doktorskiego.

Arkadiusz Orłowski