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

**Warszawa, 30 sierpnia 2019 r.**

*RECENZJA ROZPRAWY DOKTORSKIEJ*
*DLA RADY WYDZIAŁY CYBERNETYKI*
*WOJSKOWEJ AKADEMII TECHNICZNEJ W WARSZAWIE*

**Tytuł rozprawy: Problem wyszukiwania kostek w kontekście kryptoanalizy szyfrów blokowych**

**Autor rozprawy: mgr inż. Marcin DAWIEC, Wydział Cybernetyki Wojskowej Akademii Technicznej w Warszawie**

Niniejsza recenzja została opracowana na odpowiedzi na pismo Przewodniczącego Rady Wydziału Cybernetyki WAT, profesora WAT dr. hab. inż. Kazimierza Worwy, realizującego uchwałę Rady Wydziału Cybernetyki WAT nr 175/WCY/2019 z dnia 11 czerwca w sprawie wyznaczenia recenzentów rozprawy doktorskiej mgr. inż. Marcina Jana Dawca.

## Wstęp

Praca jest napisana w języku polskim i liczy 104 strony. Treść pracy podzielona jest na siedem rozdziałów i zawiera dwa dodatki. Rozdział 1 (str. 9-13) zawiera wiadomości wstępne, sformułowanie celu i zakresu rozprawy oraz omówienie jej struktury. W rozdziale 2 (strony 14-40) w sposób syntetyczny omówiono podstawy matematyczne dotyczące problematyki rozprawy: określenie zakresu działania i podstawowych pojęć kryptografii i kryptoanalizy oraz systematyczne przedstawienie własności funkcji boolowskich i sposobu ich wykorzystania w kryptografii. Rozdział 3 (str. 41-52) zawiera prezentację kryptoanalizy korzystającej z kostek (ang. cube attack), począwszy od jej wersji podstawowej, pochodzącej od Shamira i Dinura, do jej wersji zmodyfikowanych, obejmujących testowanie funkcji boolowskich i ataki na szyfry blokowe i strumieniowe, a także najbardziej głośne ataki na funkcje skrótu, w

tym Keccak (SHA-3). W rozdziale 4 (str. 53-65) przedstawiono metody pozyskiwania kostek dla celów fazy wstępnej ataku. Obejmuje on metody znane z literatury (oparte na analizie struktury szyfru, wykorzystującą metody programowania całkowitoliczbowego (MILP) oraz metody losowe), a także autorskie metody oparte na analizie postaci normalnej wielomianów głównych. Kolejny, rozdział 5 (str. 66-78) przedstawia sposób realizacji (opis aplikacji) metod przedstawionych w Rozdziale 4, w tym metody autorskiej wykorzystującą zredukowaną postać ASF wielomianów głównych. Rozdział 6 (str.79-95) w pierwszej swojej części zawiera omówienie sposobu implementacji ataku za pomocą kostek na szyfry blokowe, a w drugiej – realizacje takiego ataku na szyfr CTC autorstwa Nicolas Courtois (o zredukowanej liczbie rund). Rozdział 7 (str.96-98) zawiera podsumowanie przeprowadzonych badań, uzyskane wnioski i zarys możliwości wykorzystania opracowanego nowego sposobu poszukiwania kostek w przyszłych pracach. Dodatki A i B przedstawiają kostki dla szyfru CTC, odpowiednio, cztero- i pięciorundowego. Rozprawa doktorska zawiera także streszczenia w języku polskim i języku angielskim, spisy rysunków, tabel i algorytmów oraz listę najważniejszych symboli. Bibliografia liczy 35 pozycji, w tym 2 prace autorstwa i współautorstwa pana mgr. inż. Marcina Dawca. W pracy umieszczono 12 rysunków, 8 tabel i 14 specyfikacji algorytmów.

Dalszą część recenzji przygotowałem według punktów wzorowanych na zestawie pytań zalecanych w recenzjach wykonywanych dla RW 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) ?**

Praca dotyczy rozwiązania konkretnego zagadnienia kryptoanalizy, jakim jest opracowanie nowego sposobu poszukiwania kostek przydatnych do ataku kryptoanalitycznego (cube attack), który może być efektywnie zrealizowany z wykorzystaniem komputerów roboczych lub małych klastrach obliczeniowych, a także praktyczne potwierdzenie użyteczności nowej metody. Rozprawa jest napisana w konwencji pracy matematycznej, to znaczy omówione i zdefiniowane w niej podstawowe pojęcia wykorzystywane w opisie metody, własności obiektów i

zależności między nimi są zapisane w postaci równań matematycznych, a poszczególne kroki i etapy działania metody są sformułowane w postaci algorytmów zapisanych w pseudokodzie. Ponadto, zarówno informacje dotyczące wykorzystywanych funkcji, w szczególności wielomianów (podstawy matematyczne), jak i skonstruowanych w obiektów i określenia ich własności, zostały zapisane w postaci precyzyjnych definicji i twierdzeń ze stosownymi dowodami. Zatem zakres pracy i jej szczegółowe cele są jasno i precyzyjnie sformułowane.

W rozprawie nie sformułowano wyodrębnionej tezy, jednak jej odpowiednikiem jest zapisany w rozdziale 1.2 „cel wiodący" („wykazanie, że istnieją inne niż wymienione w rozdziale 1.1 sposoby poszukiwania kostek, które są praktycznie realizowalne") i jego rozwiniecie w postaci celów pośrednich dotyczących:

- odpowiedniego sformułowania zadania obliczeniowego (zdefiniowanie zredukowanej postaci ANF wielomianów głównych i zdefiniowanie kostki w tej postaci),
- skonstruowania algorytmu obliczeniowego (sposób poszukiwania kostek w zredukowanej postaci ANF wielomianów głównych i sposób tworzenia takich wielomianów dla szyfrów blokowych),
- wykazania efektywności opracowanej metody przez jej zastosowanie dla szyfru blokowego CTC ograniczonego do 5 rund.

W obrębie nauk technicznych pracę można zaliczyć do kategorii prac teoretycznych, na pograniczu informatyki z dziedziny nauk matematycznych. Tym niemniej, wyniki uzyskane w rozprawie mogą posłużyć do realizacji praktycznych rozwiązań kryptoanalitycznych, a przykład ilustracyjny (atak na szyfr CTC) ma walor eksperymentalny.

**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. Przytoczono i omówiono jedynie te publikacje, które są

ściśle związane z tematem rozprawy (atakiem na szyfr blokowy, w szczególności szyfr CTC) i metodami matematycznymi zaprezentowanymi w rozprawie w rozdziałach 2. (funkcje boolowskie) i 3. (metody ataków korzystających z kostek, głównie na szyfry blokowe). W efekcie liczba cytowanych publikacji jest niewielka, a temat ataków jest potraktowany bardzo wąsko. Takie ujęcie tematu jest zwykle cechą prac z zakresu matematyki, gdzie mamy krótki zarys tematu, założenia twierdzenia, samo twierdzenie (tezę) i dowód. W przypadku rozpraw z obszaru nauk technicznych wskazane byłoby omówienie tematu pracy na tle szerszego obszaru zastosowań (w tym: ataków na funkcje skrótu, tym bardziej, że w tym zakresie znaczny udział mieli polscy kryptoanalitycy). Myślę również, że tego rodzaju studia byłyby korzystne dla samego autora rozprawy, gdyż jego nowa metoda poszukiwania kostek (i kryptoanaliza z jej wykorzystaniem) mogłaby znaleźć zastosowania również dla innych klas algorytmów niż szyfry blokowe.

Reasumując odpowiedź na pytanie o dobór i analizę literatury, prace zacytowane w rozprawie właściwie wprowadzają tematykę badań przeprowadzonych przez doktoranta i stanowią dobrą podstawę do określenia efektywności zaproponowanego algorytmu wyszukiwania kostek i ataku kryptoanalitycznego. Ich dobór wykazuje też kompetencje autora i znajomość przez niego tematyki pracy. Szkoda tylko, że brak jest szerszego omówienia literatury przedmiotu, które byłoby dobrym poszerzeniem rozprawy w kierunku monograficznym, użytecznym dla szerszego grona czytelników.

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

Autor rozprawy precyzyjnie wymienił w rozdziale 1.2 szczegółowe zadania badawcze rozprawy w pięciu punktach:

1. Zdefiniowanie zredukowanej postaci ANF wielomianów głównych; (Rozwiązane w rozdziale 4.5.1).
2. Zdefiniowanie kostki w postaci ANF wielomianów głównych; (Rozwiązane w rozdziale 4.5.3).
3. Określenie sposobu poszukiwania kostek w zredukowanej postaci ANF wielomianów głównych; (Rozwiązane w rozdziale 5.2).

4. Określenie sposobu tworzenia zredukowanej postaci ANF wielomianów głównych dla szyfrów blokowych; (Rozwiązane w rozdziale 5.2).
5. Zastosowanie metody przeglądu zredukowanej postaci ANF wielomianów głównych do poszukiwania kostek w szyfrze blokowym CTC ograniczonym do 5 rund. (Rozwiązane w rozdziałach 4.4 i 6.2).

Są to problemy z zakresu matematyki i dlatego też do ich rozwiązania autor użył właściwie dobranych metod matematycznych, wspartych obliczeniami numerycznymi. Wszystkie wymienione zadania zostały w pracy zrealizowane i właściwie udokumentowane.

Przeprowadzone w rozprawie porównania skuteczności działania metody autorskiej i metod znanych z literatury na przykładzie szyfru CTC potwierdziły, że nowa metoda poszukiwania kostek w szyfrze blokowym wykorzystująca zredukowaną postać ANF wielomianów głównych może być bardziej wydajną niż metody znane z literatury, zatem przyjęte przez autora założenia i zastosowane metody analizy doprowadziły do pozytywnego rozwiązania zadania badawczego.

**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. Najważniejszym oryginalnym osiągnięciem rozprawy jest propozycja nowej procedury znajdowania kostek przydatnych do kryptoanalizy szyfrów blokowych. Jest to metoda dość uniwersalna, to znaczy możliwa do zastosowania dla różnych szyfrów. Jej skuteczność została zweryfikowana na przykładzie szyfru CTC, który wprawdzie nie należy do algorytmów stosowanych w praktyce zabezpieczeń, jest jednak obiektem referencyjnym, zatem uzyskany wynik praktyczny może stanowić odniesienie dla przyszłych prac innych autorów.

W tym miejscu chciałbym zauważyć, że autor nie zadbał o należyte opublikowanie uzyskanych wyników. Rezultaty badań zostały przedstawione w dwóch artykułach w języku polskim opublikowanych w czasopiśmie polskim o ograniczonym zasięgu międzynarodowym. Wyniki te powinny być przedmiotem publikacji

anglojęzycznej w czasopiśmie o szerszym zasięgu lub na renomowanej konferencji międzynarodowej.

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

Rozprawa jest bardzo starannie zredagowana, napisane poprawnym językiem matematycznym i oczywiście poprawna polszczyzną. Autor biegle opanował warsztat naukowy związany z obszarem kryptoanalizy, precyzyjnie formułując twierdzenia i specyfikując algorytmy, a także przedstawiając wyniki numeryczne przykładów obliczeniowych w formie tabel i wykresów. Pewnym mankamentem rozprawy jest trudność dotarcia do definicji podstawowych obiektów używanych w pracy. Na przykład, pojęcie „kostki" występujące już w tytule rozprawy i następnie często w tekście pracy używane, jest wprowadzone w formie definicji dopiero na stronie 45. Warto byłoby, jako integralną część rozprawy, załączyć glosariusz najważniejszych terminów używanych w pracy zawierający, oprócz wymienionej już „kostki", także definicje używanych klas wielomianów i innych pojęć z zakresu kryptografii i kryptoanalizy.

**Jakie są słabe strony rozprawy i jej główne wady?**

Praca jest ogólnie dobrze napisana, uzyskane wyniki są oryginalne i wartościowe. Wśród słabszych stron rozprawy można wskazać już wymienione: brak glosariusza oraz skromny przegląd literatury dotyczącej ataków z wykorzystaniem kostek, a także brak publikacji uzyskanych wyników w renomowanym czasopiśmie. Ponadto, wartość pracy byłaby znacznie większa, gdyby zaproponowaną metodę wyszukiwania kostek zastosowano do któregoś z praktycznie stosowanych algorytmów kryptograficznych, a nie do testowego szyfru CTC. Powyższe uwagi mają charakter dyskusyjny i nie wpływają na moją pozytywną ocenę uzyskanych wyników naukowych.

**Jaka jest przydatność rozprawy dla nauk technicznych?**

Rozprawa doktorska należy do ściśle rozumianego obszaru kryptoanalizy. Definiuje nową metodę wyszukiwania kostek dla szyfrów blokowych przedstawiając dla niej wyniki teoretyczne i specyfikacje algorytmów. Uzyskane wyniki mogą zatem znaleźć zastosowanie w pracach innych kryptoanalityków, zarówno jako punkt wyjściowy dalszych badań teoretycznych, jak i w realizacji testów bezpieczeństwa szyfrów blokowych.

## Podsumowanie i ocena rozprawy

W swojej rozprawie doktorskiej pan magister inżynier Marcin Dawiec 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 szyfrów blokowych, jak też innych algorytmów kryptograficznych, np. szyfrów strumieniowych i kryptograficznie bezpiecznych funkcji skrótu. Rozprawę doktorską pana magistra inżyniera Marcina Dawca 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 technicznych w dyscyplinie naukowej: informatyka (informatyka techniczna i telekomunikacja w dziedzinie nauk inżynieryjno-technicznych wg. nowej nomenklatury) i wnioskuję o jej dopuszczenie do publicznej obrony.

Kotulski

Prof. dr hab. inż. Zbigniew Kotulski