Warszawa, 4 czerwca 2022r.

dr hab. Mirosław Kurkowski, prof. UKSW, prof. WSPol

- **Instytut Informatyki**
  Uniwersytet kard. St. Wyszyńskiego w Warszawie
- **Instytut Służby Kryminalnej**
  Wyższa Szkoła Policji w Szczytnie

Recenzja rozprawy doktorskiej mgra inż. Michała Apolinarskiego

Metody oceny jakości algorytmów generowania

kluczy rundowych w szyfrach blokowych

Promotor: dr hab. inż. Krzysztof Chmiel

Promotor pomocniczy: dr inż. Anna Grocholewska-Czuryło

Niniejsza recenzja została sporządzona na prośbę Senatu Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie wyrażoną w odpowiednim piśmie przez Dziekana Wydziału Informatyki ZUT dra hab. inż. Jerzego Pejasia, prof. ZUT (uchwała WI/Dokt 193/2022). Opiniowana rozprawa doktorska poświęcona jest ocenie algorytmów generowania kluczy rundowych w szyfrach blokowych. Przewód doktorski prowadzony jest w dziedzinie nauk inżynieryjno-technicznych, w dyscyplinie naukowej Informatyka techniczna i telekomunikacja.

Wprowadzenie

W dzisiejszych sieciach i systemach komputerowych z oczywistych względów wymaga się zapewnienia odpowiedniej ochrony przesyłanych lub gromadzonych danych. Ma to być konieczna cecha kluczowych systemów komunikacyjnych zarówno społecznych, urzędowych, czy militarnych. Dane te są przesyłane przez sieci komputerowe lub inne konstruowane i dedykowane systemy łączności, a następnie przechowywane w odpowiednio zabezpieczonych bazach, czy hurtowniach danych. Newralgiczna część lub często całość tych informacji musi być odpowiednio chroniona przed dostępem osób lub instytucji do tego niepowołanych. Jedynym adekwatnym środkiem, który może zapewnić potrzebne cechy bezpieczeństwa i ochrony wrażliwych danych jest zastosowanie odpowiednich algorytmów oraz mechanizmów kryptograficznych. Do zasygnalizowanych wyżej celów wykorzystuje się często szyfry blokowe, wykonujące wiele iteracji (rund) tego samego schematu. Najczęściej w każdej kolejnej rundzie stosowana jest do szyfrowania inna wersja klucza szyfrującego, tzw. klucz rundowy.

Niniejsza rozprawa poświęcona jest ocenie algorytmów generowania kluczy rundowych w szyfrach blokowych. Jakość tych kluczy wpływa na moc kryptograficzną algorytmu zwiększając lub zmniejszając problem jego złamania w sposób zarówno teoretyczny (złożoność obliczeniowa), jak i praktyczny (ataki praktyczne na całe lub części szyfrów lub ich modyfikacje).

W praktyce kryptograficznej jakość algorytmów generowania kluczy rundowych blokowych szyfrów symetrycznych ocenia się po tym, jak wygenerowana przez algorytm sekwencja bitów klucza różni się od sekwencji losowej. Do oceny jakości opisywanych algorytmów stosować można specjalnie do tego celu opracowane testy statystyczne. Pozwalają one z pewnym prawdopodobieństwem określić czy badana sekwencja posiada statystyczne własności charakterystyczne dla sekwencji losowej albo czy jednak występują w niej jakieś defekty statystyczne. Należy tutaj pamiętać, że w przypadku symetrycznych szyfrów blokowych szyfrogram jest sekwencją binarną, która zgodnie z zaleceniami Shannona powinna mieć następujące własności:

- dyfuzję (rozproszenie) – informacja z pojedynczego znaku wiadomości szyfrowanej powinna być rozproszona po całym szyfrogramie,
- konfuzję (nieregularność) – szyfrogram powinien być statystycznie niezależny od klucza.

Zatem w szyfrogramie nie mogą występować jakiekolwiek regularności ani inne zależności między kolejnymi bitami czy nawet między kolejnymi szyfrogramami (tworzonymi przy użyciu tego samego klucza). Występowanie takich defektów ułatwia bowiem kryptoanalizę szyfru.

Autor podejmuje tę niełatwą tematykę i osiąga opisane niżej ważne wyniki. Biorąc zatem pod uwagę obecny stan nauki w rozważanym zakresie oraz najnowsze potrzeby przemysłowe, społeczne i związane z nimi trendy badawcze można z całą pewnością stwierdzić, że badanie algorytmów generowania kluczy rundowych w szyfrach blokowych jest w pełni uzasadnione i istotne biorąc pod uwagę aktualne problemy kryptograficznych systemów zabezpieczeń w sieciach komputerowych i innych systemach łączności.

Zawartość rozprawy

Rozmiar recenzowanej rozprawy jest raczej imponujący. Praca liczy wraz z dodatkami 231 stron. Bez Spisu treści, dodatków oraz Bibliografii rozprawa zawiera 196 stron rozważań. W mojej opinii układ pracy w zasadzie nie budzi zastrzeżeń i jest odpowiedni. Drobne uwagi z tym związane zostaną zamieszczone w dalszych częściach recenzji. Zacytowana w pracy

literatura przedmiotu liczy 109 pozycji i biorąc pod uwagę potrzeby zawartych w rozprawie rozważań jest w mojej opinii dobrana wystarczająco i odpowiednio.

Na początku rozprawy przedstawiono spis stosowanych oznaczeń i akronimów. We Wstępie do rozprawy (oznaczonym jako Rozdział pierwszy) autor określił Cel pracy i hipotezy badawcze:

Celem rozprawy jest zaproponowanie wykorzystania testów statystycznych oraz analizy skupień (ang. cluster analysis), jako elementu wspomagającego i wzbogacającego ocenę konstrukcji algorytmów generowania kluczy rundowych w szyfrach blokowych.

Doktorant określił również tezę rozprawy:

Proponowana metoda „hybrydowa" oceny jakości algorytmów generowania kluczy rundowych szyfrów blokowych, oparta na testach statystycznych i analizie skupień, umożliwia wyznaczenie optymalnego wariantu algorytmu, najbliższego hipotetycznie najlepszemu rozwiązaniu dla zbioru testowanych wariantów, spełniających zadane kryteria projektowe.

Poszczególne cząstkowe zadania badawcze stawiane do realizacji w ramach prowadzonych badań są następujące:

- *Opracowanie metody testowania i oceny algorytmów generowania kluczy rundowych opartej na testach statystycznych oraz analizie skupień.*
- *Przegląd i analiza różnych konstrukcji algorytmów generowania kluczy rundowych szyfrów blokowych (m.in. DES, LOKI97, KASUMI, AES (Rijndael), Serpent, PP-1, PP-2, IDEA, RC6, Speck).*
- *Ocena jakości wybranych algorytmów generowania kluczy rundowych.*

Kolejno w skład rozprawy wchodzą trzy merytoryczne rozdziały główne oraz Podsumowanie zawierające konkluzje z prowadzonych rozważań i otrzymanych wyników badawczych. W pracy zawarto również dodatek zawierający kompletną tabelę wyników p-testów NIST SP800-22 dla różnych wariantów rotacji w algorytmie generowania kluczy rundowych szyfru IDEA oraz kompletną tabelę wartości standaryzowanych cech badanych obiektów w algorytmie IDEA. Na końcu rozprawy znajduje się spis rysunków, tabel, algorytmów oraz wykaz cytowanej literatury.

Rozdział drugi poświęcony jest podstawowym aspektom bezpieczeństwa danych w sieciach i systemach komputerowych. Zaprezentowano w nim różne, stosowane w praktyce algorytmy i mechanizmy zapewniania poufności, w tym szyfry symetryczne. Szczególną uwagę poświęcono szyfrom blokowym i trybom ich pracy. Opisano również pokrótce algorytmy asymetryczne oraz mechanizmy kontroli integralności, w tym jednokierunkową funkcję skrótu i podpis cyfrowy.

Rozdział trzeci zawiera obszerny przegląd i analizę struktury algorytmów służących do generowania kluczy rundowych w wybranych szyfrach blokowych. Są to między innymi algorytmy DES, LOKI97, KASUMI, AES (Rijndael), Serpent, PP-1, PP-2, IDEA, RC6 oraz Speck. Dobór opisanych algorytmów wynika z ich popularności oraz charakterystycznej struktury. Dla każdego z ww. algorytmów, zaprezentowano jego konstrukcję oraz elementy składowe (operacje liniowe lub nieliniowe).

Rozdział czwarty prezentuje metody testowania i oceny jakości generatorów ciągów losowych oraz ciągów pseudolosowych mogących znaleźć zastosowanie jako klucze rundowe szyfrów blokowych. Przedstawiono stosowaną metodologię prowadzenia testów, w tym zasady badania hipotez statystycznych H0 oraz Ha oraz omówiono pakiet testów statystycznych NIST SP800-22. W dalszych częściach tego rozdziału autor zaprezentował wyniki przeprowadzonych samodzielnie badań i eksperymentów. Przedstawiono zaproponowany, nowy sposób doboru kluczy głównych oraz generowania danych wejściowych dla testów statystycznych NIST SP800-22. W ramach prowadzonych badań zaproponowano i opisano następujących pięć metod oceny jakości algorytmów generowania kluczy rundowych w szyfrach blokowych:

- *Metoda A (próbek) – polega na przebadaniu binarnych sekwencji, wytwarzanych przez algorytm generowania kluczy rundowych, wybranymi testami NIST SP800-22. Przykładem zastosowania metody A są badania przeprowadzone nad wybranymi algorytmami generowania kluczy rundowych w szyfrach DES, IDEA, KASUMI, PP-1 i PP-2 oraz nad różnymi wariantami modyfikacji algorytmu generowania kluczy rundowych w szyfrze PP-1.*
- *Metoda B (nadpróbek) – polega na przeprowadzeniu wszystkich rodzajów testów statystycznych pakietu NIST SP800-22, jeśli konstrukcja algorytmu generowania*
- *kluczy rundowych pozwala na wygenerowanie większej liczby kluczy, bez modyfikacji elementów składowych algorytmu, a jedynie przez zwiększenie liczby jego iteracji. Przykładem zastosowania metody B są badania przeprowadzane nad rozszerzonymi (ze zmienionym warunkiem stopu) algorytmami generowania kluczy rundowych szyfrów PP-1 oraz PP-2*
- *Metoda C (metapróbek) – polega na przeprowadzeniu wszystkich testów statystycznych NIST SP800-22, dla algorytmu generowania kluczy rundowych, niezależnie od konstrukcyjnego ograniczenia jego liczby itearcji. Metodę C zastosowano w odniesieniu do algorytmów generowania kluczy rundowych szyfrów: DES, IDEA, KASUMI, PP-1 oraz PP-2.*
- *Metoda D (podpróbek) – polega na przeprowadzeniu wybranych testów NIST SP800-22, na skróconych próbkach, w celu oceny jakości początkowych kluczy rundowych*

algorytmu. Metodę D zastosowano w odniesieniu do algorytmów generowania kluczy rundowych szyfrów: DES, IDEA, KASUMI, PP-1 oraz PP-2.

- *Metoda E (hybrydowa) – polega na przeprowadzeniu testów statystycznych NIST SP800-22, dla różnych wariantów algorytmu generowania kluczy rundowych, w połączeniu z analizą skupień (taksonomią wrocławską), w celu wyznaczenia rozwiązania najbliższego hipotetycznie najlepszemu wariantowi algorytmu. Taksonomia wrocławska to metoda analizy skupień, stosowana do łączenia pewnych obiektów (zmiennych) w grupy jednorodne pod względem z-cech (wymiarów). Przykładem zastosowania metody E (hybrydowej) są przeprowadzone przez autora badania nad wyznaczeniem najlepszego cyklicznego przesunięcia w lewo (rotacji w lewo) w algorytmie generowania kluczy rundowych szyfru IDEA. Innym przykładem wykorzystania metody E (hybrydowej) jest zastosowanie jej do wyznaczenia optymalnego wariantu modyfikacji szyfru PP-1. Spośród dwunastu rozważanych wariantów algorytmu generowania kluczy rundowych wybrano te warianty, które spełniają kryterium jakości, jakim są testy statystyczne. W analizie skupień rozważono zatem sześć wariantów algorytmu (oryginalny, bez rotacji, z operacjami XOR, ze zredukowaną liczbą S-bloków do sześciu, z pozytywnymi (prostymi) modyfikacjami, hipotetycznie najlepszy) z uwzględnieniem dziesięciu cech (dziewięć cech stanowią wyniki poszczególnych testów statycznych, natomiast dziesiątą cechą jest czas generowania kluczy).*

W rozdziale piątym doktorant zawarł wnioski z otrzymanych wyników i dokonał podsumowania rozprawy, w tym także oceny wartości teoretycznej i praktycznej proponowanych, autorskich rozwiązań.

Opinia merytoryczna rozprawy

Jak napisałem wcześniej, układ rozprawy moim zdaniem jest odpowiedni i nie budzi zastrzeżeń. Wstępne części rozprawy wprowadzające podstawowe pojęcia i definicje struktur potrzebne do dalszych rozważań moim zdaniem zostały opracowane bardzo dobrze. Uważam, że czytelnik jest dobrze zaznajomiony z podstawami teoretycznymi oraz obecnym stanem wiedzy w rozważanej tematyce, aby dalej zrozumiale śledzić zawarte w rozprawie treści. Można zastanawiać się po co w rozprawie poświęconej szyfrom symetrycznym informacje o algorytmach asymetrycznych, czy funkcjach skrótu, ale można zrozumieć, że autor chciał kompleksowo opisać choć w zarysie ogół głównych gałęzi kryptografii.

W rozdziale czwartym przedstawiono:

- metodologię testów statystycznych, służących do badania generatorów ciągów losowych i pseudolosowych,

- szczegółowy opis pakietu testów NIST SP800-22 oraz jego zastosowanie do:
  - oceny algorytmów generowania kluczy rundowych wielu szyfrów,
  - zaprojektowania algorytmu generowania kluczy rundowych dla szyfru PP-1 64/64,
  - oceny algorytmu generowania kluczy rundowych szyfru PP-2 64/128, traktowanego jako generator liczb pseudolosowych,
  - oceny algorytmów generowania kluczy rundowych wielu szyfrów,
  - oceny początkowych kluczy algorytmów generowania kluczy rundowych wielu szyfrów,
  - optymalizacji algorytmu generowania kluczy rundowych w szyfrze IDEA, polegającą na wyborze najlepszej wartości parametru rotacji,
  - optymalizacji algorytmu generowania kluczy rundowych szyfru PP-1 64/64, z uwzględnieniem czasu obliczeń,
  - optymalizacji algorytmu generowania kluczy rundowych szyfru PP-1 64/64, bez uwzględnienia czasu obliczeń.

Powyższe prace wymagały ogromnego wkładu pracy. Zasługują one na najwyższe uznanie. Badania przeprowadzono prawidłowo.

W wyniku przeprowadzonych obliczeń uzyskano wiele ciekawych wyników dotyczących jakości znanych szyfrów. I tak:

- stosując metodę próbek, przy losowych wartościach kluczy głównych, algorytmy generowania kluczy rundowych w szyfrach DES, IDEA, KASUMI, nie spełniają kryterium jakości (losowości), a w szyfrach PP-1 i PP-2 spełniają,
- w metodzie próbek, przy losowych wartościach kluczy głównych, w wariancie oryginalnym algorytmu generowania kluczy rundowych szyfru PP-1 64/64 oraz w jego wersjach (modyfikacjach): wersja 1 bez rotacji RR, wersja 2 z operacjami XOR, wersja 3.3 z sześcioma S-blokami i wersja 5 złożona z pozytywnych modyfikacji (bez RR, XOR, 6 S-bloków), spełnione jest kryterium jakości (losowości), lecz w pozostałych wersjach (opisanych w 3.1, 3.2, 4.1, 4.2, 6, 7) – nie jest spełnione to kryterium,
- w metodzie nadpróbek, przy kolejnych wartościach kluczy głównych, rozszerzony algorytm generowania kluczy rundowych w szyfrze PP-2 64/128 jest dobrym jakościowo generatorem liczb pseudolosowych,
- w metodzie nadpróbek, przy kolejnych wartościach kluczy głównych, rozszerzony algorytm generowania kluczy rundowych szyfru PP-1 64/128 można uznać za dobry jakościowo generator liczb pseudolosowych,
- w metodzie metapróbek, przy losowych wartościach kluczy głównych, algorytmy generowania kluczy rundowych szyfrów PP-1 64/128 i PP-2 64/128 spełniają, a szyfrów DES, IDEA, KASUMI nie spełniają kryterium jakości (losowości), natomiast

przy kolejnych wartościach kluczy głównych żaden z wymienionych algorytmów nie spełnia tego kryterium,

- w metodzie podpróbek, przy wariancie losowych kluczy głównych, algorytmy generowania kluczy rundowych szyfrów PP-1 64/128 oraz PP-2 64/128 spełniają kryterium jakości, a szyfrów DES, IDEA, KASUMI – nie spełniają tego kryterium,
- w metodzie hybrydowej, przy wariancie losowych kluczy głównych, optymalnym wariantem algorytmu generowania kluczy rundowych w szyfrze IDEA, jest wariant z operacją rotacji w lewo o 71 bitów,
- w metodzie hybrydowej, przy wariancie losowych kluczy głównych, optymalnym wariantem algorytmu generowania kluczy rundowych w szyfrze PP-1 64/64, z uwzględnieniem czasu obliczeń, jest wariant złożony z pozytywnymi modyfikacjami, tj. bez rotacji RR, z operacjami XOR zamiast dodawania i odejmowania modulo 256 oraz z liczbą S-bloków zredukowaną do sześciu,
- w metodzie hybrydowej, przy wariancie losowych kluczy głównych, optymalnym wariantem algorytmu generowania kluczy rundowych w szyfrze PP-1 64/64, z pominięciem czasu obliczeń, jest wariant z sześcioma S-blokami.

Na szczególne podkreślenie w rozprawie, zasługują następujące prace:

- wyodrębnienie metod A, B, C, D, na podstawie próbek, nadpróbek, metapróbek i podpróbek, stanowiących różne warianty konkatenacji kluczy rundowych,
- zaproponowanie metody E (hybrydowej) zastosowania testów statystycznych NIST SP800-22 w powiazaniu z analizą skupień, do optymalizacji algorytmu generowania kluczy rundowych szyfrów IDEA oraz PP-1 64/64.

Przedstawione wyniki badań pozwalają wyrazić przekonanie o udowodnieniu tezy rozprawy:

Podsumowując tę część recenzji stwierdzam, że moim zdaniem mgr inż. Michał Apolinarski zrealizował postawione sobie Cele badawcze i wykazał prawdziwość postawionych na początku rozprawy tez.

Uwagi polemiczne i krytyczne oraz elementy dyskusyjne

Przedstawione niżej uwagi nie zmniejszają moim zdaniem wartości naukowej rozprawy i nie mają wpływu na pozytywną opinię pracy jako całości. Zamieszczone uwagi mogą też stanowić pole do dalszych badań.

W poświęconym podstawom mechanizmów kryptograficznych rozdziale drugim, autor zawarł fragment opisujący tryby pracy szyfrów blokowych tj. ECB (ang. *Electronic Codebook*), CBC (ang. *Cipher Block Chaining*), CFB (ang. *Cipher Feedback*), OFB (ang. *Output Feedback*). Fragment ten jest oczywiście poprawny merytorycznie, jednakże w mojej

ocenie jest on nadmiarowy w kontekście prowadzonych badań i ogólnie problematyki rozprawy. Badania dotyczyły komponentu szyfru jakim jest algorytm generowania kluczy rundowych i jego wpływu na jakość szyfru niezależnie od stosowanych trybów pracy. A może należałoby zbadać czy zastosowanie różnych metod generowania kluczy ma jednak wpływ na jakość pracy szyfru w różnych trybach jego pracy?

W rozdziale trzecim zawarto przegląd oraz dość szczegółową analizę szesnastu! wybranych algorytmów generowania kluczy rundowych. Wybór ten autor argumentuje ich popularnością, ciekawą konstrukcją oraz znanymi słabościami. Niestety tylko niektóre z opisów przedstawionych szyfrów zawierają wzmiankę o aktualnie najlepszym wobec nich ataku kryptoanalitycznym. W ramach grupy szyfrów o typie konstrukcji sieci Feistela, najnowszy z analizowanych szyfrów powstał w 2021 roku (szyfr LCB-IoT). W grupie szyfrów o konstrukcji sieci SPN oraz „inne sieci" najnowsze z opisanych algorytmów są z roku 2013 (PP-2 oraz Speck).

W prezentującym wyniki badań autorskich doktoranta rozdziale czwartym brakuje wyjaśnienia dlaczego do testów i oceny wybrano algorytmy: DES, IDEA, KASUMI oraz PP-1 i PP-2? Można się domyślać, że DES został wybrany jako popularny i bardzo dobrze przebadany dawny standard szyfrowania symetrycznego stosujący generowanie kluczy rundowych. DES może zatem stanowić pewien punkt odniesienia w prowadzonych rozważaniach. Z kolei szyfry PP-1 oraz PP-2 wybrano zapewne ze względu na powiązania autora z zespołem twórców w/w szyfrów. Niestety niedosytem jest brak wśród przebadanych algorytmów obecnego standardu: AES (Rijndael). Można mieć nadzieję, że jest to jeden z dalszych celów badawczych doktoranta, który zaowocuje dalszymi publikacjami.

Algorytm konstruowania dendrytu (algorytm 4.1) składa się z 5 kroków. W metodzie E „hybrydowej" oceny jakości algorytmu generowania kluczy rundowych autor pomija krok czwarty oraz piąty tego algorytmu tworząc jak to nazywa: „dendryt wrocławski 1-stopnia skupień jednorodnych". Czy nie byłoby interesujące skonstruowanie spójnego dendrytu (drzewa), co umożliwiłoby umiejscowienie każdego wariantu ocenianego algorytmu względem wariantu hipotetycznego?

W Podsumowaniu autor wskazuje wykorzystanie testów statystycznych spoza pakietu NIST SP800-22 jako interesujący kierunek dalszych badań, w szczególności badań nad kryterium praktycznym oceny algorytmów generowania kluczy rundowych. Nie wskazuje jednak o jakie testy chodzi.

W recenzowanej rozprawie istnieje kilka aspektów otwartych, w ramach których można przeprowadzić szerszą dyskusję podczas publicznej obrony.

Uwagi redakcyjne

Jak każda praca naukowa również recenzowana rozprawa nie jest wolna od niedociągnięć, pomyłek, czy błędów natury redakcyjnej. Z przyjemnością muszę jednak stwierdzić, że rozprawa mgra inż. Michała Apolinarskiego zawiera wyjątkowo mało takich pomyłek i jest pod tym względem jedną z najlepszych rozpraw jakie do tej pory recenzowałem. Poniżej zamieszczam listę kilku przykładowych pomyłek/błędów/niejasności:

- str. 91 - *…klucz rundowych K_{32} dodawany jest…* ,
- str. 91 - *… W algorytmie tym możliwe jest zwiększenia liczby iteracji…*
- str. 93 - …*Ostatecznie bit K5[0] zależy tylko od bitu k[76] klucza głównego, o długości 128 bitów, co stanowi 0.78%.* (czego 0,78%??)
- str. 93 - *…zależy od liczby bitów klucza k: 1 (i = 1,2, …, 5).* (pierwszego, jednego bitu??)
- str. 93 - *…Operacja liniowe:…*
- str. 94 - *...funkcja nieliniowa, składająca się z operacji wykonywanych na bajtach, 64-bitowego podbloku n-bitowego bloku xi oraz bajtach, 64-bitowych podkluczy n-bitowych kluczy rundowych...*
- str. 98 - *...możliwe jest przeprowadzenia kryptoanalizy różnicowej,…*
- str. 98 – w Tabeli 3.36. może zamiast opisu kolumn: *rodzaj / operacja* lepszy byłby opis: *operacja / oznaczenie?*
- str. 100 - *…wykorzystywane są dwa klucze rundowy…*
- str. 102 - *…suma wyłączają (XOR) słów 8-bitowych…*
- str. 137 - *…testowana sekwencja (...) nie zakończy się sukcesem…*

Oczywiście błędy te nie wpływają na jednoznacznie pozytywną ocenę zwartości rozprawy.

Wniosek końcowy

Przedstawione w recenzowanej rozprawie doktorskiej rozważania związane z metodami oceny algorytmów generowania kluczy rundowych w szyfrach blokowych dotyczą bieżących, ważnych i interesujących problemów naukowych związanych z konstrukcją i metodami analizy współczesnych systemów kryptograficznych. Rozprawa doktorska mgra inż. Michała Apolinarskiego zawiera wiele oryginalnych oraz interesujących wyników. Należy podkreślić wykonanie olbrzymiej liczby badań eksperymentalnych oraz bardzo staranne i merytorycznie można powiedzieć, że wzorcowe przygotowanie rozprawy. Moje uwagi krytyczne zawarte w recenzji nie zmieniają pozytywnej opinii o rozprawie jako całości.

Biorąc pod uwagę wyniki naukowe przedstawione w recenzowanej rozprawie doktorskiej mgra inż. Michała Apolinarskiego stwierdzam, że moim zdaniem, praca ta spełnia wymagania stawiane rozprawom doktorskim przez obowiązującą aktualnie w Polsce Ustawę o Stopniach i Tytule Naukowym. Stawiam zatem wniosek o dopuszczenie mgra inż. Michała Apolinarskiego do dalszych etapów przewodu doktorskiego prowadzonego w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie Informatyka techniczna i telekomunikacja w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie.