Szczecin, 11.07.2022

STRESZCZENIE ROZPRAWY DOKTORSKIEJ

Metody oceny jakości algorytmów generowania kluczy rundowych w szyfrach blokowych

Autor: mgr inż. Michał Apolinarski
Promotor: dr hab. inż. Krzysztof Chmiel
Promotor pomocniczy: dr inż. Anna Grocholewska-Czuryło

Algorytmy generowania kluczy rundowych wykorzystywane są w szyfrach blokowych do wygenerowania z klucza głównego (przeważnie o długości pomiędzy 64 a 256 bitów), zbioru kluczy rundowych wykorzystywanych następnie, w rundach (iteracjach), właściwego procesu szyfrowania lub deszyfrowania. Istotną cechą jest to, aby wygenerowane przez ten algorytm klucze rundowe posiadały właściwości statystyczne zbliżone do ciągów losowych, co wpływa na proces kryptoanalizy szyfru.

Do oceny właściwości statystycznych ciągów pseudolosowych (za takie ciągi należy uznać szyfrogram oraz klucze rundowe), zastosowanie mają różnego rodzaju testy statystyczne, m.in. testy NIST SP800-22 wykorzystane w konkursie na standard AES do oceny szyfrów blokowych.

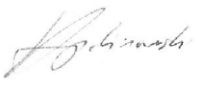
W rozprawie wykorzystano testy NIST SP800-22 do oceny algorytmów generowania kluczy rundowych, na podstawie sekwencji kluczy rundowych, o długości kilkuset lub kilku tysięcy bitów dla pojedynczej wartości klucza głównego.

Projektując algorytm generowania kluczy rundowych należy znaleźć kompromis pomiędzy szybkością generowania kluczy, a bezpieczeństwem, w szczególności kiedy projektowany szyfr ma być „lekki" (ang. *lightweight*) czyli stosowany w środowisku o małych, ograniczonych zasobach, np. karta RFID. Przy takich ograniczeniach problematyczne staje się określenie optymalnych struktur spełniających zadane kryteria. Zatem podczas projektowania algorytmu generowania kluczy rundowych warto rozważyć i przetestować różne warianty zastosowanych operacji, np. rotacji (cyklicznego przesunięcia), permutacji, podstawień, stałych lub innych przekształceń.

Celem rozprawy jest zaproponowanie wykorzystania testów statystycznych oraz analizy skupień, jako elementu wspomagającego i wzbogacającego ocenę konstrukcji algorytmów generowania kluczy rundowych w szyfrach blokowych. Poszczególne zadania cząstkowe zrealizowane w rozprawie to:

- 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 teoretyczna oraz praktyczna jakości wybranych algorytmów generowania kluczy rundowych.

11.07.2022



Szczecin, 11.07.2022

DOCTORAL THESIS ABSTRACT

QUALITY EVALUATION METHODS OF KEY SCHEDULE ALGORITHMS IN BLOCK CIPHERS

Author: mgr inż. Michał Apolinarski
Supervisor: dr hab. inż. Krzysztof Chmiel
Auxilary supervisor: dr inż. Anna Grocholewska-Czuryło

Key schedule algorithms in block ciphers are used to generate a set of round keys from a master key (that is usually between 64 and 256 bits in length). These keys are then used in rounds (iterations) during the actual encryption or decryption process. An important requirement is that the round keys generated by this algorithm should have statistical properties similar to random sequences, which affects the process of cipher cryptanalysis.

To evaluate the statistical properties of pseudorandom sequences (ciphertext and round keys should be considered as such sequences), various types of statistical tests are applicable, including the NIST SP800-22 tests used in the competition for the AES standard to evaluate block ciphers.

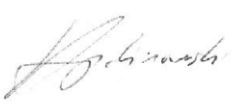
In doctoral thesis NIST SP800-22 tests were used to evaluate key schedule algorithms, based on sequences of hundreds or thousands bits long round keys, generated from a single master key.

When designing a key schedule algorithm, it is necessary to find a tradeoff between the speed of round keys generation and security, especially when the designed cipher should be "lightweight", i.e. used in an environment with small, limited resources, such as an RFID card. With such limitations, it becomes problematic to determine the optimal structures that meet the given criteria. Thus, when designing a key schedule algorithm, it is worth to consider and test different variants of the operations used, such as rotation (cyclic shift), permutation, substitution, constants or other transformations.

The main goal of the dissertation is to propose the use of statistical tests and cluster analysis as an element that supports and enhances the evaluation of the design of key schedule algorithms in block ciphers. The various sub-tasks accomplished in the dissertation are.:

- Develop a method for testing and evaluating key schedule algorithms based on statistical tests and cluster analysis.
- Review and analysis of various designs of key schedule algorithms for block ciphers (including DES, LOKI97, KASUMI, AES (Rijndael), Serpent, PP-1, PP-2, IDEA, RC6, Speck).
- Theoretical and practical evaluation of the quality of selected key schedule algorithms.

11.07.2022



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.

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

Warszawa, 17 maja 2022 r.

RECENZJA ROZPRAWY DOKTORSKIEJ
DLA WYDZIAŁU INFORMATYKI
ZACHODNIOPOMORSKIEGO UNIWERSYTETU TECHNOLOGICZNEGO
W SZCZECINIE

Tytuł rozprawy: Metody oceny jakości algorytmów generowania kluczy rundowych w szyfrach blokowych

Autor rozprawy: Michał Apolinarski, Wydział Informatyki i Telekomunikacji Politechniki Poznańskiej

Niniejsza recenzja została opracowana na odpowiedzi na pismo Dziekana Wydziału Informatyki ZUT, profesora ZUT dr. hab. inż. Jerzego Pejasia, realizującego uchwałę Senatu Zachodniopomorskiego Uniwersytetu Technologicznego z dnia 28 marca 2022 roku w sprawie wyznaczenia recenzentów w przewodzie doktorskim mgr. inż. Michała Apolinarskiego.

Wstęp

Praca jest napisana w języku polskim i liczy 231 stron. Treść pracy podzielona jest na sześć rozdziałów i wykaz literatury. Rozdział 1 (str. 8-13) zawiera wiadomości wstępne dotyczące tematyki rozprawy, sformułowanie celu i tezy rozprawy oraz omówienie jej struktury. W rozdziale 2 (strony 14-26) przedstawiono podstawowe usługi bezpieczeństwa jakimi są poufność i integralność danych. Jako algorytmy realizujące poufność zaprezentowano szyfry symetryczne i asymetryczne, a realizujące usługę integralności - kryptograficznie bezpieczne funkcje skrótu i podpisy elektroniczne (cyfrowe). Omówione też zostały tryby pracy szyfrów blokowych zwiększające bezpieczeństwo w usłudze poufności. W tym krótkim przeglądzie usług bezpieczeństwa warto było jeszcze wspomnieć o nowych trybach pracy szyfrów blokowych realizujących usługę autentyczności danych, integralności danych oraz równocześnie poufności i autentyczności. Warto też byłoby omówić konstrukcje funkcji skrótu wykorzystujących szyfry blokowe. Prezentacja tych dodatkowych zastosowań szyfrów blokowych podkreśliłoby ich wagę we współczesnej kryptografii, a zatem również wagę badań przedstawionych w recenzowanej rozprawie. Obszerny Rozdział 3 (str. 27-135) zawiera ogólną prezentację struktury szyfru blokowego, oraz przegląd i analizę algorytmów generowania kluczy rundowych kilkunastu szyfrów blokowych o różnej strukturze budowy (permutacja Feistela, sieć podstawieniowo-permutacyjna i inne) począwszy od pierwszego rekomendowanego standardy szyfru

blokowego DES z roku 1975, do najnowszych konstrukcji z lat dwutysięcznych, w tym także konstrukcji powstałych w macierzystej uczelni Doktoranta. W opisie przedstawianych algorytmów uwzględniono ich konstrukcję i wykorzystane elementy składowe (przekształcenia liniowe lub nieliniowe). Warto tutaj zwrócić uwagę na trwający obecnie konkurs NIST na lekki algorytm kryptograficzny, na który zgłoszono 57 szyfrów. Byłby to bogaty materiał badawczy do analizy algorytmów generowania kluczy rundowych. W Rozdziale 3 przedstawiono główne wyniki teoretyczne rozprawy związane z charakteryzacją cech szyfrów blokowych i porównaniem zestawów tych cech szyfrów dla 16 przebadanych algorytmów. Szczególnie wartościowy jest wybór (w rozdziale 3.5) 18 kryteriów charakteryzujących szyfry i zestawienie w tablicach własności badanych szyfrów według tych kryteriów.

Rozdział 4 (str. 136-196) jest w głównej mierze reportem w badań eksperymentalnych przeprowadzonych w ramach rozprawy. W pierwszej swej części przedstawia omówienie metod statystycznego testowania generatorów ciągów pseudolosowych i oceny ich przydatności do celów kryptograficznych. Przedstawiono zasady konstruowania testów statystycznych i wnioskowania o prawdziwości hipotez statystycznych. Zaprezentowano również powszechnie stosowany w kryptografii pakiet testów statystycznych NIST SP800-22 rev.1a. Najważniejszą częścią Rozdziału 4 i całej rozprawy są wyniki eksperymentów przeprowadzonych przez Doktoranta oraz ich analiza. W tej części przedstawiono plan eksperymentu składającego się z wygenerowania zbioru kluczy głównych szyfru oraz odpowiadającego tym kluczom ciągu kluczy rundowych tworzącego pseudolosowy strumień binarny podlegający testowaniu zestawem piętnastu testów NIST SP800-22 rev.1a. W jednym ze schematów zastosowano metody grupowania obiektów (taksonomii wrocławskiej). Testy przeprowadzono według pięciu planów dostosowanych do możliwości generowania ciągów kluczy rundowych oferowanych przez przykładowe badane szyfry blokowe. Na tej podstawie oceniono jakość algorytmów generowania kluczy rundowych w szyfrach blokowych. Schematy testów posłużyły nie tylko do oceny jakości algorytmów generowania kluczy, lecz także do próby optymalizacji tych algorytmów w ramach różnych wariantów generowania. Zaproponowana metoda optymalizacji jest wynikiem rozprawy który może znaleźć zastosowanie w badaniach nowych konstrukcji szyfrów blokowych.

Kolejny, Rozdział 5 (str. 197-203) podsumowuje rozprawę. Zawiera zestawienie wniosków uzyskanych z przeprowadzonych prac naukowych oraz uwagi Doktoranta na temat użyteczności teoretycznej i praktycznej zaprezentowanych wyników badań. Rozdział 6 (str.204-209) zawiera dodatki w postaci tabel kompletnych wyników liczbowych testów przeprowadzonych dla algorytmu IDEA.

Ponadto, praca zawiera spis rysunków (87 pozycji), spis tabel (74 pozycje) oraz spis specyfikacji algorytmów (23 algorytmy). Wykaz literatury liczy 109 pozycji, w tym 4 prace autorstwa pana mgr. inż. Michała Apolinarskiego.

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)?

Praca dotyczy oceny jakości szyfrów blokowych. Głównym celem pracy jest zaproponowanie metody zbadania jakości algorytmu generowania kluczy rundowych na podstawie klucza głównego, przeprowadzenie testów oceniających zarówno szyfry i ich procedury generowania kluczy, jak i metodę badania jakości. Ponadto zaproponowano schemat scharakteryzowania konstrukcji szyfrów blokowych względem kilkunastu cech charakterystycznych, a jako efekt wykorzystania procedury oceny sposobu generowania kluczy - metodę optymalizacji konstrukcji szyfrów. Wszystkie cele pracy zostały precyzyjnie sformułowane, ich realizacja właściwie opisana, a wyniki dobrze udokumentowane. W szczególności, właściwie sformułowana i udowodniona została teza 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.*" Zaznaczymy, że teza to tylko jeden z efektów bardzo obszernych badań obejmujących zarówno teorię budowy szyfrów blokowych, jak i ich eksperymentalne badanie.

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?

Praca dotyczy bardzo szczególnego zagadnienia dotyczącego analizy bezpieczeństwa szyfrów. Ogólne wprowadzenie do tematu kryptografii zostało ściśle ukierunkowane na rozwiązywany problem badawczy. Literatura dotycząca analizowanych szyfrów jest właściwie dobrana i umożliwia zapoznanie się ze specyfikacją algorytmów. Moim zdanie podstawy statystyczne testów powinny być zaprezentowane na podstawie literatury matematycznej z zakresu statystyki. Autor korzysta w swych badaniach eksperymentalnych z zestawu testów NIST SP 800-22 rev.1a. Testy te nie są autorstwa redaktorów tego standardu, a stanowią kompozycję testów pochodzących z kilku źródeł. Na str. 152 Autor wymienia kilka zestawów testów przeznaczonych dla celów badania jakości algorytmów kryptograficznych. Jest tam wymieniony zestaw Diehard Georga Marsaglii. Na przykład, test 5 w zestawie NIST pochodzi z Diehard. Testy 1-4 z obecnego zestawu NIST były zaproponowane w standardzie FIPS 140 i poprawione w standardzie FIPS 140-1, a test 9 był opublikowany z pracy U.M. Maurer, "A universal statistical test for random bit generators." J. Cryptology 5, 89–105 (1992). https://doi.org/10.1007/BF00193563. Warto byłoby odnieść się do źródeł przy opisie testów, ponieważ testy stanowią w rozprawie podstawowe narzędzie badawcze w części eksperymentalnej rozprawy.

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

Autor rozprawy precyzyjnie sformułował problem badawczy, następnie dokładnie sformułował metodę rozwiązania (sposób testowania), przeprowadził badanie i udokumentował wyniki. Sposób zbudowania poszczególnych eksperymentów był obiektywnie uwarunkowany zasobem posiadanych danych podlegających analizie. Sposób przeprowadzenia eksperymentu nie budzi zastrzeżeń.

Chciałbym jednak prosić Doktoranta na odpowiedź na pytanie dotyczące testów. Jak zaobserwowałem w badaniach różnych autorów, często wykorzystują oni jedynie część testów z zestawów NIST SP 800-22 (w obu wersjach), ponieważ cały zestaw bada generator wszechstronnie, dla różnych długości wygenerowanych serii, co nie zawsze jest konieczne. Pytanie jest takie: Czy przeprowadzono badanie jednego algorytmu generowania kluczy rundowych wszystkimi metodami (lub innego generatora ciągów binarnych) wszystkimi metodami A-E, żeby ocenić skuteczność metod w poprawność doboru testów (nie: jakość generatorów)?

I jeszcze jedna uwaga na marginesie. W rozprawie przebadano algorytmy kryptograficzne o różnej liczbie rund i różnej jakości generowania kluczy rundowych jako ciągów pseudolosowych. Ciekawe byłoby zbadanie algorytmu GodSave autorstwa Dianelosa Georgoudisa z firmy TecApro Internacional, w którym w podstawowej wersji przyjęto jedną rundę szyfrowania zakładając, że algorytm generowania klucza rundowego jest wystarczająco silny do takiego 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?

Szyfry blokowe stanowiące klasykę kryptografii stają się ponownie centrum zainteresowania projektantów algorytmów co najmniej z dwóch powodów. Szyfry te nadal pozostają odporne na ataki z wykorzystaniem komputerów kwantowych, a więc mogą być składnikiem nowych protokołów bezpieczeństwa (np. zaawansowane tryby pracy szyfrów) a ponadto są niezbędne w licznie wprowadzanych urządzeniach IoT (por. konkurs na lekką kryptografię). Autor rozprawy doktorskiej przeprowadził oryginalne badania teoretyczne i obliczeniowe odpowiadające potrzebom projektantów nowych algorytmów. Uzyskane wyniki są przedmiotem czterech indywidualnych publikacji autora (jedna z listy WoS), co potwierdza dużą samodzielność prowadzonych badań i ich wysoki poziom. Warto przy tym zauważyć, że publikacje (i prowadzone prace badawcze) dotyczą również badania algorytmów szyfrowania opracowanych w Politechnice Poznańskiej (PP-1 i PP-2), co dobrze świadczy o użyteczności prowadzonych prac w ramach macierzystego zespołu Doktoranta.

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

Rozprawa jest bardzo starannie zredagowana i dobrze napisana. Algorytmy

kryptograficzne są scharakteryzowane w ujednoliconej formie, co bardzo ułatwia ich porównanie. Zestawienie wyników w tabelach również znakomicie charakteryzuje algorytmy i dodatkowo, podkreśla trafność doboru parametrów charakteryzujących szyfry. Również rysunki przedstawiające schematy szyfrów są bardzo dobrze wykonane i dobrze pełnią swoją rolę. Drobne zastrzeżenie budzi rysunek 3.1, który sugeruje równoległość wykonywania rund szyfrowania i generowania kluczy rundowych. Mam także zastrzeżenie do nazwania cech algorytmu kryptograficznego w rozdziale 3 słowem "charakterystyka" z numerami od 3.1 dla algorytmu DES do 3.16. Zestawienie DES i "charakterystyka" skojarzyło mi się natychmiast z "charakterystyką różnicową" wprowadzoną przez Eli Bihama i Adi Shamira w latach 1980-tych w kontekście analizy różnicowej DES (por. Eli Biham, Adi Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer Verlag, 1993).

Pytanie dotyczące generowania kluczy głównych za pomocą generatora ciągów pseudolosowych (wzór (4.9)) dla metody C (str. 171): Czy zbadano jakość tego generatora - losowość/statystyczną niezależność generowanych kluczy? Czy nie lepiej byłoby do tego celu użyć generatora ciągów losowych?

Jakie są słabe strony rozprawy i jej główne wady?

Praca jest ogólnie dobrze napisana i nie ma wad dotyczących przeprowadzonych badań naukowych czy jakości prezentacji uzyskanych wyników. Uwagi w tym punkcie dotyczą zagadnień wprowadzających do tematu i drobnych uwag redakcyjnych.

Na str. 22 dla warunków bezpieczeństwa funkcji skrótu pominięto własność "second pre-image resistance" oznaczającą, że dla dowolnego tekstu i jego skrótu obliczeniowo trudne powinno być znalezienie innego tekstu dającego ten sam skrót.

Skrót SPN pierwszy raz użyty jest na str. 27, a jego wyjaśnienie jest na str. 30.

Na str. 33 podano, że algorytm DES został opracowany przez firmę IBM. Raczej należałoby napisać, że przez zespół Horsta Feistela z firmy IBM na zamówienie NBS.

Na str. 76 jest przedstawiona Charakterystyka 3.8 dla algorytmu AES. Jest to trochę mylące, bo AES (i inne algorytmy z konkursu NIST) to 9 szyfrów o różnych długościach klucza, długościach bloków i liczbie rund. Warto pomyśleć, jak to przedstawić bardziej przejrzyście.

Na str. 136 przedstawiono dyfuzję jako własność szyfrogramu. Jak pokazuje opis tych własności, jest to własność szyfru (lub rundy szyfru). Można też było wspomnieć o "mieszaniu i rozpraszaniu" oraz "lawinowości i zupełności" jako parach cech rundy.

W całej rozprawie (poza wykazem literatury, gdzie cytowana jest właściwa wersja dokumentu) Autor powołuje się na standard NIST SP 800-22, chociaż wykorzystuje testy z dokumentu SP 800-22 rev.1a. Pierwotny dokument SP 800-22 zawierał 16 testów. Test "Lempel-Ziv Compression Test" w poprawionej wersji został wycofany jako nie dostarczający dodatkowej informacji w stosunku do pozostawionych 15 testów (używanych przez Doktoranta w rozprawie).

Na stronie 137 jest fragment dotyczący definicji i własności testu statystycznego, opracowany zgodnie z odpowiednim fragmentem przedstawionym w NIST SP 800-22 rev.1a. Fragment ten nie dotyczy testów zawartych w standardzie. Wszystkie testy używane w SP 800-22 (w obu wersjach) to statystyczne testy istotności, a więc testy wyłącznie hipotezy H_0 bez hipotezy alternatywnej. Wnioskujemy: "hipoteza H_0 jest fałszywa i należy ją odrzucić" lub " nie ma podstaw do odrzucenia hipotezy H_0" (co nie oznacza, że prawdziwa jest jakakolwiek inna hipoteza). Popełnić można tylko błąd pierwszego rodzaju, czyli odrzucić hipotezę prawdziwą.

Jaka jest przydatność rozprawy dla nauk technicznych?

Rozprawa doktorska pana Michała Apolinarskiego stanowi kompendium wiedzy na temat współczesnych szyfrów blokowych projektowanych według różnych obowiązujących schematów. Oczywiście, nie omawia ona wszystkich znanych algorytmów, proponuje jednak ogólny schemat prezentacji szyfru zawierającego elementy charakteryzujące jego bezpieczeństwo. Według takiego schematu można prawdopodobnie przedstawić każdy szyfr blokowy, co ułatwia późniejszą analizę bezpieczeństwa i ewentualny wybór odpowiedniego rozwiązania w konkretnym zastosowaniu. Wartość praktyczna rozprawy to propozycja metody oceny algorytmów generowania kluczy rundowych umożliwiająca jej wykorzystanie jako elementu wspomagającego proces projektowania procedury generowania kluczy rundowych i kompletnych szyfrów, w szczególności znajdowania rozwiązania optymalnego.

Podsumowanie i ocena rozprawy

W swojej rozprawie doktorskiej pan magister inżynier Michał Apolinarski jasno sformułował i poprawnie zrealizował zagadnienie badawcze z zakresu bezpieczeństwa szyfrów blokowych, wykorzystując do tego celu nowoczesne metody matematyczne i obliczeniowe. Uzyskane przez niego rezultaty są nowe i oryginalne, przydatne zarówno w badaniach bezpieczeństwa szyfrów blokowych, jak również do optymalnego projektowania nowych algorytmów. Rozprawę doktorską pana magistra inżyniera Michała Apolinarskiego oceniam bardzo wysoko ze względu na poziom przeprowadzonych badań, jak też i ich bardzo duży zakres, zarówno teoretyczny, jak i doświadczalny. 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 dyscyplinie naukowej informatyka techniczna i telekomunikacja w dziedzinie nauk inżynieryjno-technicznych i wnioskuję o jej dopuszczenie do publicznej obrony.

Kotulski

Prof. dr hab. inż. Zbigniew Kotulski

UCHWAŁA NR 298

Senatu Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie z dnia 5 grudnia 2022 r.

w sprawie nadania mgr. inż. Michałowi Apolinarskiemu stopnia doktora

Na podstawie art. 179 ust. 2 i 3 pkt 2b ustawy z dnia 3 lipca 2018 r. Przepisy wprowadzające ustawę – Prawo o szkolnictwie wyższym i nauce (Dz. U. poz. 1669, z późn. zm.) w związku z art. 14 ust. 2 pkt 5 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (tekst jedn. Dz. U. z 2017 r. poz. 1789, z późn. zm.) uchwala się, co następuje:

§ 1.

Senat Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie nadaje mgr. inż. Michałowi Apolinarskiemu stopień doktora w dziedzinie nauk inżynieryjno-technicznych, w dyscyplinie informatyka techniczna i telekomunikacja.

§ 2.

Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Senatu
~~Rektor~~

dr hab. inż. Jacek Wróbel, prof. ZUT