dr hab. inż. Janusz Stokłosa
prof. Wyższej Szkoły Bankowej w Poznaniu

Poznań, 12 kwietnia 2021 r.

Recenzja rozprawy doktorskiej mgr. inż. Artura Janoski

pt. „**Zagadnienie doboru kodów w systemach szyfrowych typu McEliece'a w odniesieniu do bezpieczeństwa i efektywności**"

wykonana dla

Rady Dyscypliny Naukowej „Informatyka Techniczna i Telekomunikacja"
Wojskowej Akademii Technicznej

0. Recenzję rozprawy wykonałem na prośbę Przewodniczącego Rady, skierowaną do mnie w piśmie nr WYCH/N/00115/2021 z dn. 10.03.2021 r.

1. Komputery kwantowe – wszystko na to wskazuje, że w perspektywie około dwudziestu lat – będą w stanie łamać asymetryczne systemy kryptograficzne stosowane obecnie. Stanowiłoby to poważne naruszenie poufności i integralności danych przesyłanych, gromadzonych i przetwarzanych w systemach informatycznych. Celem kryptografii kwantowej (zwanej również kryptografią postkwantową) jest opracowanie systemów kryptograficznych odpornych na złamanie przy użyciu komputerów kwantowych o odpowiednio dużej mocy obliczeniowej, jak i klasycznych, a także takich kryptosystemów, które mogłyby być używane w istniejących protokołach i sieciach komunikacyjnych.

Istotne przyśpieszenie obliczeń za pomocą komputerów kwantowych może mieć wpływ na wymaganie większych rozmiarów kluczy w przypadku symetrycznych systemów kryptograficznych (np. AES, SHA-3). Natomiast w przypadku systemów asymetrycznych (zwanych też systemami klucza publicznego), takie algorytmy jak RSA, DSA czy algorytmy na krzywych eliptycznych, służące do wykonywania podpisów cyfrowych bądź do wymiany kluczy kryptograficznych, nie byłyby bezpieczne.

W związku z tym poszukiwania algorytmów uważanych za odporne na ataki zarówno z użyciem komputerów klasycznych, jak i kwantowych koncentrują się na algorytmach klucza publicznego. Aktualnie bierze się pod uwagę kilka obszarów poszukiwań, są wśród nich: teoria kodowania, funkcje skrótu, teoria krat, równania wielu zmiennych. Co do teorii kodowania, to pierwszym zaproponowanym kryptosystemem był system McEliece'a skonstruowany w oparciu o kody Goppy. Później opracowano inne systemy wykorzystujące kody korygujące błędy.

Systemy oparte na teorii kodowania wykorzystują losowy kod liniowy, dla którego istnieje efektywny algorytm dekodowania. Klucz prywatny umożliwia skuteczne dekodowanie; do słowa kodowego dodaje się wektor błędu w taki sposób, aby tylko posiadacz klucza prywatnego mógł poprawnie zdekodować wiadomość. Klucz publiczny jest wariantem wybranego kodu, niedającym możliwości efektywnego usunięcia błędu ze słowa kodowego. Wymaga się przy tym, aby kod użyty jako klucz publiczny był nierozróżnialny od losowego kodu liniowego. Ważną kwestią jest też taki dobór kodu, aby otrzymać klucz publiczny o jak najmniejszym rozmiarze.

W przypadku systemu McEliece'a klucz prywatny jest losowym binarnym niereduktorowanym kodem Goppy, a klucz publiczny – losową macierzą generatora losowo permutowanych wersji tego kodu. Szyfr jest słowem kodowym, do którego dodano błędy i tylko właściciel klucza prywatnego (kodu Goppy) może usunąć te błędy.

W przedłożonej mi do recenzji rozprawie doktorskiej mgr inż. Artur Janoska poświęcił szczególną uwagę kodom Goppy i kodom QC-MDPC. Autor sformułował tezę badawczą ujmując ją w trzech szczegółowych punktach:

(i) „Współczynnik sprawności R = 0,796812 kodu Goppy nadaje minimalny rozmiar klucza publicznego dla systemu McEliece'a".

(ii) „Algorytm dekodowania kodów QC-MDPC (używanych w systemie McEliece'a opartym na kodach QC-MDPC) powinien przyjmować jako parametr odcięcia liczbę #max – δ, gdzie #max oznacza maksymalny wskaźnik niezgodności dla poszczególnych bitów szyfrogramu oraz δ zmienia się od 5 do 7, w zależności od wybranego poziomu bezpieczeństwa (rozpatrywane są trzy poziomy bezpieczeństwa: 80, 128 i 256 bitów)".

(iii) „Mechanizmy asymetryczne oparte na kodach QC-MDPC bardzo dobrze nadają się do zastosowania w nowoczesnym środowisku teleinformatycznym, jakim jest sieć 5G".

2. Rozprawa zawiera streszczenia w języku polskim i angielskim, wstęp, trzy główne rozdziały, podsumowanie, wykaz literatury (84 pozycje, w tym 2 Autora rozprawy), a ponadto wykaz ważniejszych skrótów i oznaczeń, spis rysunków oraz spis tabel – razem 103 strony.

Rozdziałem 1 jest wstęp do rozprawy, w którym zarysowano problematykę badawczą, sformułowano tezę rozprawy, określono cel i zakres pracy oraz przedstawiono jej układ.

Rozdział 2 poświęcono omówieniu podstaw kryptografii asymetrycznej i teorii kodowania, a także kryptosystemów asymetrycznych opartych na teorii kodowania: kryptosystemowi McEliece'a oraz jego wersji dualnej (ekwiwalentnej) – systemowi Niederreitera. Dokonano także analizy bezpieczeństwa systemów opartych na teorii kodowania.

Kryptografia asymetryczna oparta na kodach Goppy jest przedmiotem rozważań zawartych w rozdziale 3 rozprawy. Autor definiuje kod Goppy i przedstawia algorytmy korekcji słów należących do kodów Goppy. Omawia systemy oparte na kodach Goppy, dokonuje oceny podatności tych systemów na ataki. Poświęca uwagę kwestii doboru kodu do systemu

McEliece'a ze względu na minimalizację rozmiaru klucza publicznego oraz maksymalizację bezpieczeństwa. Formułuje i udowadnia twierdzenia określające minimalny rozmiar klucza publicznego dla ustalonego poziom bezpieczeństwa dla systemu McEliece'a opartego na binarnym kodzie Goppy: twierdzenie o optymalnej sprawności kodu oraz twierdzenie o optymalnej liczbie błędów. Z udowodnionego twierdzenie o bezpieczeństwie asymptotycznym systemu McEliece'a opartego na kodzie Goppy wynika procedura wyznaczania parametrów kodu Goppy zapewniających optymalny rozmiar klucza dla określonego poziomu bezpieczeństwa w systemie McEliece'a. Algorytm wyznaczania parametrów kodu dla systemu McEliece'a umożliwia personalizowanie systemu McEliece'a poprzez dobór odpowiedniego kodu Goppy.

Rozdział 4 dotyczy kryptografii asymetrycznej opartej na kodach grafowych. Mgr Artur Janoska scharakteryzował kody LDPC i MDPC, opisał autorski sposób doboru parametru odcięcia dla algorytmów dekodowania kodów MDPC w zależności od rozmiaru rozpatrywanego kodu. Opisał schemat McEliece'a oparty na kodach QC-MDPC oraz wykonał ocenę podatności tego kryptosystemu na ataki. Zawarł opis sposobu doboru kodu do systemu McEliece'a opartego na kodzie QC-MDPC wraz z analizą różnych algorytmów dekodowania, w tym algorytmów z autorskimi modyfikacjami doboru parametru odcięcia dla kodów zapewniających różne poziomy bezpieczeństwa. W ramach prowadzonych badań zostały wykonane eksperymenty zmierzające do oceny wpływu algorytmów dekodowania na jakość systemu McEliece'a opartego na kodach QC-MDPC. Zaproponowana przez Autora metoda zwiększania wartości parametru δ dla wyższych poziomów bezpieczeństwa poprawia efektywność dekodowania. W końcowym fragmencie rozdziału 4 Autor dokonał – popartej eksperymentem – analizy możliwości wykorzystania badanych kryposystemów w sieci komórkowej 5G.

W rozdziale 5 podsumowano uzyskane w rozprawie wyniki, poddano je analizie krytycznej oraz wskazano kierunki dalszych badań.

3. Rozprawa ma charakter analityczno-eksperymentalny. Obszar badań został wybrany trafnie. Głównymi osiągnięciami Autora rozprawy są:

- sformułowanie i udowadnia twierdzenia 6 o optymalnej sprawności kodu,
- sformułowanie i udowadnia twierdzenie 7 o optymalnej liczbie błędów,
- sformułowanie i udowadnia twierdzenie 8 dotyczącego asymptotycznie optymalnych parametrów kodu dla systemu McEliece'a opartego na kodzie Goppy; wynika z niego procedura wyznaczania parametrów kodu Goppy zapewniających optymalny rozmiar klucza dla określonego poziomu bezpieczeństwa,
- algorytm 6 wyznaczania parametrów kodu dla systemu McEliece'a umożliwiający personalizowanie systemu McEliece'a poprzez dobór odpowiedniego kodu Goppy,
- ocena wpływu algorytmów dekodowania na jakość systemu McEliece'a opartego na kodach QC-MDPC.

Praca napisana jest językiem zrozumiałym i oszczędnym. Drobnych usterek redakcyjnych zauważyłem sporo.

4. Konkludując stwierdzam, że:
   - teza rozprawy została wykazana,
   - rozprawa stanowi oryginalne rozwiązanie problemu naukowego,
   - tematyka rozprawa jest aktualna i bardzo ważna,
   - Autor rozwiązał zdefiniowany przez siebie problem naukowy i użył do tego celu odpowiednich metod, tak więc wykazał się umiejętnością samodzielnego prowadzenia badań naukowych,
   - rozprawa świadczy o dużej wiedzy teoretycznej mgr. inż. Artura Janoski w zakresie informatyki, w szczególności w obszarze kryptografii.

Przedstawiona mi do recenzji dysertacja doktorska mgr. inż. Artura Janoski, mieszcząca się w dziedzinie nauki techniczne, w dyscyplinie naukowej informatyka, spełnia wymagania stawiane rozprawom doktorskim w obowiązujących przepisach prawa o szkolnictwie wyższym i nauce.

Wnoszę o dopuszczenie Autora rozprawy do jej publicznej obrony.