Warszawa, 7 lipca 2021 r.

dr hab. inż. Grzegorz Borowik, prof. Uniwersytetu SWPS
Katedra Informatyki
Wydział Projektowania
SWPS Uniwersytet Humanistycznospołeczny

Recenzja rozprawy doktorskiej pt. Zagadnienie doboru kodów w systemach szyfrowych typu McEliece'a w odniesieniu do bezpieczeństwa i efektywności

Autor rozprawy:
mgr inż. Artur Janoska

Promotor:
dr hab. inż. Andrzej Paszkiewicz, prof. WAT

Niniejsza recenzja została sporządzona na prośbę Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja w przedłożonym przez dra hab. inż. Zbigniewa Tarapatę, prof. WAT piśmie (uchwała 18/RDN ITiT/2021). Przewód doktorski prowadzony jest zgodnie z klasyfikacją dziedzin i dyscyplin naukowych w latach 2011–2018, tj. w dziedzinie nauk technicznych, w dyscyplinie Informatyka.

Mechanizmy ochrony komunikacji cyfrowej realizowane za pomocą specjalnych protokołów bezpieczeństwa wykorzystujących algorytmy kryptograficzne stały się niezbędnym elementem wielu rozwiązań. Eksplozja wzrostu usług internetowych w zakresie handlu i biznesu, w tym operacji finansowych i obrotu kapitałowego, powoduje, że realizacja mechanizmów zabezpieczenia przed nieuprawnionym dostępem do informacji jest ogromnym i aktualnym wyzwaniem. W szczególności, nowy trend w kryptografii postkwantowej stawia nowe wyzwania dla asymetrycznych systemów szyfrowych.

Motywacją do podjęcia prac przez Autora rozprawy jest możliwość skonstruowania w przyszłości komputera kwantowego, a tym samym obawa, że klasyczne systemy szyfrowania asymetrycznego mogą być w prosty sposób złamane i tym samym nie są bezpieczne. Celem pracy było przeprowadzenie badań podstawowych mających na celu: analizę możliwości zastosowania różnych kodów w systemie McEliece'a; dobór kodu do systemu asymetrycznego; modyfikację algorytmu dekodowania kodów MDPC. Przedstawione w recenzowanej rozprawie wyniki, przez ich potencjalne zastosowanie w praktyce, są ściśle związane z bezpieczeństwem informacji. Wyniki znajdują ważne zastosowania w kryptografii szyfrów asymetrycznych, w szczególności, jak pokazał Autor rozprawy, mają zastosowanie w nowej gałęzi kryptografii, jaką jest kryptografia postkwantowa oparta na teorii kodowania.

Przeprowadzone przez Autora studia literaturowe dotyczące algorytmów asymetrycznych opartych na teorii kodowania pozwoliły na sformułowanie następujących tez pracy:
- współczynnik sprawności R = 0,796812 kodu Goppy nadaje minimalny rozmiar klucza publicznego dla systemu McEliece'a;
- 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);

- mechanizmy asymetryczne oparte na kodach QC-MDPC bardzo dobrze nadają się do zastosowania w nowoczesnym środowisku teleinformatycznym, jakim jest sieć 5G.

Dwie pierwsze tezy rozprawy zostały sformułowane w sposób precyzyjny i jasny. Trzecia teza wskazuje na potencjalną możliwość praktycznego zastosowania i dyskusyjne jest czy stanowi tezę, którą można dowieść z punktu widzenia dyscypliny naukowej w której Autor przedkłada pracę. Uwzględniając powyższe wyrażam jednak przekonanie, że wybór tematu rozprawy doktorskiej mgr. inż. Artura Janoski uznać należy za perspektywiczny i ważny technicznie, a stopień trudności i zakres podjętego zadania, jego znaczenie naukowe oraz przydatność praktyczna odpowiadają ustawowym i zwyczajowo przyjętym kryteriom jakie zwykło się wiązać z rozprawą doktorską. Tematyka rozprawy doktorskiej mieści się w nurcie badań z zakresu kryptografii. Charakter rozprawy można uznać za teoretyczny, ukierunkowany w stronę praktycznych zastosowań.

Autor pracy wykazał dobre rozeznanie w literaturze przedmiotu. Wykaz literatury obejmuje 84 pozycje (są to pozycje z okresu 1962–2019, z czego większość to publikacje z ostatniego dziesięciolecia, ale zamieszczenie pozycji starszych jest jak najbardziej uzasadnione), w tym dwie pozycje autorskie mgr. inż. Artura Janoski (samodzielne). Wnioski z przeglądu stanu wiedzy oraz aktualnych badań w uznanych ośrodkach naukowych przedstawiono w sposób jasny i przekonujący. Autor w sposób właściwy odniósł się do dotychczasowego dorobku literaturowego i oceny stanu wiedzy w zakresie istotnych problemów zgodnych z tematyką pracy.

Doktorant w swojej rozprawie koncentruje się na kryptografii asymetrycznej opartej na teorii kodowania przez realizację badań związanych z systemem szyfrowania McEliece'a bazującym na kodach Goppy oraz kodach QC-MDPC. Są to systemy, które w prosty sposób przekładają się na mechanizmy enkapsulacji klucza. Usunięcie dodanego w czasie kodowania wektora błędu jest w ogólności problemem NP-trudnym, natomiast, wykorzystanie kodów Goppy sprowadza problem do problemu wielomianowego. Kolejną zaletą zastosowania zaproponowanego kryptosystemu McEliece'a jest, że wynik kodowania (tekstu jawnego) jest za każdym razem inny. Wynika to z użytej w algorytmie randomizacji, co w rezultacie sprawia, że szyfrogramy sprawiają wrażenie losowych. Podstawową zaś wadą rozważanej metody kryptografii asymetrycznej jest długość klucza publicznego, która rośnie pseudokwadratowo w porównaniu do długości klucza używanego w metodzie zabezpieczenia z wykorzystaniem klucza symetrycznego. Dodatkowo, problem rozróżnialności wymaga dedykowanego przygotowania systemu szyfrowania.

Oryginalnym osiągnięciem Autora pracy jest wskazanie optymalnej długości kodu, balansującego minimalną długość klucza publicznego oraz bezpieczeństwo w systemie szyfrowania McEliece'a. Korzystając z otrzymanej w heurystyczny sposób zależności Autor liczy sprawność kodu (stosunek wymiaru kodu do rozmiaru kodu) – przez znalezienie ograniczenia dolnego. Tym samym pokazuje, że aby system McEliece'a oparty na kodach Goppy miał optymalny rozmiar klucza dla danego parametru bezpieczeństwa, to sprawność użytego kodu w tym systemie powinna wynosić 0,796812. Chociaż w innych opublikowanych pracach pojawiły się już wyniki potwierdzające osiągnięcie Autora, to w tych pracach nie pokazano, w jaki sposób wartość ta została wyznaczona oraz w jaki sposób wykorzystać tę wartość do wyznaczania kodu, w szczególności dobierać parametry kodów używanych systemach asymetrycznych. Autor przedstawił w swojej pracy te elementy. Podejście Doktoranta pozwala w ten sposób przygotować system szyfrowania ze złożonością liniową. Opis wyników znajduje się w rozdziale 3.3: wyniki z literatury w tabeli 3.1, w tabeli 3.2 – wyniki własne (strona 61). Zaprezentowana procedura doboru parametrów kodu Goppy dla systemu McEliece'a została zaimplementowana z użyciem środowiska Mathematica (rozdział 3.3.2).

Drugim osiągnięciem Doktoranta jest modyfikacja algorytmu dekodowania kodów MDPC dla algorytmu BitFlipping oraz zastosowanie kodów prawie-cyklicznych do zmniejszenia ilości informacji w szyfratorze. Kody cykliczne umożliwiają operację generowania macierzy generującej. Wadą rozwiązania Autora jest narzucona struktura macierzy generującej. Autor zaproponował również sposób doboru parametru b w algorytmie BitFlipping, aby w sposób efektywny otrzymywać słowo kodowe dla kodów, których bezpieczeństwo szacuje się na 256 bitów klasycznego systemu symetrycznego. Inne analizowane przez Autora prace wskazują dużą nieefektywność już dla długości kodów około 128 bitów.

Autor pokazał również, że jego rozwiązania mogą w szczególności znaleźć zastosowanie w kanałach radiowych, w których zostały użyte zabezpieczenia kryptograficzne oparte na torii kodowania i gdzie występują dodatkowe błędy związane z przesyłaniem informacji: algorytm „One Round Bit Flipping" pozwala dekodować więcej błędów niż zostało oszacowanie w czasie definicji kodu. Recenzent zgadza się z tezą Autora pracy, że niezawodność kryptosystemów opartych na kodach QC-MDPC ma bardzo duże znaczenie pod kątem wykorzystania tych kodów w połączeniu z technologią 5G (New Radio). Biorąc pod uwagę, że istnieją systemy kryptograficzne oparte na kodach QC-MDPC (np. QC-MDPC-KEM, BIKE), które są bardzo zbliżone do kodów QC-LDPC, można założyć, że część z tych rozwiązań będzie prowadzić do obustronnych korzyści dla technologii 5G i kryptografii postkwantowej.

Wymienione elementy rozprawy stanowią samodzielny i oryginalny dorobek Autora.

Rozprawa stanowi spójną tematycznie całość. Następstwo rozdziałów i podrozdziałów oraz ich zawartość należy uznać za właściwe. Omawiane zagadnienia zostały uzupełnione przez algorytmy prezentowane w pseudokodzie. Zawartość poszczególnych rozdziałów i rozwój zawartych w nich myśli świadczy o dojrzałości naukowej Doktoranta oraz dobrym przygotowaniu do samodzielnego prowadzenia badań naukowych.

Słabymi stronami pracy i głównymi jej wadami są:
- w porównaniu do pierwszych dwóch tez rozprawy, trudno jest udowodnić tezę trzecią, która mówi o możliwym potencjalnym zastosowaniu opracowanych przez Autora rozwiązań;
- współczynnik sprawności osiągnięty przez Autora nie stanowi przełomu w dziedzinie kryptografii, ponieważ dostępna literatura światowa wskazuje tę wartość; osiągnięciem Autora jest heurystyczny sposób oszacowania tej wartości;
- Autor porównuje się jedynie do trzech wartości z literatury(strona 61); czy są to jedyne wartości dostępne w literaturze?; wykorzystując opracowany algorytm Autor mógłby przedstawić i omówić w pracy przykłady dla innych rozmiarów klucza;
- stylistyka pracy oraz sposób prezentacji literatury odbiega od przyjętego w tego typu pracach standardu: praca zawiera wiele błędów stylistycznych i redakcyjnych, które nie wpływają na jakość i wartość merytoryczną rozprawy; w szczególności błędy edytorskie widoczne są w pozycjach cytowanej literatury, gdzie bardzo często używana jest mała zamiast wielkiej litera; poprawienie stylistyki wielu zdań w pracy może znacznie wpłynąć na zrozumienie pracy.

Dodatkowo można wskazać:
- brak publikacji wyników badań w czasopiśmie o szerokim zasięgu;
- brak dobrego omówienia tablic z wynikami; warto uzupełnić omówienie wyników wskazując i omawiając np. pojedynczy wiersz z tablicy; według recenzenta pożądane byłoby wyjaśnienie co znajduje się w przykładowym wierszu tabeli wskazując czytelnikowi na wadę i zaletę omawianego przykładu;
- wady redakcyjne – praca zawiera czterostopniowe indeksowanie sekcji; przy tej wielkości dokumentu zaleca się indeksowanie dwustopniowe.

Rozprawę mgr. inż. Artura Janoski oceniam jako dobrą – spełniającą wymagania. Przeprowadzone przez Doktoranta prace mają charakter badań teoretycznych w dziedzinie kryptografii. Wyniki badań mogą znaleźć zastosowanie w zabezpieczeniu transmisji w sieciach o dużej przepustowości zbudowanych zgodnie ze standardem 5G. Autor rozprawy wykazał się wiedzą z zakresu zagadnień, które uczynił przedmiotem dociekań naukowych. Rozwiązał aktualne i ważne technicznie problemy naukowe, użyteczne praktycznie i wszystko wystarczająco udokumentował. Wykazał się przy tym inicjatywą twórczą, umiejętnościami rozwiązywania złożonych problemów, opanowaniem warsztatu badawczego i przygotowaniem do samodzielnego prowadzenia badań naukowych. Uważam, że przedstawiona do recenzji praca mgr. inż. Artura Janoski pt.: „Zagadnienie doboru kodów w systemach szyfrowych typu McEliece'a w odniesieniu do bezpieczeństwa i efektywności" spełnia wymagania postanowień aktualnie obowiązującej „Ustawy o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki". Dlatego wnoszę o przyjęcie recenzowanej pracy jako rozprawy doktorskiej i dopuszczenie jej Autora do dalszych etapów przewodu doktorskiego.