Streszczenie

Systemy asymetryczne oparte na teorii kodowania są jednymi z najstarszych i najbezpieczniejszych kryptosystemów. Jednak z faktu, że systemy te wykorzystują klucze o bardzo dużych rozmiarach, nie były one do tej pory rozważane jako alternatywa dla powszechnie wykorzystywanych systemów bazujących na problemach z teorii liczb. Sytuacja zmieniła się w momencie gdy okazało się, że systemy te są odporne na kryptoanalizę z użyciem komputera kwantowego. Intensyfikacja badań nad tą gałęzią kryptografii spowodowała pojawienie się nowych algorytmów oraz usystematyzowaniem zagadnień związanych z bezpieczeństwem tych systemów.

W rozprawie przedstawiono możliwościami doboru kodów Goppy oraz kodów MDPC do systemu asymetrycznego. Zaprezentowana została metoda doboru parametrów kodu Goppy do systemu McEliece'a w taki sposób, aby zapewnić najmniejszą długością klucza publicznego dla ustalonego bezpieczeństwa. W rozdziale czwartym pracy została wykonana analiza nowych systemów McEliece'a opartych na kodach QC-MDPC oraz przedstawiono ulepszoną metodę doboru parametrów dla algorytmu dekodowania tych kodów. Dodatkowo przeprowadzono analizę przydatności systemów kryptograficznych opartych na teorii kodowania w systemach z ograniczonymi zasobami sprzętowymi jak również w nowoczesnych środkach łączności, takich jakie będzie oferowała sieć 5G. Algorytmy postkwantowe oparte na teorii kodowania bardzo dobrze nadają się do wykorzystania w nowoczesnym środowisku telekomunikacyjnym, które umożliwia przesyłanie dużych ilości danych w krótkim czasie. Własność ta niweluje główną wadę systemów bazujących na teorii kodowania jaką jest duży rozmiar klucza publicznego.

Słowa kluczowe: *System McEliece'a, systemy asymetryczne oparte na teorii kodowania, kod Goppy, kod QC-MDPC, Algorytm Bit-Flipping, kryptografia postkwantowa, algorytmy ISD.*