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

Warszawa, 10 marca 2026 r.

RECENZJA ROZPRAWY DOKTORSKIEJ
DLA RADY DYSCYPLINY NAUKOWEJ
INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA
WOJSKOWEJ AKADEMII TECHNICZNEJ

Tytuł rozprawy: Synteza i optymalizacja kwantowych układów logicznych reprezentujących prymitywy kryptograficzne

Autor rozprawy: mgr inż. Adam Jagielski, doktorant Szkoły Doktorskiej

Niniejsza recenzja została przygotowana w odpowiedzi na pismo z dnia 12.12.2025 r. Przewodniczącego Rady Dyscypliny Informatyka Techniczna i Telekomunikacja WAT, dr. hab. inż. Zbigniewa Tarapaty, profesora WAT, realizującego uchwałę Rady Dyscypliny Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego nr 93/RDN ITiT/2025 z dnia 9 grudnia 2025 r. w sprawie wyznaczenia recenzentów rozprawy doktorskiej mgr. inż. Adama Jagielskiego doktoranta Szkoły Doktorskiej i uchwałę nr 94/RDN ITiT/2025 w sprawie powołania Komisji Doktorskiej mgr. inż. Adama Jagielskiego, doktoranta Szkoły Doktorskiej.

Omówienie rozprawy

Praca jest napisana w języku polskim i liczy 140 stron. Składa się z dziewięciu numerowanych rozdziałów poprzedzonych wykazem oznaczeń i wstępem, a zakończona jest podsumowaniem, bibliografią, spisem rysunków i spisem tabel. Bibliografia liczy 105 pozycji, w tym 2 prace autorstwa i 1 współautorstwa Doktoranta. Praca zawiera 31 rysunków oraz 56 tabel. Brakuje streszczenia rozprawy

w języku polskim i streszczenia w języku angielskim.

Promotorem rozprawy doktorskiej jest dr hab. Andrzej Paszkiewicz, a promotorem pomocniczym dr inż. Krzysztof Kanciak.

Wstęp (str. 7 - 12) zawiera motywację podjęcia tematyki badań, którą jest wykorzystania kwantowych układów logicznych w kryptografii, a także przegląd prac na podobne tematy podjętych w innych ośrodkach badawczych, sformułowanie celu pracy i zestawienie wyników uzyskanych w dalszych jej rozdziałach.

Rozdział 1 (str. 13 - 16) stanowi zestawienie podstawowych definicji i twierdzeń wykorzystywanych w rozprawie.

Rozdział 2 (str. 17 - 26) przedstawia dalsze informacje wstępne. Opisuje model obliczeń kwantowych, od definicji pojęcia qubitu i operacji na qubitach, poprzez przedstawienie pojęcia rejestru kwantowego i stanów splątanych, aż do wybranych działań na rejestrach kwantowych.

Rozdział 3 (str. 27 - 41) wprowadza pojęcie odwracalnych przekształceń logicznych a także przedstawia sposoby ich implementacji za pomocą odwracalnych bramek logicznych i odwracalnych układów logicznych. Określa też zestaw operacji logicznych przydatnych do realizacji szyfrów (ARX), realizowalnych w układach kwantowych. Przedstawia tez sposób realizacji permutacji Feistela za pomocą operacji z zestawu ARX. Celem końcowym tego rozdziału jest zdefiniowanie procesu optymalnej syntezy odwracalnych układów logicznych, co wymaga zdefiniowania metryk układu i zaproponowania struktur układów wykorzystujących qubity pomocnicze.

Rozdział 4 (str. 42 - 54) przedstawia kroki algorytmu Grovera rozwiązującego problem spełnialności dla funkcji boolowskich z wykorzystaniem kwantowego systemu obliczeniowego. Przedstawiono też w tym rozdziale model ataku na szyfr symetryczny wykorzystujący kwantową wyrocznię szyfrującą.

Rozdział 5 (str. 55 - 68) poświęcony jest implementacji skrzynek podstawieniowych za pomocą bramek MCT. Wprowadzono sposób kodowania układów odpowiedni do zapisu kwantowych układów logicznych, a następnie metodę przypisania układu kryptograficznego do układu logicznego. W części badawczej tego rozdziału przeprowadzono modelowanie wybranych skrzynek 3x3, 4x4 i 5x5, stosowanych w szyfrach znanych z konkursów kryptograficznych na nowe algorytmy (NIST

Lightweight Cryptopgraphy, NIST SHA, NESSIE) oraz optymalizację ich implementacji w układach bramek.

Rozdział 6 (str. 69 - 78) stanowi uogólnienie i rozwinięcie wyników badań z rozdziału 5. Przedstawia metody generowania szablonów identyczności dla funkcji odwracalnych pozwalających na rozmnażanie implementacji funkcji zaimplementowanych w układach bramek logicznych. Proponuje metody optymalizacji utworzonych rozwiązań z wykorzystaniem świadków suboptymalności. Przedstawia też wyniki badań eksperymentalnych dla szablonów rozmiaru 6x7 i świadków o rozmiarach 6x4,

Rozdział 7 (str. 79 - 99) poświęcony jest badaniu własności kryptograficznych optymalnych konstrukcji nieliniowych funkcji odwracalnych przedstawionych jako układy bramek MCT. Rozważono tu najbardziej popularne miary jakości stosowane zwykle przy opisie funkcji boolowskich i badaniu odporności szyfrów na analizę różnicowa i liniową. Precyzyjnie zdefiniowano te miary, przedstawiono ich własności i przeprowadzono badania układów zdefiniowanych w poprzednich rozdziałach obliczając dla nich odpowiednie wartości parametrów. Wnioskiem z badań jest zidentyfikowanie pozytywnej korelacji między rozważanymi parametrami bezpieczeństwa skrzynek podstawieniowych a optymalnym rozmiarem ich implementacji jako układów bramek MCT.

Kolejne dwa rozdziały poświęcone są badaniu kosztu implementacji wyroczni kwantowych realizujących funkcje szyfrujące w celu oszacowania skuteczności ataków.

Rozdział 8 (str. 100 - 114) poświęcony jest rodzinie szyfrów SPARKLE opartych na konstrukcji gąbki. Skonstruowano w nim algorytm Grovera z wyrocznią szyfrującą do ataku ze znanym tekstem jawnym. Przebadano koszt układu szyfrującego dla czterech wersji szyfru o różnych długościach klucza i różnych długościach tagu uwierzytelniającego. Oszacowano również koszt ataku na takie szyfry.

Rozdział 9 (str. 115 - 123) również analizuje szyfr postaci gąbki, tym razem ASCON. Rozważono dwie wersje szyfru o różnych rozmiarach bloku danych. Podobnie jak w rozdziale 8, skonstruowano układ szyfrujący oraz oszacowano koszt układu i koszt ataku.

Podsumowanie (str. 124 - 126) to omówienie w punktach przeprowadzonych pięciu

głównych zadań badawczych zrealizowanych w rozprawie, propozycje dalszych kierunków badań i wizja praktycznego wykorzystania wyników pracy.

Struktura pracy jest bardzo przejrzysta. Rozdziały wstępne (1-3) wprowadzają niezbędne definicje i twierdzenia. Rozdział 4 stanowi łącznik między wiedzą literaturową a badaniami własnymi, natomiast kolejne rozdziały to już w dominującym zakresie wyniki własnych badań Doktoranta. Praca posiada wszystkie niezbędne elementy formalne (poza streszczeniami), to znaczy wykazy oznaczeń, tabel i rysunków, co ułatwia jej czytanie.

Ocena 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)?

Celem pracy jest zbadanie możliwości realizacji symetrycznych algorytmów kryptograficznych w układach kwantowych bramek logicznych oraz konstrukcji ataków na takie algorytmy. W ramach badań przeprowadzono syntezę optymalnych układów logiki odwracalnej reprezentujących wybrane skrzynki podstawieniowe i syntezę szablonów identyczności. Zbadano korelację między parametrami bezpieczeństwa skrzynek podstawieniowych i optymalnym rozmiarem ich implementacji w kwantowej logice odwracalnej. Zbadano też bezpieczeństwo kwantowe szyfrów SPARKLE i ASCON.

W rozprawie nie sformułowano tradycyjnej tezy, która następnie w trakcie badań miałaby być wykazana. Zamiast tego sformułowano powyższe zadania badawcze, które następnie z sukcesem zrealizowano. Są to zarówno propozycje algorytmów i metod ich optymalizacji, jak również obliczenia numeryczne potwierdzające skuteczność ich działania oraz znajdujące korelację między parametrami jakościowymi algorytmów i sposobem ich implementacji. Jak z tego zakresu przeprowadzonych prac wynika, praca ma charakter teoretyczno-doświadczalny.

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?

Bibliografia rozprawy jest obszerna, liczy 105 pozycji, w tym 2 prace autorstwa i 1 współautorstwa Doktoranta. Dobór publikacji wynika ze sposobu prezentacji rezultatów pracy. W zakresie obliczeń kwantowych i podstaw kryptografii cytowane są prace ściśle związane z tokiem rozumowania i prowadzonego wywodu. Nie ma tu szerokiego omówienia obu tych dziedzin, co jest zrozumiałe ze względu na ich rozmiar i różnorodność tków tematycznych. Każdy z tych tematów to temat na obszerną monografię. Licznie cytowane są specyfikacje algorytmów analizowanych i wymienianych w rozprawie, ze wskazaniem oryginalnych źródeł w repozytoriach organizacji standaryzacyjnych (głównie NIST). W wykazie literatury brakuje wskazania numerów DOI, co dzisiaj jest powszechnie wymagane, lub też odnośników url do repozytoriów udostępniających artykuły lub standardy. Podsumowując, bibliografia jest kompetentnie dobrana i właściwie wykorzystana w tekście rozprawy doktorskiej.

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

Zakres prac przewidziany do realizacji został przedstawiony w punktach we Wprowadzeniu. W celu ich realizacji najpierw przedstawiono podstawy teoretyczne: definicje i twierdzenia, a następnie przeprowadzono kroki umożliwiające ich realizację. Przedstawione analizy teoretyczne i implementacje komputerowe dowodzące hipotez poszczególnych zadań. Taki sposób przeprowadzenia badań jest skuteczny i właściwy. Pozwala na sprawdzenie poprawności poszczególnych kroków i weryfikację wyników końcowych.

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?

Początkowe cztery rozdziały rozprawy stanowią oryginalne i wartościowe wprowadzenia do tematyki konstruowania optymalnych kwantowych logicznych układów obliczeniowych i podstaw teoretycznych ich wykorzystania do kryptanalizy algorytmów symetrycznych. Kolejne pięć rozdziałów to już w pełni oryginalne i nowe wyniki badawcze uzyskane przez Doktoranta. Przedstawiają one skonstruowane przez

Autora optymalne implementacje przykładowych skrzynek podstawieniowych wyrażonych jako układy logiki kwantowej i odwracalnej (rozdział 5). Zaimplementowano te skrzynki i znaleziono ich optymalne reprezentacje w układach bramek. Dotyczy to w szczególności skrzynek szyfru ASCON. W kolejnym rozdziale (rozdział 6) znaleziono kompletną przestrzeń szablonów identyczności oraz przedstawiono reguły podstawień służących do optymalizacji układów logiki kwantowej i odwracalnej. W rozdziale 7 wykazano istnienie korelacji między znanymi z literatury i powszechnie używanymi parametrami charakteryzującymi poziom bezpieczeństwa skrzynek podstawieniowych i optymalnymi rozmiarami implementacji skrzynek zrealizowanych w logice kwantowej. W rozdziałach 8 i 9 przeprowadzono pełną analizę oceny bezpieczeństwa kwantowego szyfrów z rodziny SPARKLE oraz szyfru ASCON, nowych algorytmów skonstruowanych w układzie gąbki (sponge).

Znaczna część wyników uzyskanych w doktoracie została opublikowana w trzech artykułach Doktoranta. Jeden z nich, „GROVER ON SPARKLE. QUANTUM RESOURCE ESTIMATION FOR A NIST LWC CALL FINALIST", Quantum Information and Computation, Vol. 22, No. 13&14 (2022) 1132–1143 (wspólny z dr. K. Kanciakiem) był sześciokrotnie cytowany w specjalistycznych artykułach z dobrych czasopism. Można zatem stwierdzić, że wyniki uzyskane w ramach pracy doktorskiej weszły do światowego obiegu informacji naukowej.

Jakie są słabe strony rozprawy i jej główne wady?

Praca przedstawia pewien określony zaplanowany zakres badań, który został jasno sformułowany i w pełni zrealizowany. Wskazano też w pracy kierunki przyszłych badań rozwijających analizowane już w rozprawie problemy i metody. Zadania te zostały zrealizowane bez zastrzeżeń, zatem trudno tu mówić o słabych stronach rozprawy. To, na co chciałbym zwrócić uwagę, to szersza perspektywa badań związanych z bezpieczeństwem kwantowym i atakami kwantowymi. Mam w związku z tym dwa pytania.

1. Co można powiedzieć o kwantowym bezpieczeństwie innych klas algorytmów symetrycznych poza struktura gąbki, np. prostych sieci S-P, permutacji Feistela/rozszerzonych struktur tego typu, ortogonalnych kwadratów łacińskich, itd.?

2. Jaki jest rzeczywisty aktualny poziom bezpieczeństwa algorytmów symetrycznych w sytuacji, gdy można przeprowadzać ataki takie, jak zademonstrowane recenzowanej rozprawie? (możliwość realnego skonstruowania układów kwantowych do przeprowadzenia ataku)

Uwagi redakcyjne:

- w rozprawie brak jest streszczenia w języku polskim i w języku angielskim;
- kilkukrotnie użyto niepoprawnej formy językowej w znaczeniu przenośnym „oparty o" zamiast poprawnej „oparty na": str. 9, 10 (dwukrotnie), 18, 42, 83, 116;
- w wydawnictwach naukowych opisy tabel umieszczane są zwykle nad tabelami, a opisy rysunków pod rysunkami. Wynika to z tego, ze tabela może zajmować więcej niż jedną stronę. W tej rozprawie opisy tabel są umieszczone pod tabelami;
- po niektórych wzorach brakuje przecinków lub kropek: 1.8, 1.9, 1.10, 2.1. 2.2, 2.3, 2.4, 2.5, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.14, 2.15, 2.17, 2.18, 2.19, 2.20, 2.22, 3.3, 3.6, 3.7, 3.12, 3.13, 3.14, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.14, 4.18, 4.19, 4.20, 4.22, 4.23, 4.24, 4.25, 4.26, 4.27, 4.30, 4.32, 4.33, 4.34, 4.35, 4.36, 4.37, 4.38, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.2, 6.3, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10, 7.11, 8.1, 8.2, 8.3;
- str. 28: niepełne zdanie opisujące wzór 3.5;
- str. 30: niepełne zdanie opisujące wzór 3.8;
- str. 31: kropka zamiast przecinka w środku zdania opisującego wzór 3.11;
- str. 35 brak znaku przestankowego kończącego wypunktowanie po wzorze;
- str. 48: brak znaku przestankowego w zdaniu zawierającym wzór 4.21;
- str. 51 niepełne zdanie opisujące wzór 4.31;
- str. 71 niepełne zdanie opisujące wzór 6.1;
- str. 72 niepełne zdanie opisujące wzór 6.4;
- str. 84 brak kropki po wzorze bez numeru;
- str. 85, 86 (dwa razy) brak znaków przestankowych w wypunktowaniu;
- str. 102 wypunktowanie kończy się średnikiem zamiast kropką.

Jaka jest przydatność rozprawy dla nauk technicznych?

Recenzowana rozprawa doktorska dotyczy tematyki bardzo aktualnej i szeroko analizowanej zarówno przez naukowców, jak i kryptanalityków praktycznie łamiącym zabezpieczenia. Zagadnieniem już rozwiązanym teoretycznie a praktycznie zmierzającym do efektywnej implementacji jest złamanie klasycznych algorytmów asymetrycznych, tzn. takich, gdzie bezpieczeństwo oparte jest na trudności faktoryzacji lub problemie logarytmu dyskretnego. Autor tej rozprawy podjął próbę kryptanalizy algorytmów symetrycznych. W tym obszarze bezpieczeństwa nie słychać o skutecznych implementacjach ataków. Dlatego też wszelkie badania tego obszaru kryptografii są niezwykle ważne praktycznie, aby móc oszacować potencjalne zagrożenia dla szyfrów symetrycznych, a także proponowanych oraz oczekiwanych rozwiązań postkwantowych.

Podsumowanie i ocena końcowa rozprawy

W swojej rozprawie doktorskiej pan magister inżynier Adam Jagielski jasno sformułował i poprawnie zrealizował zagadnienie badawcze z zakresu rozwoju współczesnych metod kryptanalizy algorytmów symetrycznych z wykorzystaniem kwantowych układów logicznych. Uzyskane przez Doktoranta rezultaty teoretyczne i wyniki eksperymentów są nowe i oryginalne i mogą stanowić podstawę dalszych badań o bardzo dużym potencjale poznawczym i aplikacyjnym.

Rozprawę doktorską pana magistra inżyniera Adama Jagielskiego oceniam bardzo wysoko. Uważam, że uzyskane w niej wyniki badawcze spełniają wymagania określone w art. 187 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. 2018 poz. 1668, tekst ujednolicony) rozprawom doktorskim w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie naukowej: informatyka techniczna i telekomunikacja i wnioskuję o jej dopuszczenie do publicznej obrony.

Zbigniew Kotulski

Prof. dr hab. inż. Zbigniew Kotulski