prof. dr hab. Zbigniew Puchała
Instytut Informatyki
Teoretycznej i Stosowanej PAN
ul. Bałtycka 5, 44-100 Gliwice

Gliwice, 31 marca 2026 r.

Recenzja rozprawy doktorskiej mgra inż. Adama Jagielskiego pt.: „*Synteza i optymalizacja kwantowych układów logicznych reprezentujących prymitywy kryptograficzne*”

Uwagi wstępne

Forma drukowana recenzowanej rozprawy obejmuje 141 stron. Praca jest napisana w języku polskim i zawiera wprowadzenie, dziewięć rozdziałów merytorycznych, podsumowanie, wykaz oznaczeń oraz bibliografię liczącą 105 pozycji.

Tytuł pracy trafnie oddaje jej zawartość i zakres badawczy. Układ rozprawy jest logiczny oraz przejrzysty: rozdziały 1–4 tworzą część pojęciową i metodyczną, natomiast rozdziały 5–9 zawierają zasadnicze wyniki własne Autora. Taka kompozycja dobrze porządkuje materiał, prowadząc czytelnika od podstaw modelu obliczeń kwantowych i logiki odwracalnej do autorskich metod syntezy oraz ich zastosowań w analizie bezpieczeństwa kryptograficznego.

Praca zawiera wyniki opublikowane wcześniej przez Autora w formie artykułów naukowych:

1. A. Jagielski, *Optimal SAT Solver Synthesis of Quantum Circuits Representing Cryptographic Nonlinear Functions*, *International Journal of Electronics and Telecommunications*, 69, 261–267, 2023.

2. A. Jagielski, *Complete synthesis of identity templates for quantum and reversible logic MCT circuits using SAT-solvers and proposal of suboptimality witness notion*, *International Journal of Electronics and Telecommunications*, 70(3), 727–732, 2024.

3. A. Jagielski, K. Kanciak, *Grover on sparkle quantum resource estimation for a NIST LWC call finalist*, *Quantum Information and Computation*, 22, 1132–1143, 2022.

Z podsumowania rozprawy wynika ponadto, że wyniki badań z rozdziałów 7 i 9 zostały zgłoszone do publikacji.

Przedmiot rozprawy

Przedmiotem rozprawy jest synteza i optymalizacja odwracalnych oraz kwantowych układów logicznych reprezentujących prymitywy kryptograficzne, a następnie wykorzystanie tych układów do ilościowej oceny bezpieczeństwa wybranych szyfrów symetrycznych w modelu ataków kwantowych opartych o algorytm Grovera. Jest to tematyka aktualna i ambitna badawczo, położona na styku obliczeń kwantowych, logiki odwracalnej, metod formalnych oraz kryptologii symetrycznej.
Wprowadzenie oraz rozdział 1 (*Pojęcia podstawowe*). Autor szeroko uzasadnia wagę problemu, osadzając go w kontekście kryptografii lekkiej, konkursów standaryzacyjnych NIST oraz rosnącego znaczenia analiz bezpieczeństwa postkwantowego. W rozdziale pierwszym wprowadza aparat pojęciowy z zakresu algebry Boole'a, funkcji boolowskich i odwracalnych, niezbędny do dalszych rozważań.
Rozdział 2 (*Model obliczeń kwantowych*). Rozdział ten porządkuje podstawowe pojęcia dotyczące qubitów, rejestrów kwantowych, pomiaru i operacji kwantowych. Jego rola jest przygotowawcza, ale potrzebna, ponieważ pozwala na spójne przejście od klasycznej logiki odwracalnej do modelu układów kwantowych.
Rozdział 3 (*Logika kwantowa i odwracalna*). Autor omawia funkcje odwracalne, rodziny bramek NCT i MCT, układy odwracalne, operacje ARX, metryki układu, qubity pomocnicze oraz metody syntezy i optymalizacji. Rozdział stanowi solidne zaplecze teoretyczne dla wyników własnych z dalszej części pracy.
Rozdział 4 (*Algorytm Grovera*). Przedstawiono mechanizm działania algorytmu Grovera, jego optymalność oraz model ataku na szyfr symetryczny ze znanym tekstem jawnym. Cennym elementem tego rozdziału jest sformułowanie warunku unikalności rozwiązania oraz oszacowanie minimalnej liczby bloków wiadomości koniecznych do przeprowadzenia ataku, z uwzględnieniem przypadku szyfrów AEAD i wykorzystania tagu uwierzytelniającego.
Rozdział 5 (*Optymalne układy implementujące skrzynki podstawieniowe*). Jest to pierwszy rozdział zawierający zasadnicze wyniki własne. Autor proponuje kodowanie problemu syntezy układu jako problemu SAT, a następnie stosuje je do wyznaczania optymalnych implementacji skrzynek podstawieniowych i innych funkcji nieliniowych wybranych prymitywów kryptograficznych. Na szczególne uznanie zasługuje systematyczne przebadanie funkcji o rozmiarach 3×3, 4×4

i 5×5, dla różnych wariantów zbioru bramek i liczby bitów pomocniczych. Autor uzyskuje optymalne implementacje dla szeregu funkcji, natomiast dla skrzynki Ascon nie uzyskuje jeszcze pełnego dowodu optymalności, lecz wyznacza istotny poznawczo przedział 13–17 bramek dla rozmiaru implementacji. Dodatkowo przedstawia heurystyczną transpilację uzyskanych układów do zestawu Clifford+T.

Rozdział 6 (*Synteza szablonów identyczności*). Autor rozwija metodykę z rozdziału 5 i proponuje kompletną syntezę szablonów identyczności. Istotnym wkładem jest nie tylko sam algorytm, lecz także wykorzystanie symetrii szablonów poprzez odbicie, permutację linii, rotację i zamianę niezależnych bramek. Pozwala to istotnie skrócić czas syntezy; zaprezentowane przyspieszenia sięgają od około $\times 15$ do ponad $\times 635$. Drugim oryginalnym elementem tego rozdziału jest pojęcie świadka suboptymalności. W rezultacie Autor wyznacza kompletną przestrzeń unikalnych szablonów identyczności do rozmiaru 6×7 oraz kompletną przestrzeń unikalnych świadków suboptymalności do rozmiaru 6×4.

Rozdział 7 (*Korelacja właściwości kryptograficznych*). W mojej ocenie jest to jeden z najciekawszych fragmentów rozprawy. Autor bada związek pomiędzy klasycznymi właściwościami kryptograficznymi skrzynek podstawieniowych a rozmiarem ich optymalnej implementacji jako układu MCT. Analiza ma charakter wyczerpujący dla pełnych przestrzeni skrzynek 3×3 i 4×4 i obejmuje takie miary, jak stopień algebraiczny, nieliniowość, SAC, DDT oraz LAT. Szczególnie cenne jest tu połączenie przeglądu pełnej przestrzeni funkcji z wydajną implementacją BFS oraz szeregiem optymalizacji obliczeniowych. Uzyskany wniosek o dodatniej korelacji pomiędzy jakością kryptograficzną a rozmiarem optymalnej implementacji ma charakter nowy i jest bardzo dobrze udokumentowany właśnie na tym materiale badawczym; rozprawa nie przedstawia go natomiast jako zamkniętego twierdzenia ogólnego dla większych rozmiarów skrzynek.

Rozdział 8 (*Atak na szyfr SPARKLE*). Autor konstruuje odwracalny układ realizujący funkcję szyfrującą rodziny SPARKLE i przeprowadza szczegółowe szacunki kosztu ataku Grovera dla czterech wariantów szyfru: SCHWAEMM128-128, SCHWAEMM192-192, SCHWAEMM256-128 oraz SCHWAEMM256-256. Wyniki mają postać precyzyjnych oszacowań zasobów logicznych dla skonstruowanej wyroczni, wyrażonych liczbą bramek, szerokością układu, liczbą qubitów pomocniczych oraz głębokością. Rozdział ma znaczenie praktyczne, ponieważ dostarcza dobrze uargumentowanych górnych ograniczeń wynikających z przedstawionej konstrukcji wyroczni dla finalisty konkursu NIST LWC.

Rozdział 9 (*Atak na szyfr Ascon*). Autor wykonuje analogiczną analizę dla szyfru Ascon, zwycięzcy konkursu NIST LWC. Rozdział wykorzystuje wyniki z wcześniejszych części pracy, w szczególności implementację warstwy nieliniowej Ascon i model ataku z rozdziału 4. Również tutaj otrzymujemy precyzyjne oszacowania zasobów logicznych oraz szacunki kosztu w modelu logicznym dla warian-

tów Ascon-128 oraz Ascon-128a, które należy interpretować jako górne ograniczenia wynikające z przedstawionej konstrukcji wyroczni, a nie jako finalne koszty implementacyjne fault-tolerant.
Podsumowanie. Końcowa część pracy syntetyzuje pięć głównych badań przeprowadzonych przez Autora, wskazuje ich praktyczne znaczenie oraz sensownie wytycza dalsze kierunki rozwoju. Całość tworzy spójny program badawczy, w którym wyniki metodologiczne są bezpośrednio wykorzystywane w analizach aplikacyjnych.

Uwagi techniczne niewpływające na ocenę merytoryczną

1. W pracy występują drobne usterki redakcyjne i językowe, w tym sporadyczne literówki oraz niezręczne stylistycznie sformułowania. Nie wpływa to na odbiór zasadniczej treści, ale przy ostatecznej redakcji publikacyjnej warto byłoby przeprowadzić jeszcze jedną staranną korektę.

2. Zapis terminologii nie jest wszędzie całkowicie jednolity. Dotyczy to zwłaszcza równoległego używania terminów polskich i angielskich oraz skrótów bez pełnego ujednolicenia stylu.

3. Część tabel, szczególnie w rozdziałach 8 i 9, jest bardzo bogata informacyjnie. Dodatkowe krótkie komentarze interpretacyjne bezpośrednio po tabelach ułatwiłyby czytelnikowi szybsze uchwycenie najważniejszych zależności między wariantami szyfrów.

4. W kilku miejscach syntetyczne opisy wyników są sformułowane mocniej niż szczegółowe ustalenia przedstawione później w tekście. Dotyczy to zwłaszcza trzech typów sytuacji: po pierwsze, przypadku skrzynki Ascon z rozdziału 5, gdzie uzyskano cenne zawężenie do przedziału 13–17 bramek, ale nie pełny dowód optymalności; po drugie, rozdziału 7, gdzie dodatnia korelacja została bardzo dobrze udokumentowana dla pełnych przestrzeni skrzynek 3×3 i 4×4, lecz nie ma jeszcze charakteru twierdzenia ogólnego dla większych rozmiarów; po trzecie, rozdziałów 8 i 9, gdzie podane koszty należy rozumieć jako oszacowania zasobów logicznych dla skonstruowanych wyroczni, a nie jako końcowe koszty realizacji fault-tolerant. Uwaga ta ma charakter redakcyjno-porządkujący i nie obniża mojej oceny wartości pracy.

Uwagi dyskusyjne

1. W rozdziale 5 dla skrzynki podstawieniowej Ascon Autor uzyskuje bardzo wartościowy wynik w postaci zawężenia rozmiaru implementacji do przedziału 13–17 bramek, pozostaje jednak luka pomiędzy dolnym i górnym ograniczeniem. Podczas obrony warto doprecyzować, jakie bariery obliczeniowe lub modelowe uniemożliwiły domknięcie dowodu optymalności i które kierunki badawcze dają największą szansę na pełne rozstrzygnięcie tego przypadku.

2. Rozdziały 8 i 9 dostarczają starannych oszacowań kosztów ataków w modelu logicznym, tj. w liczbie bramek, szerokości układu, liczbie qubitów pomocniczych i głębokości. Byłoby jednak pożądane jeszcze wyraźniejsze odróżnienie tych metryk logicznych od metryk implementacyjnych właściwych modelowi fault-tolerant, zwłaszcza kosztu operacji T, T-depth czy narzutu związanego z korekcją błędów.

3. Wynik z rozdziału 7, wskazujący na dodatnią korelację pomiędzy klasycznymi właściwościami kryptograficznymi a rozmiarem optymalnej implementacji, jest przekonujący dla pełnych przestrzeni skrzynek 3×3 i 4×4. Z ostrożności metodologicznej przejście od tych dwóch pełnych przestrzeni do większych skrzynek, np. 8×8, powinno być jednak traktowane jako dobrze umotywowana hipoteza badawcza, a nie jeszcze jako twierdzenie o charakterze ogólnym.

4. Model ataku oparty o algorytm Grovera zakłada możliwość zapewnienia unikalności rozwiązania poprzez odpowiednią liczbę bloków znanego tekstu jawnego i ewentualne wykorzystanie tagu uwierzytelniającego. Podczas obrony warto byłoby szerzej omówić wrażliwość uzyskanych oszacowań na założenia o unikalności rozwiązania i dostępności danych, w tym na mniej korzystne sytuacje operacyjne, np. ograniczoną liczbę bloków lub obecność dodatkowych kolizji.

Ocena merytoryczna rozprawy

Rozprawa podejmuje aktualny i ważny problem badawczy. Rozwój technologii kwantowych powoduje, że ocena bezpieczeństwa kryptografii symetrycznej z uwzględnieniem rzeczywistych kosztów implementacji kwantowych staje się zagadnieniem istotnym nie tylko teoretycznie, ale także z punktu widzenia praktyki projektowania i standaryzacji algorytmów kryptograficznych. Autor trafnie identyfikuje niszę badawczą: zamiast ograniczać się do ogólnych stwierdzeń o kwadratowym przyspieszeniu Grovera, przechodzi do szczegółowej analizy zasobów

logicznych, której podstawą jest formalna synteza układów odwracalnych.

Za najważniejszą zaletę rozprawy uważam jej metodologiczną dojrzałość. Autor nie poprzestaje na pojedynczym wyniku, lecz buduje spójny ciąg narzędzi: od formalizacji problemu syntezy jako problemu SAT, poprzez kompletną syntezę szablonów identyczności i wprowadzenie świadków suboptymalności, aż po analizę korelacji właściwości kryptograficznych i końcowo po oszacowania kosztów ataków na konkretne szyfry. Taki układ świadczy o samodzielności badawczej i umiejętności prowadzenia programu naukowego, w którym wyniki jednego etapu stają się narzędziem kolejnego.

Na szczególne podkreślenie zasługuje fakt, że znaczna część rezultatów ma charakter wyczerpujący i deterministyczny, a nie heurystyczny. Dotyczy to zarówno wyznaczania optymalnych układów dla wielu funkcji nieliniowych, jak i kompletnej przestrzeni szablonów identyczności do rozmiaru 6×7 oraz pełnej analizy przestrzeni skrzynek 3×3 i 4×4. W dziedzinie, w której często dominują przybliżenia, próbki losowe albo wyniki czysto konstruktywne bez dowodów optymalności, jest to walor bardzo istotny.

Wysoko oceniam także rozdział 7. Samo postawienie pytania o zależność między klasycznymi miarami bezpieczeństwa a kosztem optymalnej implementacji odwracalnej jest pomysłem oryginalnym i twórczym. Jeszcze ważniejsze jest to, że Autor nie ogranicza się do intuicji, lecz bada pełne przestrzenie odpowiednich funkcji dla skrzynek 3×3 i 4×4 oraz uzyskuje wnioski o wyraźnej wartości poznawczej. Dodatnia korelacja została dzięki temu wyczerpująco zbadana i bardzo dobrze udokumentowana właśnie dla tego materiału badawczego. Wynik ten może mieć znaczenie nie tylko dla analizy istniejących szyfrów, ale także dla projektowania nowych skrzynek podstawieniowych z uwzględnieniem kryteriów bezpieczeństwa kwantowego.

Rozdziały 8 i 9 mają z kolei wyraźny walor aplikacyjny. Autor konstruuje kompletne wyrocznie szyfrujące dla rodzin SPARKLE i Ascon oraz przedstawia szczegółowe szacunki zasobów logicznych potrzebnych do przeprowadzenia ataku Grovera. Sam Autor uczciwie wskazuje przy tym, że chodzi o górne ograniczenia wynikające z przedstawionej konstrukcji wyroczni oraz z niepełnej wiedzy o optymalności niektórych podukładów, a nie o finalne koszty implementacyjne w modelu fault-tolerant. Nie obniża to wartości tych wyników; przeciwnie, świadczy o dojrzałym i ostrożnym sposobie interpretacji własnych rezultatów.

Do mocnych stron pracy należy zaliczyć:

- trafny wybór ważnego i nowoczesnego problemu badawczego,
- umiejętne połączenie metod formalnych, algorytmiki, obliczeń równoległych i analizy kryptologicznej,
- uzyskanie kilku samodzielnych i oryginalnych wyników o różnym charakterze:

metodologicznym, teoretycznym i aplikacyjnym,

- dbałość o odtwarzalność procedur badawczych oraz ilościowy charakter analiz,

- wejście części wyników do obiegu naukowego, o czym świadczą publikacje oraz cytowanie wyniku dotyczącego SPARKLE w raporcie NIST.

Pewien niedosyt pozostawia przede wszystkim to, że nie wszystkie elementy udało się domknąć formalnie do poziomu pełnej optymalności, a wnioski o korelacji dotyczą na razie pełnych przestrzeni skrzynek małych rozmiarów, tj. 3×3 i 4×4. Są to jednak w mojej ocenie naturalne ograniczenia ambitnego programu badawczego, a nie słabości podważające wartość rozprawy. Autor wyraźnie je identyfikuje i uczciwie opisuje, co dodatkowo wzmacnia wiarygodność pracy.

Ocena końcowa i wnioski

Rozprawa doktorska mgr inż. Adama Jagielskiego pt.: „*Synteza i optymalizacja kwantowych układów logicznych reprezentujących prymitywy kryptograficzne*" stanowi wartościowe i oryginalne osiągnięcie naukowe Autora. Praca dotyczy istotnego problemu z obszaru informatyki kwantowej i kryptologii, a jej wyniki wnoszą nową wiedzę zarówno do metod syntezy układów odwracalnych, jak i do ilościowej oceny bezpieczeństwa prymitywów kryptografii symetrycznej wobec ataków kwantowych.

Autor do rozwiązania postawionych problemów wykorzystał właściwe i nowoczesne metody badawcze, łącząc narzędzia logiki odwracalnej, formalizacji SAT, obliczeń równoległych, analizy algorytmicznej i kryptologii. Na szczególne podkreślenie zasługuje konsekwentne połączenie rozważań metodologicznych z analizą pełnych przestrzeni badanych obiektów oraz z praktycznymi zastosowaniami do rzeczywistych szyfrów.

Oryginalnymi osiągnięciami badawczymi Autora są:

- opracowanie i zastosowanie formalnej metody syntezy SAT do wyznaczania optymalnych implementacji funkcji nieliniowych używanych w prymitywach kryptograficznych,

- wyznaczenie kompletnej przestrzeni szablonów identyczności do rozmiaru 6×7 oraz wprowadzenie pojęcia świadków suboptymalności,

- sformułowanie problemu korelacji pomiędzy klasycznymi właściwościami kryptograficznymi skrzynek podstawieniowych a rozmiarem ich optymalnej implementacji oraz jego wyczerpujące zbadanie na pełnych przestrzeniach skrzynek 3×3 i 4×4,

- opracowanie szczegółowych oszacowań zasobów logicznych ataków Grovera na szyfry z rodzin SPARKLE i Ascon.

Jest to istotny wkład mgr inż. Adama Jagielskiego w rozwój dyscypliny naukowej informatyka techniczna i telekomunikacja, w szczególności w obszarze obliczeń kwantowych, logiki odwracalnej i kryptologii. Rozległość przeprowadzonej analizy, jakość przedstawionych wyników oraz umiejętność powiązania teorii z zastosowaniami uzasadniają stwierdzenie, że Autor posiada wiedzę teoretyczną, zdolności koncepcyjne oraz kompetencje niezbędne do samodzielnego prowadzenia pracy naukowej.

Uważam, że przedstawiona rozprawa spełnia wymogi ustawowe stawiane pracom doktorskim w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja i wnoszę o przyjęcie jej przez Radę Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej oraz o dopuszczenie mgra inż. Adama Jagielskiego do publicznej obrony.

Zbigniew Puchała

prof. dr hab. Zbigniew Puchała