Dr hab. inż. Grzegorz Borowik Warszawa, dnia 3 listopada 2025 r.

Recenzja

osiągnięcia naukowego i aktywności naukowej dra inż. Michała Jakuba Wrońskiego

w postępowaniu o nadanie stopnia doktora habilitowanego
w dziedzinie nauk inżynieryjno-technicznych,
w dyscyplinie **informatyka techniczna i telekomunikacja**

1. Wprowadzenie

Recenzja została przygotowana na prośbę dr. hab. inż. Zbigniewa Tarapaty, prof. WAT, Przewodniczącego Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja w Wojskowej Akademii Technicznej (pismo z dnia 12 lutego 2025 r.), w związku z powołaniem komisji habilitacyjnej do przeprowadzenia postępowania o nadanie stopnia naukowego doktora habilitowanego nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja oraz powierzeniem mi funkcji recenzenta w tym postępowaniu. Recenzja dotyczy osiągnięć naukowych dr. inż. Michała Jakuba Wrońskiego.

W recenzji wziąłem pod uwagę przede wszystkim wymagania określone w ustawie z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2023 r. poz. 742 z późn. zm.), a także Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 19 stycznia 2018 r. w sprawie szczegółowego trybu i warunków przeprowadzania czynności w przewodzie doktorskim, w postępowaniu habilitacyjnym oraz w postępowaniu o nadanie tytułu profesora (Dz. U. z 2018 r. poz. 261). Uwzględniłem również powszechnie przyjęte kryteria oceny osiągnięć naukowych, artystycznych i dydaktycznych osób ubiegających się o nadanie stopnia doktora habilitowanego, a także wytyczne i interpretacje Rady Doskonałości Naukowej publikowane na jej oficjalnych stronach internetowych.

Zgodnie z **art. 219 ust. 1** ustawy Prawo o szkolnictwie wyższym i nauce, stopień doktora habilitowanego nadaje się osobie, która:

1) posiada stopień doktora;

2) posiada w dorobku osiągnięcia naukowe albo artystyczne, stanowiące znaczny wkład w rozwój określonej dyscypliny, w tym co najmniej:

   a) 1 monografię naukową wydaną przez wydawnictwo, które w roku opublikowania monografii w ostatecznej formie było ujęte w wykazie sporządzonym zgodnie z przepisami wydanymi na podstawie art. 267 ust. 2 pkt 2 lit. a, lub

   b) 1 cykl powiązanych tematycznie artykułów naukowych opublikowanych w czasopismach naukowych lub w recenzowanych materiałach z konferencji międzynarodowych,

które w roku opublikowania artykułu w ostatecznej formie były ujęte w wykazie sporządzonym zgodnie z przepisami wydanymi na podstawie art. 267 ust. 2 pkt 2 lit. b, lub

c) 1 zrealizowane oryginalne osiągnięcie projektowe, konstrukcyjne, technologiczne lub artystyczne;

3) wykazuje się istotną aktywnością naukową albo artystyczną realizowaną w więcej niż jednej uczelni, instytucji naukowej lub instytucji kultury, w szczególności zagranicznej.

W dokumencie Rady Doskonałości Naukowej pt. „Postępowania dotyczące nadawania stopnia doktora habilitowanego" czytamy, że „Recenzje należy uznać za wyraz osobistej oceny, o charakterze eksperckim, wkładu osoby ubiegającej się o nadanie stopnia doktora habilitowanego w rozwój określonej dyscypliny naukowej albo artystycznej. Nie stanowią one natomiast opinii biegłego w rozumieniu przepisów k.p.a., czy też dokumentu urzędowego w rozumieniu obowiązujących przepisów prawa. Brak jest także podstaw do uznania, że w toku procedowanego postępowania osoba ubiegająca się o nadanie stopnia doktora habilitowanego może polemizować ze sporządzonymi recenzjami." Dalej dokument wskazuje, że recenzenci „. . . oceniają, czy osiągnięcia naukowe osoby ubiegającej się o stopień doktora habilitowanego odpowiadają wymaganiom określonym w art. 219 ust. 1 pkt 2, i przygotowują recenzje. Z przepisu tego może wynikać, że podstawową i jedyną rolą recenzenta jest dokonanie oceny, czy osiągnięcia naukowe albo artystyczne osoby ubiegającej się o nadanie stopnia doktora habilitowanego odpowiadają wymaganiom określonym w art. 219 ust. 1 pkt 2 tej ustawy. Należy jednak przyjąć, że od recenzentów można oczekiwać dokonania oceny spełnienia wszystkich przesłanek warunkujących nadanie tego stopnia, w tym przede wszystkim, czy wskazane w dokumentacji wniosku informacje o aktywności naukowej albo artystycznej, o której mowa w art. 219 ust. 1 pkt 3 p.s.w.n., są istotne w ramach danej dyscypliny."

Podstawą opracowania recenzji były następujące materiały:

1. wniosek o przeprowadzenie postępowania w sprawie nadania stopnia doktora habilitowanego w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja,
2. kopia dokumentu potwierdzającego posiadanie stopnia doktora,
3. autoreferat w języku polskim,
4. wykaz osiągnięć naukowych, stanowiących znaczny wkład w rozwój dyscypliny informatyka techniczna i telekomunikacja,
5. kopie siedmiu publikacji, wchodzących w skład przedłożonego cyklu powiązanych tematycznie artykułów naukowych, zatytułowanego *„Zastosowanie wyżarzania kwantowego w kryptologii"*, stanowiącego osiągnięcie naukowe,
6. oświadczenia o wkładzie pracy dla publikacji wieloautorskich wchodzących w skład przedłożonego cyklu publikacji stanowiącego osiągnięcie naukowe,
7. dane wnioskodawcy.

2. Ogólny przebieg kariery naukowej habilitanta

Dr Michał Wroński uzyskał w roku 2018 stopień doktora nauk technicznych w dyscyplinie informatyka, specjalność kryptologia, na Wydziale Cybernetyki Wojskowej Akademii Technicznej. Tytuł rozprawy doktorskiej: *„Zastosowanie ciał rozszerzonych i specjalnych postaci krzywych eliptycznych w celu przyspieszenia obliczania krotności punktu na krzywej eliptycznej"*.

Od ukończenia studiów habilitant jest związany zawodowo z Wojskową Akademią Techniczną, a od sierpnia 2023 roku również z NASK–PIB, gdzie pełni funkcję eksperta ds. cyberbezpieczeństwa. W WAT zajmował kolejno stanowiska: młodszego inżyniera, inżyniera, asystenta badawczo-dydaktycznego oraz adiunkta.

Przebieg kariery zawodowej wskazuje na konsekwentne utrzymywanie aktywności naukowej w obszarze kryptologii, z rozszerzeniem zainteresowań o zagadnienia obliczeń kwantowych.

3. Charakterystyka dorobku publikacyjnego

3.1. Publikacje

W autoreferacie dr Michał Wroński przedstawił cykl siedmiu powiązanych tematycznie publikacji zatytułowany *„Zastosowanie wyżarzania kwantowego w kryptologii"*, stanowiący osiągnięcie naukowe w rozumieniu art. 219 ust. 1 pkt 2 lit. b ustawy Prawo o szkolnictwie wyższym i nauce. Cykl obejmuje prace opublikowane w latach 2021–2024 w renomowanych czasopismach i materiałach konferencji międzynarodowych.

Cykl publikacji tworzą:

- **Prace opublikowane w materiałach konferencyjnych (trzy):**

  H1: M. Wroński, *Index calculus method for solving elliptic curve discrete logarithm problem using quantum annealing*, International Conference on Computational Science (ICCS), Springer, 2021. Wkład: 100%, 140 pkt, konferencja rangi A wg CORE.

  H3: M. Wroński, *Practical solving of discrete logarithm problem over prime fields using quantum annealing*, ICCS, Springer, 2022. Wkład: 100%, 140 pkt, konferencja rangi A wg CORE.

  H4: O. Żołnierczyk, M. Wroński, *Searching B-Smooth Numbers Using Quantum Annealing: Applications to Factorization and Discrete Logarithm Problem*, ICCS, Springer, 2023. Wkład: 30%, 140 pkt, konferencja rangi A wg CORE.

- **Prace opublikowane w czasopismach naukowych (cztery):**

  H2: E. Burek, M. Wroński, K. Mańk, M. Misztal, *Algebraic attacks on block ciphers using quantum annealing*, *IEEE Transactions on Emerging Topics in Computing*, 2022. Wkład: 40%, 140 pkt, Impact Factor: 5,9.

  H5: M. Wroński, E. Burek, Ł. Dzierzkowski, O. Żołnierczyk, *Transformation of Elliptic Curve Discrete Logarithm Problem to QUBO Using Direct Method in Quantum Annealing Applications*, *Journal of Telecommunications and Information Technology*, 2024. Wkład: 65%, 40 pkt.

H6: M. Wroński, Ł. Dzierzkowski, *Base of exponent representation matters – more efficient reduction of discrete logarithm problem and elliptic curve discrete logarithm problem to the QUBO problem*, *Quantum Information and Computation*, 2024. Wkład: 70%, 100 pkt, Impact Factor: 0,7.

H7: M. Wroński, E. Burek, M. Leśniak, *(In)security of stream ciphers against quantum annealing attacks on the example of the Grain 128 and Grain 128a ciphers*, IEEE Transactions on Emerging Topics in Computing, 2025. Wkład: 50%, 140 pkt, Impact Factor: 5,1.

Sumarycznie cykl obejmuje:

- siedem publikacji naukowych (trzy konferencyjne i cztery w czasopiśmie),
- łącznie 840 pkt MEiN, po uwzględnieniu procentowego udziału autora: 544 pkt,
- łączny Impact Factor: 11,7, po uwzględnieniu procentowego udziału autora: IF = 5,4.

Wszystkie prace łączy wspólna tematyka badawcza dotycząca zastosowania wyżarzania kwantowego (*quantum annealing*) do problemów kryptograficznych, takich jak logarytm dyskretny, krzywe eliptyczne czy ataki algebraiczne na szyfry blokowe i strumieniowe. Trzy publikacje zostały zaprezentowane w ramach serii konferencji *International Conference on Computational Science (ICCS)*, zaliczanej do konferencji rangi A według klasyfikacji CORE, a następnie opublikowane w serii *Lecture Notes in Computer Science* wydawnictwa Springer. Pozostałe cztery prace ukazały się w recenzowanych czasopismach naukowych z listy MEiN, w tym dwie w wysoko punktowanym czasopiśmie *IEEE Transactions on Emerging Topics in Computing.*

Cykl publikacji jest spójny tematycznie i obejmuje opracowanie oraz analizę metod przekształcania wybranych problemów kryptograficznych do postaci umożliwiającej ich rozwiązanie przy użyciu wyżarzania kwantowego. W niektórych pracach autor ilustruje zaproponowane rozwiązania przykładami obliczeń wykonanych na rzeczywistych platformach D-Wave. Zakres publikacji stanowi podstawę do dalszej analizy merytorycznej w kontekście oceny osiągnięcia naukowego.

3.2. Tematyka i zawartość dokonania naukowego

Tematyka osiągnięcia naukowego dra Michała Wrońskiego dotyczy zastosowania wyżarzania kwantowego (*quantum annealing*) w kryptologii, w szczególności w kryptoanalizie wybranych algorytmów kryptograficznych. Autor wskazuje, że motywacją badań była potrzeba oceny odporności współczesnych systemów kryptograficznych na potencjalne zagrożenia wynikające z rozwoju technologii kwantowych oraz zbadanie granic praktycznego zastosowania dostępnych wyżarzaczy kwantowych, takich jak D-Wave, w rozwiązywaniu problemów kryptograficznych. Celem prac było również określenie, w jakim zakresie wyżarzanie kwantowe może być wykorzystane do kryptoanalizy algorytmów asymetrycznych i symetrycznych oraz czy może przewyższyć skuteczność klasycznych metod, takich jak pełne przeszukiwanie czy algorytm Grovera.

Cykl publikacji obejmuje siedem prac (H1–H7), które – zgodnie z deklaracją autora – tworzą tematycznie spójne osiągnięcie naukowe. Poszczególne artykuły dotyczą transformacji wybranych problemów kryptograficznych do postaci kwadratowego problemu binarnej optymalizacji

(*Quadratic Unconstrained Binary Optimization, QUBO*) oraz analizy możliwości ich rozwiązywania z wykorzystaniem algorytmów wyżarzania kwantowego. Przedstawione problemy obejmują zarówno zagadnienia kryptografii asymetrycznej, takie jak *Discrete Logarithm Problem* (DLP), *Elliptic Curve Discrete Logarithm Problem* (ECDLP) i *Integer Factorization Problem* (IFP), jak również wybrane przypadki szyfrów symetrycznych i strumieniowych.

W pierwszej grupie prac (H1, H3, H4) autor przedstawia zastosowanie wyżarzania kwantowego do rozwiązywania klasycznego problemu logarytmu dyskretnego w grupach multiplikatywnych i na krzywych eliptycznych. Wykorzystuje przy tym podejście oparte na metodzie rachunku indeksowego oraz analizie liczb B-gładkich. Prace te zawierają opis procedur przekształcania problemu do formy QUBO oraz wskazówki dotyczące implementacji modeli na architekturze D-Wave. W pracy H4 rozszerzono analizę o wyszukiwanie liczb B-gładkich, co pozwala autorowi porównać efektywność obliczeniową dla różnych klas instancji problemu DLP.

Druga grupa publikacji (H2, H5, H6) dotyczy zastosowania metod wyżarzania kwantowego w kryptoanalizie: (i) atakach algebraicznych na szyfry blokowe oraz (ii) redukcji i rozwiązywaniu problemu logarytmu dyskretnego w systemach kryptograficznych opartych na krzywych eliptycznych. Autor proponuje metody redukcji wielomianowych układów równań nad ciałami skończonymi do formy QUBO, umożliwiającej ich rozwiązanie w postaci problemu optymalizacyjnego. W pracy H2 zaproponowano redukcje algebraicznych układów równań opisujących komponenty szyfrów blokowych do postaci QUBO oraz oszacowano rozmiary powstałych modeli i wymagania dotyczące zasobów wyżarzania kwantowego. Natomiast prace H5 i H6 dotyczą redukcji i rozwiązywania problemu logarytmu dyskretnego w systemach kryptograficznych opartych na krzywych eliptycznych. W pracy H6 autor analizuje ponadto wpływ sposobu reprezentacji wykładników na efektywność tej redukcji.

W pracy H7 autor przenosi analizę na obszar szyfrów strumieniowych, badając potencjalną podatność algorytmów Grain-128 i Grain-128a na ataki z wykorzystaniem wyżarzania kwantowego. Zastosowano tu podejście analogiczne do wcześniejszych prac autora, oparte na przekształceniu problemu algebraicznego do formy QUBO oraz analizie zależności złożoności obliczeniowej od rozmiaru przestrzeni poszukiwań i liczby zmiennych binarnych.

Warto zarazem zauważyć, że część empiryczna cyklu obejmuje wyłącznie przypadki małej skali: w H1 rozważono ECDLP nad polem 8-bitowym, w H3 DLP nad polami 4–6 bitowymi, w H4 faktoryzację liczby 26-bitowej i DLP nad polem 18-bitowym, w H5 ECDLP nad polem 3-bitowym $\mathbb{F}_7$, zaś w H6 DLP nad 6-bitowym polem $\mathbb{F}_{47}$. Przykłady te potwierdzają poprawność proponowanych redukcji do QUBO i ich wykonalność na platformach D-Wave, lecz nie umożliwiają wiarygodnej oceny skuteczności i skalowalności dla parametrów bezpieczeństwa stosowanych w praktyce.

Osiągnięcie habilitacyjne obejmuje zatem szereg propozycji teoretycznych oraz implementacyjnych dotyczących redukcji złożonych problemów kryptograficznych do postaci optymalizacji binarnej, a także próby ich praktycznej realizacji na urządzeniach kwantowych. Autor deklaruje wykonanie eksperymentów obliczeniowych na platformach D-Wave, których wyniki mają charakter ilustracyjny i służą weryfikacji poprawności modeli. Pod względem konstrukcyjnym cykl obejmuje prace o charakterze koncepcyjnym, metodologicznym oraz w ograniczonym zakresie aplikacyjnym. Dominują rozważania formalne i opis procedur przekształceń matematycznych, natomiast część empiryczna ma charakter pomocniczy i ograniczony do eksperymentów o ma-

łej skali. Łącznie prace te stanowią próbę systematyzacji podejść do zastosowania wyżarzania kwantowego w kryptoanalizie, ze szczególnym uwzględnieniem klasycznych problemów trudnych obliczeniowo.

3.3. Autoocena wkładu pracy habilitanta

Z przedstawionego przez dra Michała Wrońskiego zestawienia wynika, że w większości publikacji wchodzących w skład osiągnięcia habilitacyjnego pełnił on wiodącą rolę organizacyjną i merytoryczną. W dwóch artykułach (H1, H3) jest autorem samodzielnym, natomiast w pozostałych pięciu jego zadeklarowany wkład mieści się w zakresie 30–70%. Z danych w wykazie dorobku wynika, że średni udział autora w całym cyklu wynosi ok. 65%. Współautorzy reprezentują ośrodki krajowe, z którymi habilitant współpracował w ramach zespołów badawczych.

Habilitant wskazuje, że we wszystkich pięciu publikacjach wieloautorskich był odpowiedzialny za koncepcję badań, opracowanie metod i modeli matematycznych prowadzących do redukcji rozważanych problemów kryptograficznych do postaci QUBO, a także za projektowanie i nadzór nad eksperymentami obliczeniowymi z wykorzystaniem wyżarzania kwantowego. Uczestniczył w analizie efektywności i poprawności modeli oraz koordynował prace badawcze i redakcyjne. Współautorzy wnieśli wkład głównie w implementację i realizację eksperymentów, weryfikację teoretyczną oraz opracowanie opisów metod i przykładów ilustrujących uzyskane wyniki.

Deklarowany rozkład udziału w poszczególnych publikacjach jest logicznie spójny i odpowiada pozycji autora w zespole. W publikacjach, w których nazwisko dra Wrońskiego znajduje się na pierwszym miejscu, przypisany procentowy wkład jest istotnie wyższy (65–100%), co można uznać za uzasadnione. W pozostałych przypadkach wartości 30–50% wydają się proporcjonalne do liczby współautorów i zakresu przypisanych zadań.

Uwzględniając charakter i tematykę cyklu, a także opisany udział habilitanta w opracowaniu modeli, realizacji badań i analizie wyników, można przyjąć, że odgrywał on kluczową rolę w realizacji przedstawionych prac. Deklarowane udziały procentowe mieszczą się w typowym zakresie dla publikacji wieloautorskich i wskazują na istotny i samodzielny wkład dra Wrońskiego w osiągnięcie habilitacyjne.

4. Ocena bibliometryczna (po uzyskaniu stopnia doktora)

Według danych przedstawionych przez habilitanta, dorobek naukowy zrealizowany po uzyskaniu stopnia doktora obejmuje łączną wartość **2230 punktów MEiN**, w tym **1073 punkty po uwzględnieniu udziału procentowego**, oraz **sumaryczny Impact Factor równy 20,6** (**9,9** po uwzględnieniu udziału procentowego). Dane te pochodzą z wykazu osiągnięć zawartego w rozdziale I.2.2 „Wyniki sumaryczne całego dorobku zrealizowanego po uzyskaniu stopnia doktora".

Należy jednak zauważyć, że w przedstawionym zestawieniu występują nieścisłości wymagające weryfikacji. Na przykład pozycja nr 25 – *„Searching for an Efficient System of Equations Defining the AES Sbox for the QUBO Problem"* – została faktycznie opublikowana w czasopiśmie *Journal of Telecommunications and Information Technology*, a nie, jak podano w wykazie, w *International Journal of Electronics and Telecommunications*. Zgodnie z aktualnym wykazem

czasopism MEiN, żadne z tych czasopism nie posiada wartości 140 punktów, co oznacza zawyżenie punktacji w zestawieniu habilitanta.

Aktualne dane bibliometryczne (na dzień 31 października 2025 r.) przedstawiają się następująco:

- w bazie **Scopus**: indeks Hirscha wynosi 5, liczba cytowań 81 (dla 28 publikacji indeksowanych), z czego cztery pozycje należą do cyklu habilitacyjnego;
- w bazie **Web of Science**: indeks Hirscha wynosi 3, liczba cytowań 20 (13 bez autocytowań), z czego jedynie dwie publikacje pochodzą z cyklu przedstawionego do oceny.

Wartości te wskazują na umiarkowany zasięg oddziaływania naukowego i ograniczoną liczbę odniesień do prac habilitanta w literaturze światowej. Mimo że publikacje w cyklu zostały pozytywnie zrecenzowane i opublikowane w uznanych źródłach, liczba cytowań pozostaje niska, co sugeruje niewielkie zainteresowanie środowiska naukowego tą tematyką. W tym kontekście wkład habilitanta w rozwój dyscypliny należy uznać za specjalistyczny, lecz o ograniczonym wpływie międzynarodowym.

Habilitant w uzasadnieniu odnosi się do bazy *Google Scholar*, uznając ją za najbardziej reprezentatywną dla jego dyscypliny ze względu na cytowania preprintów oraz niejawny charakter części jego dorobku. Należy jednak podkreślić, że w procedurach oceny dorobku naukowego w dyscyplinie *informatyka techniczna i telekomunikacja* przyjmuje się wskaźniki pochodzące z baz *Scopus* i *Web of Science*, które obejmują publikacje spełniające określone kryteria indeksacji. Dane z *Google Scholar*, obejmujące również cytowania z prac dyplomowych, niezweryfikowanych raportów lub dokumentów nieindeksowanych, nie mogą stanowić podstawy oceny parametrycznej.

Na tle aktualnych standardów obowiązujących w dyscyplinie *Informatyka techniczna i telekomunikacja* wskaźniki bibliometryczne habilitanta należy ocenić jako **niskie**. Zarówno wartości indeksu Hirscha w bazach *Scopus* i *Web of Science*, jak i liczba cytowań prac indeksowanych, pozostają istotnie poniżej poziomu typowego dla osób ubiegających się o nadanie stopnia doktora habilitowanego w tej dyscyplinie. Ograniczony zasięg cytowań oraz niewielka liczba publikacji w wysoko punktowanych czasopismach sugerują, że dorobek naukowy posiada charakter wąsko wyspecjalizowany i o ograniczonym oddziaływaniu w skali międzynarodowej. Wskazane nieścisłości w punktacji czasopism oraz zawyżone wartości punktowe wymagają korekty przed uznaniem danych za wiarygodne.

Warto również zauważyć, że habilitant posiada w dorobku inne publikacje dotyczące wyżarzania kwantowego, które tematycznie wiążą się z przedstawionym cyklem, jednak nie zostały do niego włączone. Autor nie uzasadnił przyczyn takiego wyboru. Niezależnie od tego, ich uwzględnienie nie miałoby wpływu na ocenę parametryczną dorobku, ponieważ nie zwiększyłoby wartości wskaźników bibliometrycznych w bazach indeksacyjnych.

Należy również zauważyć, że habilitant nie przedstawił informacji o odbyciu staży naukowych ani dłuższych pobytów badawczych w zagranicznych instytucjach akademickich, co ogranicza jego doświadczenie w zakresie mobilności międzynarodowej. Brak aktywności w tym obszarze, w połączeniu ze stosunkowo niewielką liczbą wystąpień na konferencjach międzynarodowych organizowanych poza granicami kraju (siedem spośród piętnastu wystąpień konferencyjnych), przekłada się na ograniczone możliwości rozpowszechniania wyników badań oraz budowania rozpoznawalno-

ści naukowej autora w środowisku międzynarodowym. W konsekwencji może to również częściowo tłumaczyć niewielką liczbę cytowań publikacji habilitanta w bazach *Scopus* i *Web of Science*.

5. Ocena pozostałych dokonań

5.1. Zatrudnienie, staże i współpraca naukowa

Dr Michał Wroński jest zatrudniony w Wojskowej Akademii Technicznej, gdzie pełni funkcję adiunkta, oraz w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym (NASK-PIB), jako ekspert w obszarze cyberbezpieczeństwa. Łączy zatem działalność akademicką z praktyką badawczą w instytucji o profilu wdrożeniowym, co sprzyja aplikacyjnemu ukierunkowaniu prowadzonych prac.

Z dokumentacji wynika, że habilitant nie odbył staży naukowych, w tym zagranicznych, ani nie realizował pobytów typu postdoc (również w kraju). Aktywność zawodowa i naukowa ogranicza się zasadniczo do dwóch ośrodków (WAT i NASK-PIB), co wskazuje na umiarkowaną mobilność akademicką. Brak dłuższych pobytów w instytucjach zagranicznych, które są istotnym elementem rozwoju samodzielności naukowej i budowania sieci współpracy międzynarodowej, należy ocenić jako słabą stronę dorobku habilitanta.

W zakresie współpracy naukowej habilitant wskazuje m.in. udział w projektach krajowych oraz kontakt z ośrodkami zagranicznymi w ramach konferencji i inicjatyw naukowych, takich jak *International Network on Quantum Annealing (INQA, 2024)*. Współpraca ta ma jednak charakter raczej punktowy i nie przybrała formy długofalowych partnerstw badawczych lub wspólnych projektów międzynarodowych.

5.2. Udział w projektach

Habilitant wskazuje w dokumentacji udział w dziewięciu projektach badawczych (osiem przedstawionych w punkcie II.4 *Wykazu osiągnięć naukowych* oraz jeden przedstawiony w punkcie II.10), realizowanych głównie w ramach krajowych programów finansowania nauki. We wszystkich przypadkach pełnił funkcję członka zespołu, odpowiadając za wykonywanie dokumentacji projektowej oraz programowanie. Jedynie w projekcie *ROTOR* sprawował funkcję kierownika jednego z zadań, co stanowi pojedynczy przypadek udziału w projekcie o zwiększonej odpowiedzialności merytorycznej.

W ocenie dorobku naukowego przyjmuje się zazwyczaj, że istotnym elementem potwierdzającym samodzielność badawczą jest doświadczenie w kierowaniu projektami lub pełnienie roli głównego badacza w zespołach realizujących projekty finansowane w drodze konkursu, również wewnętrznego. W przedstawionych przez habilitanta projektach nie odnotowano takiej roli, a zakres zadań miał charakter wykonawczy. Świadczy to o ograniczonej samodzielności w zakresie pozyskiwania finansowania oraz kierowania zespołami badawczymi.

Należy przy tym podkreślić, że uzyskane doświadczenie projektowe ma wartość praktyczną i potwierdza udział w pracach zespołów badawczych, jednak z punktu widzenia kryteriów oceny dorobku naukowego osoby ubiegającej się o stopień doktora habilitowanego należy uznać je za niewystarczające. Dorobek projektowy habilitanta, mimo udziału w kilku bardziej znaczących

przedsięwzięciach (m.in. *ROTOR*, *ISSIP-PKI*, *Lightweight Post Quantum Security Schemes*), ma charakter pomocniczy i nie wskazuje na samodzielną inicjatywę badawczą.

5.3. Udział w komitetach programowych, redakcyjnych i organizacyjnych; recenzowanie prac

Dr Michał Wroński uczestniczył w pracach komitetów organizacyjnych i programowych kilku konferencji naukowych, głównie z zakresu kryptologii i informatyki teoretycznej. Z wykazu dorobku wynika, że był członkiem komitetów programowych konferencji *Central European Conference on Cryptology* (CECC 2022–2024) oraz *Number-Theoretic Methods in Cryptology (NuTMiC 2024).* Ponadto pełnił funkcję współprzewodniczącego komitetu organizacyjnego konferencji CECC 2024 oraz brał udział w komitecie organizacyjnym konferencji *Mathematical Cryptology and Cybersecurity 2020.*

Habilitant deklaruje także członkostwo w międzynarodowej organizacji *IACR (International Association for Cryptologic Research)* oraz w Komitecie Naukowym Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa, co potwierdza jego zaangażowanie w środowisko naukowe, choć nie podaje pełnionych funkcji ani zakresu aktywności w tych gremiach.

W zakresie działalności recenzenckiej dr Wroński sporządził łącznie siedemnaście recenzji dla czasopism naukowych i materiałów konferencyjnych. Zakres tej aktywności potwierdza jego kompetencje eksperckie w dziedzinie kryptologii, choć liczba recenzji oraz udział w komitetach redakcyjnych pozostają umiarkowane jak na kandydata do stopnia doktora habilitowanego. Brak jest także informacji o uczestnictwie w stałych radach naukowych lub redakcjach czasopism.

5.4. Wyróżnienia

Habilitant otrzymał kilka wyróżnień za działalność naukową, w tym po doktoracie czterokrotnie *Stypendium Rektora-Komendanta Wojskowej Akademii Technicznej za działalność publikacyjną* (w latach 2018, 2020, 2021 i 2022). Najważniejszym osiągnięciem w tym zakresie jest uzyskanie w 2024 roku *Stypendium dla Wybitnych Młodych Naukowców*, przyznawanego przez Ministra Nauki i Szkolnictwa Wyższego.

Wyróżnienia te stanowią lokalne potwierdzenie aktywności publikacyjnej habilitanta. Należy jednak zauważyć, że poza wymienionymi nagrodami indywidualnymi brak jest informacji o innych formach uznania, takich jak nagrody zespołowe, wyróżnienia międzynarodowe czy nagrody instytucjonalne. W konsekwencji, choć uzyskane wyróżnienia świadczą o dobrej ocenie dotychczasowej działalności naukowej, ich liczba i zakres mają ograniczony wpływ na ocenę dorobku w kontekście ubiegania się o stopień doktora habilitowanego.

5.5. Działalność dydaktyczna

Dr Michał Wroński prowadzi od wielu lat zajęcia dydaktyczne w Wojskowej Akademii Technicznej z zakresu kryptologii, informatyki i matematyki. W jego dorobku dydaktycznym znajdują się wykłady, laboratoria i seminaria dla studentów studiów inżynierskich, magisterskich oraz doktoranckich, w tym zajęcia w języku angielskim. Habilitant wypromował kilkanaście prac dyplomowych i pełnił funkcję promotora pomocniczego w zakończonym przewodzie doktorskim.

Od 2018 roku organizuje seminaria kryptologiczne w Instytucie Matematyki i Kryptologii WAT, które przekształciły się w cykliczne *Kryptologiczne Seminaria Międzyuczelniane*, integrujące środowisko badaczy kryptologii. Uczestniczy także w pracach komisji wydziałowych zajmujących się doskonaleniem programów studiów i oceną jakości prac dyplomowych.

Działalność dydaktyczna habilitanta ma charakter systematyczny i spójny z jego profilem naukowym. Należy jednak zauważyć, że brak jest elementów świadczących o szerszej innowacyjności dydaktycznej, takich jak opracowanie nowych programów kształcenia, materiałów dydaktycznych, podręcznika, czy projektów finansowanych ze środków dydaktycznych.

5.6. Inne

Poza działalnością opisaną w poprzednich podpunktach habilitant wykazywał aktywność ekspercką na poziomie krajowym, m.in. jako recenzent wniosków badawczych oraz ekspert oceniający materiały objęte ograniczeniami dostępu. Uczestniczył również w inicjatywach branżowych, co wpisuje się w upowszechnianie wyników badań poza środowiskiem akademickim. Elementy te mają charakter uzupełniający względem podstawowej aktywności publikacyjnej i dydaktycznej habilitanta.

Na poziomie dorobku formalnego nie stwierdzono monografii ani patentów. W punkcie III.4 Wykazu odnotowano jedno wdrożenie instytucjonalne związane z realizacją zadania II.3 projektu *ROTOR*, którego wyniki – zgodnie z dokumentacją – zostały częściowo wykorzystane w praktyce.

6. Podsumowanie i ocena końcowa

6.1. Mocne strony wniosku

Osiągnięcie habilitacyjne jest tematycznie spójne i dotyczy aktualnego obszaru badań, jakim jest zastosowanie wyżarzania kwantowego w kryptoanalizie. Autor prezentuje konsekwentną linię badawczą, obejmującą transformacje wybranych problemów kryptograficznych (DLP, ECDLP, IFP, wybrane szyfry symetryczne) do postaci problemów optymalizacyjnych. Na uwagę zasługuje udział w publikacjach w uznanych źródłach (w tym prace w czasopiśmie o wysokim IF oraz komunikaty w serii konferencyjnej CORE A) oraz dwa artykuły samodzielne wchodzące w skład cyklu. Wkład merytoryczny habilitanta, deklarowany jako wiodący w większości prac (typowo 30–70%, a w dwóch przypadkach 100%), wskazuje na istotną rolę autora w koncepcji i realizacji badań. Na podkreślenie zasługuje także element nowości metodologicznej w H6 (alternatywna reprezentacja wykładnika), który prowadzi do zmniejszenia liczby zmiennych logicznych w redukcji DLP/ECDLP do QUBO i może stanowić punkt wyjścia do dalszych badań nad skalowalnością. Działalność dydaktyczna i organizacyjna (seminaria kryptologiczne, prace w komisjach wydziałowych) pozostają spójne z profilem naukowym.

6.2. Słabe strony wniosku

Wskaźniki bibliometryczne (h-index i liczba cytowań w bazach Scopus oraz Web of Science) są niskie jak na etap ubiegania się o stopień doktora habilitowanego, co świadczy o ograniczonym oddziaływaniu międzynarodowym dorobku. W dokumentacji występują nieścisłości w zakresie punktacji MEiN wybranych pozycji, wymagające korekty. Część empiryczna obejmuje wyłącznie

przypadki małej skali (m.in. 8-bit ECDLP – H1; 4–6 bit DLP – H3; 26-bit IFP i 18-bit DLP – H4; ECDLP nad $\mathbb{F}_7$ – H5; DLP nad $\mathbb{F}_{47}$ – H6), co pozwala potwierdzić poprawność redukcji do QUBO i ich wykonalność na D-Wave, lecz nie umożliwia wiarygodnej oceny skuteczności i skalowalności dla praktycznych parametrów kryptograficznych. Dorobek projektowy ma w przeważającej mierze charakter wykonawczy; brak jest doświadczenia w roli kierownika projektu lub głównego badacza w przedsięwzięciach finansowanych w drodze konkursu. Nie odnotowano staży podoktorskich ani dłuższych pobytów badawczych za granicą, a mobilność naukowa jest umiarkowana (aktywność skoncentrowana zasadniczo w dwóch ośrodkach). Liczba wystąpień na konferencjach międzynarodowych za granicą jest mała, co w połączeniu z brakiem samodzielnych wdrożeń, monografii i patentów nie sprzyja zwiększaniu rozpoznawalności i cytowalności wyników. Autor mógłby klarowniej uzasadnić dobór publikacji w cyklu oraz włączyć inne posiadane prace o zbliżonej tematyce.

6.3. Ocena końcowa

Przedstawiony cykl publikacji spełnia wymóg spójności tematycznej i dotyczy problematyki istotnej z punktu widzenia rozwoju metod kryptoanalizy w kontekście obliczeń kwantowych. Jednocześnie charakter osiągnięcia – polegający na konsekwentnym rozwijaniu jednej, wąskiej osi badawczej (redukcje problemów kryptograficznych do QUBO i ich walidacje na małych instancjach na D-Wave) – zbliża ten cykl bardziej do profilu pracy doktorskiej lub etapu badań podoktorskich niż do standardu habilitacyjnego, który zwyczajowo łączy skalę, uogólnienia, wpływ i potwierdzoną samodzielność (w tym kierownictwo projektów, mobilność międzynarodową, rozpoznawalność i cytowalność). Ponadto poziom udokumentowanego oddziaływania naukowego (cytowalność, h-index), ograniczona skala i zakres walidacji eksperymentalnej, brak samodzielnych osiągnięć projektowych i mobilności międzynarodowej powodują, że przedstawione osiągnięcia nie wypełniają w sposób przekonujący przesłanki „znacznego wkładu w rozwój dyscypliny" w rozumieniu art. 219 ust. 1.

Należy przy tym podkreślić, że przedstawione w recenzji uwagi i oczekiwania wobec dorobku habilitanta nie mają charakteru rygorystycznej listy wymagań, lecz stanowią wskazanie kierunków, w których cykl mógłby zostać pogłębiony i uzupełniony w przyszłości. Ich celem jest wskazanie obszarów wymagających dalszego rozwoju, a nie oczekiwanie spełnienia wszystkich postulatów jednocześnie.

Niemniej, pomimo dostrzegalnego potencjału i konsekwentnie prowadzonej linii badawczej, obecny zakres i skalę oddziaływania dorobku naukowego należy ocenić jako zbyt ograniczone, by uzasadniały nadanie stopnia doktora habilitowanego na obecnym etapie.

W świetle powyższego rekomenduję ocenę negatywną w postępowaniu o nadanie stopnia doktora habilitowanego.

PODPIS ZAUFANY
GRZEGORZ ANDRZEJ
BOROWIK
03.11.2025 07:47:34 GMT+1
Dokument podpisany elektronicznie
podpisem zaufanym