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

Gliwice, 27 czerwiec 2025 r.

Recenzja rozprawy habilitacyjnej i całokształtu dorobku naukowego, dydaktycznego i organizacyjne dra Michała Wrońskiego

Podstawowe dane o kandydacie

- Kandydat uzyskał stopień doktora z nauk technicznych w dyscyplinie informatyka, specjalność kryptologia, w roku 2018 w Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego, Wydział Cybernetyki. Tytuł rozprawy doktorskiej: *Zastosowanie ciał rozszerzonych i specjalnych postaci krzywych eliptycznych w celu przyspieszenia obliczania krotności punktu na krzywej eliptycznej.*
- Przebieg pracy naukowo-zawodowej:
  - Młodszy inżynier (podporucznik), Wojskowa Akademia Techniczna, Warszawa, wrzesień 2011 - wrzesień 2014,
  - Inżynier (porucznik), Wojskowa Akademia Techniczna, Warszawa, wrzesień 2014 - styczeń 2017,
  - Asystent badawczo-dydaktyczny, Wojskowa Akademia Techniczna, Warszawa, styczeń 2017 - listopad 2020,
  - Adiunkt, Wojskowa Akademia Techniczna, Warszawa, listopad 2020 - styczeń 2023,
  - Adiunkt (stanowisko cywilne - pełen etat), Wojskowa Akademia Techniczna, Warszawa, luty 2023 - lipiec 2023,
  - Adiunkt (stanowisko cywilne - pół etatu), Wojskowa Akademia Techniczna, Warszawa, sierpień 2023 - obecnie,
  - Ekspert ds. Cyberbezpieczeństwa (pełen etat), Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy, Warszawa, sierpień 2023 - obecnie.

Strona formalna wniosku

Obiektem oceny habilitanta jest, według art. 219 ust 1. pkt 2b Ustawy Prawo o szkolnictwie wyższym i nauce, osiągnięcie naukowe w postaci jednotematycznego cyklu publikacji pt. *Zastosowanie wyżarzania kwantowego w kryptologii*

Według ustawy stopnień doktora habilitowanego nadaje się osobie, która:

- posiada stopień doktora;
- posiada w dorobku osiągnięcia naukowe albo artystyczne, stanowiące znaczny wkład w rozwój określonej dyscypliny, w tym co najmniej:
  - 1 monografię naukową, wydaną przez wydawnictwo, które w roku opublikowania monografii w ostatecznej formie byto ujęte w wykazie sporządzonym zgodnie z przepisami wydanymi na. Podstawie art. 267 ust. 2 pkt 2 lit. a, lub
  - 1 cykl powiązanych tematycznie artykułów naukowych opublikowanych w czasopismach naukowych lub w recenzowanych materiałach z konferencji międzynarodowych, które w roku opublikowania artykuły w ostatecznej formie były ujęte w wykazie sporządzonym zgodnie z przepisami wydanymi na podstawie art. 267 ust. 2 pkt 2 lit. b, lub
  - 1 zrealizowane oryginalne osiągnięcie projektowe, konstrukcyjne, technologiczne lub artystyczne;
- wykazuje się istotna aktywnością naukowa albo artystyczna realizowana w więcej niż jednej uczelni, instytucji naukowej lub instytucji kultury, w szczególności zagranicznej.
- Osiągnięcie może stanowić część pracy zbiorowej, jeżeli opracowanie wydzielonego zagadnienia jest indywidualnym wkładem osoby ubiegającej się o stopień doktora habilitowanego.

Ocena dorobku naukowego

- Tytuł osiągnięcia naukowego przedstawionego do oceny: *Zastosowanie wyżarzania kwantowego w kryptologii.*
- Dane naukometryczne. Dane różnią się w różnych bazach. Według Google Scholar: Indeks H: 7, 126 cytowań.

  Zarówno indeks Hirscha jak i indeks cytowań nie stanowi kryterium oceny habilitanta. Są one zbyt zależne od wielu niemerytorycznych czynników.

- Artykuły przedstawione jako osiągnięcie naukowe opublikowane są w dobrych (w zakresie swojej specjalizacji) czasopismach.
  - **International Conference on Computational Science (publikacje: H1, H3, H4)**
    * Ranga: A według rankingu CORE.
    * Punkty ministerialne: 140 pkt.
    * Wysoka rozpoznawalność międzynarodowa.
  - **IEEE Transactions on Emerging Topics in Computing (publikacja: H2, H7)**
    * Impact Factor: 5.1
    * Punkty ministerialne: 140 pkt.
    * Wysokiej jakości czasopismo o znaczącym wpływie na dziedzinę informatyki, szczególnie technologii wschodzących i innowacyjnych.
  - **Journal of Telecommunications and Information Technology (publikacja: H5)**
    * Punkty ministerialne: 40 pkt.
    * Czasopismo o niższym, bardziej lokalnym oddziaływaniu, ale solidne merytorycznie.
  - **Quantum Information and Computation (publikacja: H6)**
    * Impact Factor: 0.7
    * Punkty ministerialne: 100 pkt.
    * Specjalistyczne czasopismo naukowe, koncentrujące się na tematyce obliczeń i informacji kwantowej, o umiarkowanym wpływie w środowisku naukowym.

- Habilitant odegrał kluczową rolę w powstaniu publikacji składających się na osiągnięcie naukowe dotyczących zastosowania wyżarzania kwantowego w kryptologii. Jego wkład obejmował zarówno inicjowanie projektów, opracowywanie kluczowych idei i formalizmu matematycznego, jak i prowadzenie dowodów głównych wyników. Był także zaangażowany w proces przygotowywania manuskryptów, ich przesyłania do recenzji oraz odpowiadania na uwagi recenzentów. Jego specjalistyczna wiedza w zakresie kryptologii, obliczeń kwantowych oraz matematycznej teorii bezpieczeństwa algorytmów kryptograficznych przyczyniła się znacząco do osiągniętych wyników. Fakty te są potwierdzone odpowiednimi oświadczeniami współautorów.

Badania habilitanta koncentrują się na zastosowaniu metod wyżarzania kwantowego w kryptoanalizie różnego rodzaju algorytmów kryptograficznych, zarówno symetrycznych, jak i asymetrycznych. Szczególnie ważnym aspektem tych badań jest określenie możliwości praktycznego zastosowania wyżarzania kwantowego do rozwiązywania problemów kryptologicznych o rzeczywistych rozmiarach.

Ponadto habilitant bada kwestie związane z optymalizacją i transformacją problemów kryptologicznych do postaci Quadratic Unconstrained Binary Optimization (QUBO) oraz analizuje ich rozwiązywalność z wykorzystaniem współczesnych technologii kwantowych.

Habilitant skupia się na następujących kierunkach badawczych:

1. Wykorzystanie wyżarzania kwantowego do rozwiązywania problemów logarytmu dyskretnego (DLP) oraz logarytmu dyskretnego na krzywych eliptycznych (ECDLP).

2. Badanie możliwości stosowania metod hybrydowych (klasyczno-kwantowych) w kryptoanalizie, zwłaszcza w metodach opartych na przesiewaniu i zbieraniu relacji.

3. Analiza efektywności algorytmów kwantowych w kontekście bezpieczeństwa szyfrów strumieniowych i blokowych, porównując je do algorytmów klasycznych oraz algorytmu Grovera.

Habilitant zajmuje się również zagadnieniami dotyczącymi wpływu obliczeń kwantowych na bezpieczeństwo współczesnych algorytmów kryptograficznych, jak również możliwości adaptacji i standaryzacji nowych, odpornych na kwantowe ataki kryptograficznych mechanizmów bezpieczeństwa.

Znaczenie wyników badań. Wyniki badań habilitanta mają istotne znaczenie dla rozwoju kryptografii kwantowej oraz dla oceny bezpieczeństwa współczesnych mechanizmów kryptograficznych. Dzięki swoim badaniom, habilitant wskazał potencjalne zagrożenia związane z zastosowaniem metod wyżarzania kwantowego w kryptoanalizie algorytmów kryptograficznych.

Jednym z istotnych osiągnięć jest opracowanie praktycznych metod redukcji problemów logarytmu dyskretnego (DLP) oraz logarytmu dyskretnego na krzywych eliptycznych (ECDLP) do postaci problemu QUBO, umożliwiających ich rozwiązywanie z wykorzystaniem komputerów kwantowych.

Habilitant przyczynił się również do zrozumienia realnych możliwości ataków kwantowych na szyfry symetryczne, co jest kluczowe w kontekście standaryzacji i wyboru bezpiecznych algorytmów kryptograficznych.

Dzięki swojemu interdyscyplinarnemu podejściu, łączącemu wiedzę z zakresu kryptologii, matematyki, fizyki kwantowej i informatyki, habilitant wnosi istotny

wkład w rozwój nowoczesnych technologii kwantowych oraz bezpieczeństwa cyfrowego.

Osiągnięcia dydaktyczne

Działalność dydaktyczna

- Prowadzenie zajęć dydaktycznych na kierunkach informatycznych w Wojskowej Akademii Technicznej, w tym z zakresu kryptologii, bezpieczeństwa systemów informatycznych oraz obliczeń kwantowych.
- Opieka naukowa nad pracami dyplomowymi studentów, w tym pracą magisterską zakończoną publikacją naukową.
- Rozwój i aktualizacja materiałów dydaktycznych dotyczących kryptografii i bezpieczeństwa komputerowego, uwzględniających najnowsze trendy i technologie.
- Aktywne uczestnictwo w procesie ewaluacji jakości kształcenia oraz w pracach zespołów programowych.

Działalność organizacyjna i popularyzatorska

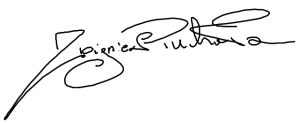
- Organizacja seminariów i warsztatów dotyczących kryptografii kwantowej oraz bezpieczeństwa cybernetycznego.
- Udział w projektach edukacyjnych mających na celu popularyzację wiedzy z zakresu nowych technologii oraz bezpieczeństwa cyfrowego.

Osiągnięcia w dziedzinie popularyzacji nauki

- Udział jako prelegent w konferencjach popularyzujących naukę oraz warsztatach edukacyjnych dotyczących technologii kwantowych i bezpieczeństwa cyfrowego.
- Autorstwo materiałów edukacyjnych popularyzujących kryptologię oraz obliczenia kwantowe skierowanych do szerokiego kręgu odbiorców.
- Współpraca z instytucjami edukacyjnymi w zakresie popularyzacji zagadnień związanych z nowoczesnymi technologiami i ich wpływem na bezpieczeństwo.

Ocena i wnioski końcowe

Uważam, że całokształt aktywności naukowej, organizacyjnej i dydaktycznej dr. Michała Wrońskiego jest **pozytywny** i uważam, że **spełnia** wymagania stawiane przez stosowną ustawę. Na podstawie przedstawionej analizy **popieram wniosek o nadanie stopnia doktora habilitowanego w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja** dr. Michałowi Wrońskiemu.



Digitally signed by
Zbigniew Puchała
Date: 2025.06.27 12:53:21
CEST

prof. dr hab. Zbigniew Puchała