dr hab. inż. Mariusz Uchroński
Katedra Automatyki, Mechatroniki
i Systemów Sterowania
Wydział Informatyki i Telekomunikacji
Politechnika Wrocławska
Wyb. Wyspiańskiego 27
50-370 Wrocław

Wrocław, 01.08.2025

Ocena dorobku naukowego i aktywności naukowej dr. inż. Michała Wrońskiego w związku z postępowaniem w sprawie nadania stopnia naukowego doktora habilitowanego w dziedzinie nauk technicznych w dyscyplinie informatyka techniczna i telekomunikacja

Niniejsza recenzja dotyczy osiągnięcia naukowego oraz istotnej aktywności naukowej dr. Michała Wrońskiego związanej z postępowaniem habilitacyjnym prowadzonym przez Radę Dyscypliny Informatyka Techniczna i Telekomunikacja w Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego. Formalną podstawą do sporządzenia recenzji było pismo Przewodniczącego Rady Dyscypliny prof. Zbigniewa Tarapaty z dnia 19.05.2025 (wpłynęło do Politechniki Wrocławskiej 20.05.2025) oraz Uchwale Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego z dnia 13.05.2025

Recenzja została sporządzona w oparciu o przesłane materiały obejmujące:

- cykl publikacji powiązanych tematycznie pt. *„Zastosowanie wyżarzania kwantowego w kryptologii”*,
- Autoreferat,
- wykaz opublikowanych prac naukowych po uzyskaniu stopnia doktora,
- informacje o współpracy z otoczeniem społecznym i gospodarczym,
- informacje naukometryczne.

Przedstawiona dokumentacja, wraz z Autoreferatem składającym się z 42 stron oraz dokumenty uzupełniające zawierają materiały niezbędne do przygotowania opinii zgodnie z kryteriami zawartymi w Rozporządzeniu Ministra Nauki i Szkolnictwa Wyższego z dnia 19 stycznia 2018 r.

1. **Ocena cyklu publikacji powiązanych tematycznie dr. Michała Wrońskiego p.t. *„Zastosowanie wyżarzania kwantowego w kryptologii”*.**

Zaprezentowane przez Habilitanta osiągnięcie naukowe będące podstawą postępowania habilitacyjnego składa się z 7 publikacji naukowych (3 z nich posiadają wskaźnik *Impact Factor*):

[H1] Wroński M., Index calculus method for solving elliptic curve discrete logarithm problem using quantum annealing, Proceedings of International Conference on Computational Science, Springer, 2021, 149-155 (140 pkt),

[H2] Burek E., Wronski M. J., Mank K., Misztal M., Algebraic attacks on block ciphers using quantum annealing, IEEE Transactions on Emerging Topics in Computing, 2022, 678 – 689 (140 pkt),

[H3] Wroński M., Practical solving of discrete logarithm problem over prime fields using quantum annealing, Proceedings of International Conference on Computational Science, Springer, 2022, 93-106 (140 pkt),

[H4] Żołnierczyk O., Wroński M., Searching B-Smooth Numbers Using Quantum Annealing: Applications to Factorization and Discrete Logarithm Problem, Proceedings of International Conference on Computational Science, Springer, 2023, 3-17 (140 pkt),

[H5] Wroński M., Burek E., Dzierzkowski Ł., Żołnierczyk O., Transformation of Elliptic Curve Discrete Logarithm Problem to QUBO Using Direct Method in Quantum Annealing Applications, Journal of Telecommunications and Information Technology, 2024, 75-82 (40 pkt),

[H6] Wroński M., Dzierzkowski Ł., 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 24 (7&8), 2024, 0541-0564 (100 pkt),

[H7] Wroński M., Burek E., Leśniak M., (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 (early access) (140 pkt).

Cele badań prowadzonych w ramach przedstawionego cyklu publikacji to:

- określenie górnego limit rozmiaru danych dla klasycznych algorytmów asymetrycznych w kontekście możliwości deszyfracji przy użyciu istniejącej infrastruktury wyżarzaczy kwantowych,
- potencjalne zastosowanie kwantowych wyżarzaczy w kryptoanalizie w kontekście symetrycznych algorytmów szyfrujących.

Mchwisław

Lektura ocenianego cyklu publikacji pozwala stwierdzić, że powyższe cele zostały osiągnięte przez opracowanie nowych metod rozwiązywania problemów kryptograficznych o ograniczonych rozmiarach z wykorzystaniem kwantowego wyżarzania zarówno w sposób bezpośredni jak i hybrydowy. Prace [H2], [H6] i [H7] zostały opublikowane w czasopismach posiadających *Impact Factor*. Natomiast prace [2] i [4] zostały opublikowane w czasopismach bez wskaźnika *Impact Factor*. Prace [H1], [H3], H[4] zostały opublikowane w materiałach konferencji ICCS, która jest znaczącą konferencją w tematyce informatyki przyciągającą wielu uczestników prezentujących referaty o wysokim poziomie merytorycznym. Należy zwrócić uwagę na fakt, że 2 z 7 prac stanowiących cykl są publikacjami jednoautorskimi.

W pracy [H1] zaprezentowany został sposób realizacji metody indeksu na krzywych eliptycznych (odmiana ECDLP, *Elliptic Curve Discrete Logarithm Problem*) z wykorzystaniem wyżarzania kwantowego. W tym celu autor przekształcił problem wyszukiwania relacji do problemu QUBO, a następnie rozwiązał dla krzywej eliptycznej zdefiniowanej nad 8-bitowym ciałem prostym wykorzystując środowisko obliczeniowe D-Wave LeapHybridSolver. Pomimo braku wykorzystania natywnego podejścia do obliczeń kwantowych z użyciem DWaveSampler po wcześniejszym osadzeniu problemu QUBO w topologii QPU praca prezentuje nowatorskie podejście do rozwiązywania problemów w kryptologii. Praca została opublikowana w materiałach konferencji ICCS 2021.

Praca [H4] będąca naturalną kontynuacją pracy [H1] dotyczy zastosowania faktoryzacji liczb całkowitych z wykorzystaniem sita kwadratowego oraz rozwiązywania problemu logarytmu dyskretnego (DLP, *Discrete Logarithm Problem*) za pomocą metody indeksu. Eksperymenty obliczeniowe (część kwantowa zaproponowanego podejścia) zostały oparte o natywny solver korzystający bezpośrednio z QPU uruchomiony na komputerze kwantowym D-Wave Advantage. Uzyskane wyniki eksperymentów obliczeniowych wskazują na możliwość rozwiązania problemu DLP o rozmiarach od 14 do 18 bitów w czasie odpowiednio od 0,9s do 18s. Praca została opublikowana w materiałach konferencji ICCS 2023.

W pracy [H3] została przedstawiona efektywna metoda redukcji problemu logarytmu dyskretnego (DLP) w ciele prostym do problemu QUBO. W zaproponowanej przez Habilitanata efektywna metodzie redukcji do problemu QUBO transformacja jest wykonywana przez dekompozycję problemu z wykorzystaniem regularnego drzewa binarnego o maksymalnej wysokości. Eksperymenty obliczeniowe zostały wykonane bezpośrednio na QPU komputera kwantowego D-Wave Advantage. Podejście efektywne zostało zastosowane dla problemu logarytmu dyskretnego nad ciałem F_{11} i zestawione z podejściem brutalnym dla DLP nad ciałem F_{59} oraz z podejściem mieszanym dla DLP nad ciałem F_{23}. Dodatkowo w pracy zawarte zostało porównanie osadzeń na QPU dla rozwiązywanych problemów QUBO z wykorzystaniem wyżarzacza kwantowego z topologią Pegasus. Na podstawie przeprowadzonych eksperymentów obliczeniowych Habilitant wysunął wniosek, że w rozwiązywaniu problemów QUBO na wyżarzaczach kwantowych istotny jest nie tylko sam rozmiar problemu (liczba zmiennych binarnych), ale także liczba interakcji między zmiennymi. Praca została opublikowana w materiałach konferencji ICCS 2022.

W pracy [H5] została przedstawiona metoda redukcji problemu logarytmu dyskretnego na krzywych eliptycznych (Edwardsa) do problemu QUBO z wykorzystaniem około $3n^3$ kubitów logicznych. W pracy zawarte zostały wyniki praktycznych eksperymentów obliczeniowych w ramach których został rozwiązany logarytm dyskretny na krzywej Edwardsa w podgrupie rzędu 8 nad ciałem F_7. Osadzenie problemu QUBO z 58 zmiennymi wymagało 112 fizycznych kubitów w topologii Pegasus na komputerze kwantowym D-Wave Advantage 6.1. Jest to praca współautorska opublikowana w czasopiśmie Journal of Telecommunications and Information Technology.

Praca [H6] zawiera udoskonalone wyniki uzyskane w pracach [H3] i [H5]. Udoskonalenie oparte jest na użyciu innej niż binarna reprezentacji wykładnika. W pracy zostało wykonane oszacowanie łącznej liczby zmiennych binarnych wymaganych do przekształcenia problemu logarytmu dyskretnego do problemu QUBO. Uzyskany wynik jest asymptotycznie lepszy od $3n^3$ otrzymanego dla binarnej reprezentacji wykładnika przedstawionego w pracy [H5]. Eksperymenty obliczeniowe zostały przeprowadzone dla DLP nad ciałem prostym F_{47} dla bazy o podstawie 2 oraz o podstawie 3 na komputerze kwantowym D-Wave Advantage2, a także dla DLP nad ciałem prostym F_{13} dla bazy o podstawie 2 oraz o podstawie 3 na komputerze kwantowym D-Wave Advantage. Udało się rozwiązać jedynie przykład dla DLP nad ciałem prostym F_{47} dla bazy o podstawie 3, dla którego liczba zmiennych problemu QUBO wynosiła 36, a liczba użytych kubitów w topologii Zephyr wynosiła 117. Brakuje porównania tego wyniku z użyciem komputera kwantowego D-Wave Advantage z topologią Pegasus. Potencjalnie pozwoliłoby to na odpowiedź na pytanie czy nowa generacja komputerów kwantowych D-Wave pozwala efektywniej rozwiązywać problemy QUBO (lub uzyskiwać lepsze osadzenia w topologii Zephyr). W pracy brakuje również szerszego komentarza co do uzyskanych osadzeń modelu QUBO dla dwóch architektur komputera kwantowego D-Wave: *Zephyr* oraz *Pegasus.* Jest to praca współautorska opublikowana w czasopiśmie Quantum Information and Computation.

Praca [H2] opera się na spostrzeżeniu, że operacja binarna w ciele binarnym może być przekształcona w analogiczny sposób jak każda operacja w innym ciele binarnym. Spostrzeżenie to pozwoliło na znaczące uproszczenie transformacji ataku na AES do problemu QUBO. Zaproponowana przez Habilitanta metoda pozwoliła po zastosowaniu innych usprawnień do transformacji algorytmu AES-128 do problemu QUBO przy użyciu 30 026 zmiennych. Pomimo redukcji liczby zmiennych o ponad 56% wynikowy problem QUBO nie może być rozwiązany na dostępnych obecnie komputerach kwantowych. Przeprowadzona przez Habilitanta analiza wskazuje, że problem QUBO reprezentujący AES-128 nie będzie możliwy do rozwiązania w najbliższych latach. Praca została opublikowana w prestiżowym czasopiśmie *IEEE Transactions on Emerging Topics in Computing.*

Praca [H7] będąca rozwinięciem pracy [H2] dotyczy efektywnej redukcji ataku algebraicznego na szyfry Grain 128 oraz Grain 128a do problemu QUBO. Wprowadzone udoskonalenia pozwalają na skutecznie zmniejszenie o kilkaset całkowitą liczbę zmiennych wynikowego problemu QUBO. Uzyskana redukcja liczby zmiennych jest kluczowa ponieważ jakość uzyskiwanych rozwiązań na komputerach kwantowych silnie zależy od liczby zmiennych

problemu QUBO. W pracy została przeprowadzona analiza ograniczeń osadzania modelu QUBO dla komputera kwantowego D-Wave z topologią Zephyr, co uzasadnia brak możliwości osadzenia problemów QUBO dla pełnych ataków na szyfry Grain 128 oraz Grain 128a. Z tego powodu przeprowadzone zostały eksperymenty dla mniejszych rozmiarów problemów QUBO reprezentujących ataki na szyfry Grain 128 oraz Grain 128a. Praca została opublikowana w czasopiśmie *Transactions on Emerging Topics in Computing*.

Podsumowując, prace wchodzące w skład cyklu publikacji stanowią przemyślaną sekwencję oraz prezentują proces tworzenia metodologii rozwiązywania problemów kryptograficznych na komputerach kwantowych opartych o kwantowe wyżarzanie. Zakres przeprowadzonych eksperymentów obliczeniowych (w wymiarze ilościowym oraz rozmiarów problemów) nie jest szeroki co jest konsekwencją obecnego stanu technologii obliczeń kwantowych. Obecnie jesteśmy w tzw. erze NISQ (*ang. noisy intermediate scale quantum*) - technologia kwantowa nie jest ani całkowicie niezawodna, ani zdolna do rozwiązywania problemów średniej lub dużej wielkości. Istotnym osiągnięciem naukowym Habilitanta jest tutaj opracowanie modeli QUBO pozwalających na rozwiązywanie problemów kryptograficznych w środowiskach obliczeniowych opartych o wyżarzanie kwantowe. Opracowane modele QUBO mogą stanowić podstawę do przeprowadzenia kryptoanalizy w innych środowiskach obliczeń kwantowych (np. istniejących już komputerach kwantowych w technologii niskotemperaturowych kubitów nadprzewodzących). Wyniki badań naukowych Habilitanta wskazują na gotowość do przeprowadzenia kryptoanalizy w środowisku obliczeń kwantowych. Pomimo istniejących ograniczeń technologicznych kryptoanaliza algorytmów AES-128 oraz Grain 128 zawarta w pracach [H2] oraz [H7] ma charakter praktyczny w porównaniu do wyników z pozostałych prac z cyklu.

Wyniki badań naukowych uzyskane w cyklu powiązanych tematycznie publikacji uzyskane zostały w procesie badawczym, na który składały się analiza teoretyczna, studium przypadku oraz eksperymenty obliczeniowe. Oceniany dorobek naukowy Habilitanta stanowi istotny wkład w rozwój dyscypliny informatyka w zakresie kryptologii i kyptoanalizy z zastosowaniem wyżarzania kwantowego. Opublikowane prace zawierają oryginalne wyniki oraz prezentują konsekwentną pracę badawczą. W mojej ocenie przedstawiony cykl powiązanych tematycznie publikacji naukowych spełnia ustawowe i zwyczajowe wymagania stawiane rozprawom habilitacyjnym.

2. **Ocena pozostałego dorobku naukowego po uzyskaniu stopnia doktora**

Pozostały dorobek Habilitanta (poza pracami składającymi się na cykl publikacji) obejmuje: 12 prac w czasopismach informatycznych posiadających wskaźnik *Impact Factor*, 10 prac w innych czasopismach o tematyce dotyczącej cyberbezpieczeństwa, 10 prac w materiałach konferencji krajowych i międzynarodowych, 1 rozdział w monografii. Wskazany dorobek naukowy dotyczy metod i algorytmów modelowania problemów z dziedziny szyfrowania.

Z perspektywy naukometrycznej dorobek naukowy Habilitanta jest na wystarczającym poziomie. Wskazuje na to współczynnika Hirscha (*h-index*) wynoszący 7 według Google Scholar (4 bez autocytowań), a także sumaryczna liczba cytowań wynosząca według Google Scholar 126 na dzień składania wniosku (60 bez autocytowań). Sumaryczny *Impact Factor* dorobku Habilitanta, wynoszący ponad 21 w mojej ocenie jest zadawalający.

W mojej ocenie całość dorobku naukowego Habilitanta jest znacząca i wystarczającą jako podstawa do nadania stopnia doktora habilitowanego w dyscyplinie informatyka techniczna i telekomunikacja.

3. **Ocena dorobku dydaktycznego i popularyzatorskiego oraz w zakresie współpracy międzynarodowej**

Habilitant wykazuje zaangażowanie w projekty badawcze (także o znaczeniu międzynarodowym), a także współpracował (lub wciąż współpracuje) z podmiotami gospodarczymi oraz agencjami wojskowymi i rządowymi. Ponadto Habilitant współuczestniczył w przygotowaniu wniosku projektowego do programu „Perun", dotyczącego oceny odporności algorytmów kryptograficznych na ataki z wykorzystaniem wyżarzania kwantowego. Rola Habilitanta tym projekcie sprowadza się do analizy algorytmów symetrycznych i asymetrycznych w kontekście nowoczesnych zagrożeń kwantowych.

Na dorobek dydaktyczny habilitanta składa się realizacja wykładów, laboratoriów oraz seminariów z zakresu kryptologii, matematyki dyskretnej, podstaw informatyki oraz cyberbezpieczeństwa. Warto zwrócić uwagę na udział Habilitanta w współtworzeniu programów nauczania w obszarze dostosowania ich do dynamicznych zmian w dziedzinie kwantowych metod obliczeniowych i kryptografii co ma duże znaczenie w popularyzacji szeroko pojętych obliczeń kwantowych.

Habilitant był promotorem 5 prac inżynierskich oraz 12 prac magisterskich oraz był promotorem w 1 zakończonym przewodzie doktorskim. Obecnie pełni funkcję promotora pomocniczego 3 otwartych przewodach doktorskich.

Na tym etapie współpraca międzynarodowa Habilitanta pomimo zaangażowany w projekty badawcze o znaczeniu międzynarodowym przejawia się jedynie przez udział w konferencjach o zasięgu międzynarodowym.

4. **Wykazywanie się istotną aktywnością naukową albo artystyczną realizowaną w więcej niż jednej uczelni**

W mojej ocenie kryterium związane z wykazaniem się przez Habilitanta istotną aktywnością naukową w więcej niż jednej uczelni jest spełnione w stopniu wystarczającym. Przebieg kariery naukowej Habilitanta wskazuje na zatrudnienie na stanowisku badawczo-dydaktycznym (adiunkta) w Wojskowej Akademia Techniczna (WAT) w Warszawie. Równocześnie był zatrudniony na stanowisku eksperta ds. cyberbezpieczeństwa w Naukowej i Akademickiej Sieci Komputerowej (NASK)- Państwowym Instytucie Badawczym. Podczas zatrudnienia

w wymienionych wyżej jednostkach naukowych Habilitant oblikował szereg prac naukowych (także w ramach cyklu publikacji podlegających ocenie) afiliując je zarówno do WAT (prace [H1-H4]) jak i do NASK ([H5-H7]).

5. Podsumowanie i ocena końcowa

Na podstawie wyników badań naukowych zawartych w przedstawionym do oceny cyklu powiązanych tematycznie publikacji, całokształcie dorobku naukowego Habilitanta, informacjach o działalności dydaktycznej i organizacyjnej oraz wykazywaniu się istotną aktywnością naukową realizowaną w więcej niż jednej uczelni stwierdzam, że dr Michał Wroński posiada kwalifikacje do samodzielnej pracy naukowej. Uzyskane przez Habilitanta osiągnięcia naukowe stanowią istotny wkład badawczy dla informatyki w obszarze zastosowania wyżarzania kwantowego w kryptologii. Dodatkowo liczba cytowań i potencjalne liczne zastosowania uzyskanych wyników badań naukowych w praktyce sprawiają, że przedstawiony do oceny cykl publikacji stanowiący podstawę ubiegania się o stopień doktora habilitowanego oraz dorobek Habilitanta mieszczący się w dyscyplinie Informatyka Techniczna i Telekomunikacja spełnia ustawowe oraz zwyczajowe wymagania dotyczące habilitacji określone w art.219 ust.1 pkt 2 Ustawy z dnia 20 lipca 2018 r., „Prawo o szkolnictwie wyższym i nauce" (Dz.U. z 2022 poz.574 ze zm.) i wnoszę o dopuszczenie dr. Michała Wrońskiego do dalszych etapów postępowania habilitacyjnego.

Mariusz Uchroński