prof. dr hab. Wojciech Bożejko
Kierownik Katedry Automatyki, Mechatroniki
i Systemów Sterowania
Wydział Informatyki i Telekomunikacji
Politechnika Wrocławska
Wyb. Wyspiańskiego 27
50-370 Wrocław

Wrocław, 25 kwietnia 2025 r.

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

Przedmiotem niniejszej recenzji jest ocena osiągnięcia naukowego oraz istotnej aktywności naukowej dr. Michała Wrońskiego w związku z przewodem habilitacyjnym prowadzonym przez Radę Dyscypliny Informatyka Techniczna i Telekomunikacja w Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego. Podstawą formalną sporządzenia recenzji było zlecenie Przewodniczącego Rady Dyscypliny prof. Zbigniewa Tarapaty, wyrażone w piśmie z dnia 12.02.2025 (wpłynęło do Politechniki Wrocławskiej 28.02.2025) oraz Uchwale Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego z dnia 14.01.2025 r.

Recenzja została sporządzona w oparciu o przesłane materiały obejmujące cykl publikacji powiązanych tematycznie pt. *„Zastosowanie wyżarzania kwantowego w kryptologii”*, Autoreferat oraz wykaz opublikowanych prac naukowych po uzyskaniu stopnia doktora, a także informacje o współpracy z otoczeniem społecznym i gospodarczym i informacje naukometryczne. Przedstawiona dokumentacja, w której Autoreferat obejmuje 42 strony, oraz uzupełniające źródła 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”*.

Dr Michał Wroński jako osiągnięcie naukowe, mające być podstawą postępowania habilitacyjnego, przedstawił cykl 7 publikacji naukowych, w tym 3 posiadających 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).

Głównym celem badań, które doprowadziły do powstania tych publikacji, było poszukiwanie odpowiedzi na pytania o:

1. górny limit rozmiaru danych dla klasycznych algorytmów asymetrycznych w kontekście możliwości deszyfracji przy użyciu istniejącej infrastruktury wyżarzaczy kwantowych, a także
2. potencjalne zastosowanie kwantowych wyżarzaczy w kryptoanalizie w kontekście symetrycznych algorytmów szyfrujących.

W efekcie opracowane zostały nowe metody rozwiązywania problemów kryptograficznych, dla niewielkich rozmiarów danych, zarówno przy użyciu kwantowego wyżarzania (prace [H3], [H5], [H6]), jak i poprzez podejście hybrydowe oparte na sitach (przy użyciu obliczeń klasycznych i kwantowych, prace [H1], [H4]).

Czasopisma, w których opublikowane zostały prace [H2], [H6] oraz [H7] posiadają *Impact Factor* (prace [H2] i [H7] wysoki, ponad 5) i plasują się w tematyce informatycznej:

zastosowaniu adiabatycznych obliczeń kwantowych w kryptografii i cyberbezpieczeństwie. Pozostałe prace cyklu opublikowane zostały w czasopiśmie Journal of Telecommunications and Information Technology (bez wskaźnika *Impact Factor*) oraz materiałach konferencyjnych (prace [H1], [H3], H[4]) konferencji ICCS. Warto zauważyć, że 2 z 7 prac stanowiących cykl jest publikacjami jednoautorskimi, a w pozostałych udział Habilitanta jest istotny lub wiodący.

Praca [H1] dotyczy wykorzystania środowiska obliczeń kwantowych D-WaveLeap do analizy możliwości ataku na problem logarytmu dyskretnego (DLP, *Discrete Logarithm Problem*) przy pomocy metod opartych na przesiewaniu, konkretnie z pomocą metody indeksu na krzywych eliptycznych (odmiana ECDLP, *Elliptic Curve Discrete Logarithm Problem*), z wykorzystaniem wyżarzania kwantowego. Praca jest jednoautorska. Habilitant wprowadza interesujący sposób potencjalnego wykorzystania maszyny kwantowej bazującej na sformułowaniu QUBO do kryptoanalizy. Wadą podejścia jest wykorzystanie środowiska D-Wave LeapHybridSolver, a nie natywnego kwantowego wyżarzania (D-WaveSampler). Środowisko hybrydowe *LeapHybrid* dostarczane przez firmę D-Wave oferuje daleko większe możliwość rozwiązywania całkiem sporych problemów niż czyste kwantowe wyżarzanie, jednak jest to osiągane za pomocą klasycznych solverów, a kwantowe wyżarzanie służy jedynie do podziału przestrzeni problemu na podprzestrzenie.[1] Mimo to, praca jest nowatorska pod względem podjętej problematyki, mimo że aktualne możliwości (zarówno teraz, jak i w 2021 roku, w trakcie powstawania pracy) nie pozwalają na rozwiązywania praktycznych rozmiarów przykładów za pomocą czystego kwantowego wyżarzania. Praca została opublikowana w materiałach konferencji ICCS 2021.

W artykule [H2] pokazano redukcję ataku algebraicznego na algorytm AES do postaci QUBO, co doprowadziło do sformułowania modelu QUBO, dla algorytmu AES-128, wykorzystującego około 30 000 zmiennych logicznych. Skupiono się na minimalizacji liczby zmiennych dla modelu QUBO szukając minimalnego systemu równań z minimalną liczbą jednomianów stopnia 2 spełniających warunki zadane przez model szyfrowania AES-128. Eksperymenty dla wybranych przykładów wykonano na maszynie D-Wave Advantage, której znalezienie prawidłowego rezultatu zajęło 18 minut. Pracę opublikowano w prestiżowym czasopiśmie *IEEE Transactions on Emerging Topics in Computing*.

W pracy [H3] zaproponowana została efektywna metoda redukcji problemu logarytmu dyskretnego do problemu QUBO, z wykorzystaniem $2n^2$ zmiennych logicznych, gdzie n jest (ustaloną) liczbą bitów reprezentacji binarnej ustalonego zakresu poddanego analizie (w pracy maksymalnie 16). Przeprowadzone badania eksperymentalne mają charakter studium przypadku, na wybranych instancjach problemu przeprowadzono procedurę poszukiwania logarytmu dyskretnego. Wyniki raczej nie podlegają uogólnieniu, ale wartościowe jest samo skonstruowanie eksperymentu wraz ze szczegółowym opisem procedury osadzenia (*embeddingu*) modelu QUBO na konkretnych kubitach architektury maszyny D-Wave.

Praca [H4] rozszerza wyniki pracy [H1] poprzez zastosowanie wyżarzania kwantowego, tym razem natywnego, opartego na solverze D-Wave *Advantage_system4.1*, do rozwiązywania

[1] C. McGeoch, P. Farre, W. Bernoudy, Hybrid Solver Service Advantage: Technology Update, Technical Report, 2020, https://www.dwavesys.com/ media/m2xbmlhs/14-1048a-a_d-wave_hybrid_solver_service_plus_advantage_technology_update.pdf.

problemu logarytmu dyskretnego poprzez wykorzystanie metody indeksu oraz metody faktoryzacji (zaczerpniętej z literatury) do poszukiwania relacji w sicie kwadratowym oraz metodzie indeksów. Wkład habilitanta polegał na zaproponowaniu tematyki pracy oraz opracowaniu części badań związanych z wykorzystaniem liczb gładkich (*B-smooth numbers*). Jest to praca dwuautorska opublikowana w materiałach konferencji ICCS 2023.

Praca [H5] dotyczy realizacji metody rozwiązywania problemu logarytmu dyskretnego na strukturze krzywych eliptycznych poprzez przekształcenie problemu do modelu QUBO. Pokazano, jak wydajnie wykonać taką transformację przy użyciu liczby zmiennych logicznych (kubitów logicznych) rzędu $3n^3$ dla przypadku krzywej Edwardsa. Z kolei problem logarytmu dyskretnego logarytmu w podgrupie multiplikatywnej nad ciałem skończonym wymagał liczby zmiennych rzędu $2n^2$, co zostało pokazane na przykładzie studium przypadku o niewielkim rozmiarze (gdyż taki dał się jeszcze policzyć na maszynie D-Wave).

Praca [H6]. Wynik uzyskany w pracach [H3] oraz [H5] został poprawione w pracy [H6] przy użyciu odmiennej niż binarna reprezentacji wykładnika (krotności punktu). Zaproponowaną metodę przetestowano na niewielkim przykładzie DLP nad ciałem F_p (ciałem prostym o charakterystyce p), konkretnie F_{47}, polegającym na wyznaczeniu y takiego, że $2^y \equiv 36 \bmod 47$, oraz na przykładzie ECDLP nad ciałem F_{13}. Te studia przypadku nie tyle potwierdziły skuteczność zaproponowanej metody (gdyż dwa testy nie wystarczą do statystycznego uzasadnienie efektywności metody), ile zilustrowały zaproponowaną metodologię. Eksperymenty powtórzona dla dwóch architektur maszyny D-Wave: *Zephyr* oraz *Pegasus* wskazując istotne różnice w osadzeniu modelu QUBO dla różnych topologii maszyny.

Praca [H7] jest rozwinięciem wyników pracy [H2] opisująca efektywną redukcję do problemu QUBO ataku algebraicznego na szyfry strumieniowe Grain 128 oraz Grain 128a. Zaproponowano analizę szyfrów Grain 128 oraz Grain 128a oraz wprowadzono ulepszenia redukcji ataków na te szyfry do problemu QUBO. Zauważono także, że zaproponowana metoda będzie dla odpowiednio dużych instancji szyfru bardziej efektywna, zarówno od ataku przeglądu zupełnego (*brute force*) jak i ataku przy pomocy kwantowego algorytmu Grovera. Praca ma 3 autorów, wkład Habilitanta oceniam jako znaczący, a została zaakceptowana (*early access*, w momencie pisania recenzji nie ukazała się jeszcze wersja ostateczna) do opublikowania w czasopiśmie *IEEE Transactions on Emerging Topics in Computing*.

2. Podsumowanie oceny cyklu publikacji

Prace stanowiące cykl obejmują zakres przygotowania modelu QUBO oraz przeprowadzenia eksperymentów w formie analizy studium przypadku. Kolejność prac w cyklu jest przemyślana i odpowiada procesowi tworzenia przez Habilitanta własnej metodologii rozwiązywania problemów kryptograficznych na wyżarzaczach kwantowych poprzez transformację ich do modeli QUBO. Pewną wadą przedstawionych badań jest bardzo niewielki zakres wykonanych eksperymentów obliczeniowych, sprowadzających się do analizy jednego lub kilku przypadków o małych rozmiarach. Wyjątkiem jest tu prace [H2] oraz [H7] dotycząca

kryptoanalizy algorytmów AES-128 oraz Grain 128, mających wymiar praktyczny.

Mimo powyższych uwag należy podkreślić, że prace [H2], [H6] oraz [H7] należące do cyklu opublikowane zostały w czasopismach o dobrych i bardzo dobrych wartościach bibliometrycznych (*Impact Factor* nawet powyżej 5), dotyczących tematyki informatycznej. Istotne jest także, że 2 z 7 prac cyklu jest artykułami samodzielnymi.

Wśród nowych wyników przedstawionych w cyklu wyżej wymienionych publikacji warto wyróżnić rezultaty związane z opracowaniem:

i.) autorskiej metodologii konstrukcji modelu QUBO dla problemów DLP oraz ECDLP,

ii.) koncepcji wykorzystania wyżarzaczy kwantowych do kryptoanalizy algorytmów AES oraz Grain.

Konkludując ocenę wyżej wymienionych prac dr. Michała Wrońskiego uważam, że rezultaty uzyskane w cyklu powiązanych tematycznie publikacji, mimo pewnych uchybień (niewielka liczba eksperymentów na maszynie kwantowej niepozwalająca na analizę statystyczną wyników), są cenne poznawczo, zostały uzyskane metodami badawczymi opartymi na weryfikacji poprzez eksperymenty obliczeniowe lub analizę teoretyczną połączoną ze analizą przypadku oraz wnoszą istotny wkład w rozwój dyscypliny informatyka w zakresie realizacji algorytmów kryptoanalizy na maszynach realizujących paradygmat adiabatycznych obliczeń kwantowych. Przedstawione w nim artykuły prezentują konsekwentną pracę badawczą dotyczącą opisu, analizy i syntezy rozwiązań. Opublikowane prace zawierają oryginalne wyniki w zakresie omawianej problematyki. Uważam zatem, że przedstawiony cykl powiązanych tematycznie publikacji naukowych spełnia ustawowe i zwyczajowe wymagania stawiane rozprawom habilitacyjnym.

3. Ocena pozostałego dorobku naukowego po uzyskaniu stopnia doktora

Na pozostały dorobek Habilitanta, poza pracami składającymi się na cykl publikacji, składa się także:

- 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.

Podsumowując, pozostały dorobek habilitanta, poza cyklem publikacji, uzyskany po doktoracie, obejmuje 22 prace (w tym 12 posiadających wskaźnik *Impact Factor*) i 1 współautorski rozdział w monografii, plasując się tematycznie w dyscyplinie informatyka techniczna i telekomunikacja - obejmuje metody i algorytmy modelowania problemów z dziedziny szyfrowania.

Ocena bibliometryczna dorobku Habilitanta w postaci współczynnika Hirscha (*h-index*) jest na wystarczającym poziomie i wynosi 7 według Google Scholar (4 bez autocytowań). Wystarczająco dobra jest także sumaryczna liczba cytować (bez autocytowań) wynosząca

według Google Scholar 126 na dzień składania wniosku (60 bez autocytowań). Również sumaryczny *Impact Factor* dorobku Habilitanta, wynoszący ponad 21, należy uznać za dobry.

Podsumowując, oceniam całość dorobku naukowego Habilitanta jako znaczącą i stanowiącą wystarczającą podstawę do nadania stopnia doktora habilitowanego w dyscyplinie informatyka techniczna i telekomunikacja.

4. Ocena dorobku dydaktycznego i popularyzatorskiego oraz w zakresie współpracy międzynarodowej

Dr inż. Michał Wroński jest od 2011 roku związany jest z Wojskową Akademią Techniczną w Warszawie, gdzie przeszedł ścieżkę zawodową od młodszego inżyniera do adiunkta. W latach 2017–2023 jako adiunkt realizował wykłady, laboratoria oraz seminaria z zakresu kryptologii, matematyki dyskretnej, podstaw informatyki oraz cyberbezpieczeństwa. W ramach swojej działalności dydaktycznej współtworzył programy nauczania, dostosowując je do dynamicznych zmian w dziedzinie kwantowych metod obliczeniowych i kryptografii.

Habilitant jest również zaangażowany w projekty badawcze o znaczeniu międzynarodowym. W ramach konsorcjum składającego się z Akademii Górniczo-Hutniczej, Wojskowej Akademii Technicznej, Uniwersytetu Jagiellońskiego, NASK–PIB oraz Instytutu Informatyki Teoretycznej i Stosowanej PAN, współuczestniczył w przygotowaniu wniosku projektowego do programu „Perun", dotyczącego oceny odporności algorytmów kryptograficznych na ataki z wykorzystaniem wyżarzania kwantowego. W projekcie tym odpowiada za analizę algorytmów symetrycznych i asymetrycznych w kontekście nowoczesnych zagrożeń kwantowych.

Dr Wroński wypromował 5 prac inżynierskich oraz 12 prac magisterskich. Był promotorem pomocniczym w 1 zakończonych przewodzie doktorskim, aktualnie pełni tę funkcję w 3 otwartych przewodach doktorskich.

Z kolei współpraca międzynarodowa Habilitanta nie rozwinęła się jeszcze i jak na razie wyraża się w uczestnictwie w konferencjach o zasięgu międzynarodowym.

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

W ciągu swojej kariery naukowej dr Wroński był zatrudniony na stanowisku badawczo-dydaktycznym (adiunkta) w Wojskowej Akademia Techniczna (WAT) w Warszawie. Równocześnie pracował także w Naukowej i Akademickiej Sieci Komputerowej (NASK)-Państwowym Instytucie Badawczym, będąc zatrudnionym na stanowisku eksperta ds. cyberbezpieczeństwa. Opublikował szereg artykułów naukowych (w tym w ramach cyklu publikacji przedstawionych jako osiągnięcie habilitacyjne) z afiliacjami zarówno do pierwszej (prace [H1-H4]), jak i drugiej z wymienionych instytucji ([H5-H7]). Fakt ten uważam za wystarczający do stwierdzenia istnienia wymaganej przez Ustawę aktywności naukowej realizowanej w więcej niż jednej uczelni. Choć nie jest to aktywność w uczelniach zagranicznych, jednak kryterium niniejsze uważam za spełnione w stopniu wystarczającym.

5. Podsumowanie i ocena końcowa

Uwzględniając wyniki zawarte w przedstawianym cyklu publikacji powiązanych tematycznie oraz całokształcie dorobku naukowego Habilitanta, a także informacje o Jego pracy 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 Niego osiągnięcia naukowe stanowią istotny wkład badawczy dla informatyki w obszarze zagadnień związanych z algorytmami kryptograficznymi bazującymi na platformach obliczeń kwantowych. Słabą stroną Habilitanta jest brak współpracy międzynarodowej.

Ponadto liczba cytowań i potencjalne liczne zastosowania Jego metodologii w praktyce sprawiają, że 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.

Wojciech Bożejko