Zielona Góra , 28.10.2019

Recenzja osiągnięcia habilitacyjnego **"Wybrane, wzajemne relacje miedzy nielokalnością Bella , kontekstualnością , kluczem kryptograficznym bezpiecznym względem kwantowego adwersarza i kwantowym splątaniem"** (współ)-autorstwa **dra Karola Horodeckiego** i będącego monotematycznym cyklem publikacji oraz ocena jego dorobku naukowego.

Recenzję wykonano na zamówienie Centralnej Komisji ds. Stopni i Tytułów w związku z powołaniem mnie w dniu 05.09 .2019 na recenzenta tej rozprawy.

1. ***Tematyka rozprawy : jej aktualność i znaczenie*** .

Z punktu widzenia fundamentu klasycznej teorii obliczeń czyli klasycznego rachunku 0-1 predykatów, uniwersalnie implementowalnego jako klasyczna algebra Boola , odkrycie kwantowej teorii informacji /obliczeń nastąpiło (wedle wielu badaczy) w momencie zauważenia [G. Birkhoff and J. von Neumann, *The Logic of Quantum Mechanics, *Annals of Mathematics, Vol. 37, pp. 823-843, 1936]* że na gruncie mechaniki kwantowej odpowiedni, kwantowy rachunek 0-1 predykatów nie ma (w ogólności) implementacji na gruncie klasycznych algebr Boola ale w ogólności za pomocą ortomodularnych logik kwantowych będących uogólnieniem klasycznych algebr Boola a które to logiki kwantowe ,zgodnie z tw. Gleasona można reprezentować poprzez kraty domkniętych podprzestrzeni na ośrodkowych przestrzeniach Hilberta. Jest to też zgodne z tym, ze w przypadku dwóch niekomutujących operatorów normalnych nie istnieje w ogólności łączna miara spektralna dla nich.

Dalszy postęp w teorii kwantowej informacji nastąpił w próbie uogólnienia tych wyników na przypadek dwu-częściowych układów kwantowych rozdzielonych w przestrzeni i znajdujących się we wspólnym stanie kwantowym, mających własność splątania. Dyskusje na temat interpretacji wyników pomiarowych wynikających ze splątania w kontekście przeprowadzania lokalnych pomiarów na takich układach trwały faktycznie już od lat 30tych .W przełomowej pracy irlandzkiego fizyka J.T. Bella [Bell, John (1964). "On the Einstein Podolsky Rosen Paradox" (PDF). *Physics*. **1** (3): 195–200]sformułowane zostały pewne warunki dotyczące lokalności i realizmu których spełnienie implikuje zachodzenie pewnych nierówności korelacyjnych zwanych nierównościami Bella . W przypadku najprostszych scenariuszy dotyczących kwantowych układów qubitowych złożonych z dwóch części i pomiarów lokalnych obserwabli 0-1 -kowych , po dwie na każdej z części ,tzw . klasa (2,2,2) układów J.T. Bell udowodnił , że jeżeli warunki lokalnego realizmu zachodzą to odpowiednie funkcje korelacyjne spełniają pewna nierówność zwana dzisiaj nierównością Bella (lub równoważnie nierówność CHSH). Przez bezpośredni rachunek ,możliwy do przeprowadzenia np. w przypadku układów qubitowych i wielu stanów kwantowych można obliczyć na gruncie formalizmu mechaniki kwantowej wartość tych korelacji dokładnie i stwierdzić przez te obliczenia ze nierówności korelacyjne Bella są w stanach rdzennie kwantowych (splątanych) na ogół łamane. Jak zauważył Fine [Fine, A. ,(1982) , Hidden variables , Joint Probability , and the Bell inequalities ,Phys. Rev. Lett. 48(5), 291-295] korelacje statystyczne w takich układach qubitowych spełniają odpowiednie nierówności korelacyjne Bella tylko wtedy kiedy istnieją łączne rozkłady prawdopodobieństw dla czterech obserwabli/predykatów pojawiających się tym kontekście , a to w pewnym sensie jest warunkiem na istnienie łącznej miary spektralnej dla czwórki parami komutujących obserwabli (struktura iloczynu tensorowego łącznej przestrzeni stanów).Matematycznie obraz jaki tu się pojawia to wypukły zbiór 16d opisujący wszystkie możliwe wyniki pomiarów dla ustalonego scenariusza jak wyżej ale indeksowany wszystkimi możliwymi stanami kwantowymi badanego układu (2,2,2). Daje to *pewien wypukły podzbiór w przestrzeni 16d Zachowań zwany zbiorem zachowań kwantowych .Zbiór* Zachowań spełniających warunki Bella stanowi wielościan wypukły zawarty w zbiorze zachowań kwantowych którego ściany określają

właśnie nierówności korelacyjne Bella. Struktura wielościanu Bella w tym przykładzie (np. zbiór wierzchołków opisujących Zachowania klasyczne ekstremalne)są dobrze znane. W słynnej pracy Tsirelsona [B. S. Cirel'son, *Quantum Generalizations of Bell's Inequality*, Lett. Math. Phys. 4, 93 (1980).] oszacowano z góry korelator Bella (zwany tez w tym kontekście jako nierówność CHSH)na przestrzeni wszystkich Zachowań Kwantowych układu typu (2,2,2). Stanowi to wartość maksymalnego łamania nierówności Bella dla takich układów kwantowych i scenariusza pomiarów jak wyżej opisano.

Wszystkie te rozważania jak wyżej ,opisane dla układów (2,2,2) można rozwinąć w wielu kierunkach . Można np. rozważać układy kwantowe złożone z większej ilości części , układy o wyższych spinach (qudity) czy tez z większa liczba lokalnych pomiarów wykonywanych na jego częściach. Można też rozszerzyć je przez podanie dowodów maksymalnego łamania nierówności Bella na przypadek stanów próżniowych kwantowych układów nieskończenie-wymiarowych , w tym na przypadki oddziałujących pól kwantowych.

Inny obszar uogólnień dotyczy prób wyjścia poza Zachowania Kwantowe ,ale zachowania spełniające (co wydaje się mocno kontrowersyjne) warunek lokalności w sensie STW (Szczególna Teoria Względności).Takie Zachowania nazywa się Zachowaniami pod-świetlnymi (non-signaling Behaviours , tez spotykane nazewnictwo w polskojęzycznej literaturze :Zachowania niesygnalizujące).Oczywiście każde Zachowanie Kwantowe spełnia warunki pod-świetlności . Chociaż matematycznie taka konstrukcja nie budzi kontrowersji to powstaje jednakowoż pytanie o ich fizyczne istnienie –to znaczy o odpowiedz na pytanie czy w ogóle w Świecie Rzeczywistym istnieją tak zachowujące się układy i nie będące układami kwantowymi w sensie standardowej definicji Zachowania Kwantowego .Tak zdefiniowany zbiór zachowań pod-świetlnych jest wielościennym podzbiorem wypukłym wszystkich możliwych (matematycznie) Zachowań probabilistycznych dla zadanego układu i scenariusza pomiarów .W ostatnim okresie można zaobserwować spora aktywność badawczą związaną czy to z zastosowaniem Zachowań pod-świetlnych do różnego rodzaju zagadnień numerycznych formułowanych dla Zachowań kwantowych (np. dobrze znane scenariusze relaksacji liniowych typu NPA (Navascues,...i inni) do rozwiązywania zadań optymalizacji nieliniowych związanych z łamaniem nierówności Bella na zbiorach Zachowań Kwantowych) czy tez bezpośrednie próby uogólnienia znanych pojęć ,własności i konstrukcji znanych w kontekście Zachowań kwantowych stricte.

Najlepiej zbadana jest sytuacja w przypadku układów typu (2,2,2). Zbiór wierzchołków wielościanu zachowań pod-świetlnych składa się z 24 wierzchołków , w tym 16 spełniających warunki LHV Bella (tzw. pudełka lokalne) i 8 wierzchołków (zwanych pudełkami Popescu- Rohlicha) nielokalnych. Znane są warunki konieczne i dostateczne na to żeby dane Zachowanie pod-świetlne było nielokalnym zachowaniem. Wiele wątków przedstawionej rozprawy habilitacyjnej dotyczy uogólnień pojęć , konstrukcji ,.... znanych w kontekście Zachowań kwantowych na zachowania pod-świetlne (chociaż wydaja się one nie fizyczne !) ale niekwantowe ale mające potencjalne zastosowania w kwantowych protokołach kryptograficznych (o czym pisze wyraźniej w następnym paragrafie przy prezentacji wyników zawartych w przedstawionym osiągnięciu.

Większość wyników uzyskanych w rozprawie habilitacyjnej dra Karola Horodeckiego dotyczy analizy właściwości i zagadnień kwantowych kierowanych głównie w kierunku Kwantowej Teorii Komunikacji ,której zwieńczeniem (na dzisiaj przewidywalnym) ma być realizacja projektu zwanego Kwantowym Internetem [Wehner et al. ,Quantum Internet : A vision for the road ahead , Science 362, 2018] .Aktualnie istnieje wiele różnego rodzaju studiów oraz badan nad możliwością implementacji sprzętowej wielu pomysłów dotyczących konstrukcji Kwantowego Internetu. To co wydaje się najbardziej znane w ramach tych aktywności dotyczy prób stworzenia nowej jakości ,jeżeli chodzi o poziom bezpieczeństwa transferu danych poprzez Internet Kwantowy. Jakości gwarantującej absolutne bezpieczeństwo w odróżnieniu od obecnie stosowanych protokołów klasycznych. A które to , nawet po eliminacji wielu luk związanych z sama fizyczna ich implementacja dają bezpieczeństwo jedynie warunkowe .Ażeby to zrealizować zaproponowano wiele rożnych wersji protokołów Kwantowych

Transferów Kluczy (QKD protokoły),ale jak zauważono już w pierwszym okresie konstruowania tych technologii każda ich rzeczywista implementacja była łatwa !! do "zhakowania". Zademonstrowano wiele udanych ataków na implementacje QKD atakując na różne sposoby detektory fotonowe bezpośrednio. Podano nawet możliwości wykorzystania splatania typu spin-orbita w funkcji falowej fotonów do realizacji wiązki fotonów klasycznych !! dla której zachodzi zjawisko łamania nierówności Bella (światło klasyczne !!). Ażeby ominąć tego rodzaju słabości związane z możliwością ataku na same urządzenia generujące i odbierające klucze zaproponowano schematy i protokoły zwane Device Independent QKD (DIQKD) czy tez trochę mniej wymagające technologicznie semi-DI QKD , gdzie nad bezpieczeństwem transferów w założeniu ma czuwać mechanizm łamania warunków LHV Bella. Ale i to było /jest wyzwaniem bo jak wiadomo pomiary związane z łamaniem nierówności Bella cierpiały przez wiele dziesięcioleci na różne słabości , z których najdłużej przetrwały luki związane z brakiem odpowiednich technologii jednofotonowych .Dwie podstawowe luki w badaniach nad korelacjami Bella to tzw. luka związana z lokalnością (locality loop-hole) oraz luka związana z możliwością podsyłania fałszywych fotonów (tzw. Fair sampling- loophole). Warto podkreślić że przy malej efektywności źródeł generujących splątane pary fotonów do wpływu na korelacje miedzy pomiarami mogą się dołączyć jeszcze zjawiska związane z absorpcja nawet pojedynczych fotonów w kanałach transmisyjnych.

Zagadnienia będące przedmiotem analiz i rozszerzeń przedstawionego osiągnięcia habilitacyjnego dra Karola Horodeckiego można ulokować gdzieś na styku współczesnej i bieżącej Informatyki Kwantowej oraz podstaw Teorii Kwantowej (z punktu widzenia fizyki). Z tego powodu bezsprzecznie są one bardzo aktualne i mające duży potencjał poznawczy ,a także co jest warte szczególnego podkreślenia dające spore możliwości ulepszenia istniejących (prototypów) podwalin Komunikacji Kwantowej od strony praktycznej

.

2. Opis oryginalnego osiągnięcia .

Przedstawiona rozprawa habilitacyjna dra Karola Horodeckiego stanowi bardzo rozległy problemowo ale spójny tematycznie cykl siedmiu artykułów (które są zaprezentowane poniżej bardziej szczegółowo) poświęconych fundamentalnym aspektom i zagadnieniom informatyki kwantowej i które zostały w większości napisane we współpracy z wieloma innymi, wiodącymi badaczami z tego obszaru. Pomimo wielu rożnych wątków badawczych udało się drowi Karolowi Horodeckimi znaleźć wspólne spoiwo koncepcyjne przez użycie którego udało mu się w sposób koherentny opisać w swoim , dołączonym do wniosku habilitacyjnego autoreferacie swoje bogate osiągnięcia badawcze. Spoiwem które zespoliło , na pierwszy rzut dość luźno powiązany tematycznie cykl przedstawionych publikacji jako osiągniecie habilitacyjne publikacji jest abstrakcyjna teoria zasobów .

Dobrze znany przykład zasobu kwantowego to np. splątanie kwantowe , ciągle jeszcze dalekie od ostatecznego sformułowania i kompletnego zrozumienia pomimo gigantycznego wysiłku włożonego w tym obszarze, przez setki a nawet tysiące badaczy w ostatnich dziesięcioleciach. Jedna z miar ilości splatania często używana w przedstawionym osiągnięciu jest tzw. (jego ilość) splątanie destylowane wprowadzone do Informatyki Kwantowej już w latach 90-tych którego miarą dualna jest koszt uzyskania splatania . Główne zasoby kwantowe badane przez Autora dysertacji habilitacyjnej (zwanej tez osiągnięciem habilitacyjnym) to: splątanie kwantowe ,nielokalność typu Bella , bezpieczny (względem ataków kwantowych) klucz kryptograficzny oraz zasób zwany kontekstualnością kwantowa jak tez kontekstualnością poza-kwantowa (patrz poniżej).Głębokie związki , analogie ,... pomiędzy takimi zasobami jak splatanie kwantowe i, nielokalność Bella czy też bezpieczeństwem protokołów kryptograficznych (bezpieczeństwo klucza)są dobrze znane w kontekście Kwantowej Kryptografii w szczególności przy ocenach poziomu bezpieczeństwa w zadanych implementacjach protokołów typu (semi - DI) -QKD .Tego typu zależności i podobieństwa są od lat badane i istnieje na dzień dzisiejszy potężna literatura ich się tycząca .Mniej znana i mniej eksploatowana jest

zinterpretowana w przedstawionej dysertacji jako zasób kwantowy kontekstualność kwantowa i jej uogólnienia na zachowania pod-świetlne (niesygnalizujące) i niekoniecznie kwantowo-mechaniczne .

Związki , analogie i podobieństwa pomiędzy niektórymi zasobami wokół których jest skoncentrowana treść przedstawionej dysertacji były badane przez dra Karola Horodeckiego już w pracach wykonanych i opublikowanych przez niego i szereg jego współautorów w trakcie przygotowywania przez niego rozprawy doktorskiej i po jej obronie (w roku 2009).Praca doktorska dra Karola Horodeckiego dotyczyła analizy związków zachodzących pomiędzy splataniem kwantowym a bezpieczeństwem (względem ataków kwantowych) na znane protokoły QKD , także tych znanych jako (semi)-DI wersje .Inny zasób który w tym kontekście się pojawił już w pracy doktorskiej to zdefiniowane na gruncie termodynamiki kwantowej pojęcie tzw. kwantowej czystości traktowanej jako zasób kwantowy związany ze splątaniem i co z a tym idzie z bezpieczeństwem transferu klucza kryptograficznego. Klasa dopuszczalnych operacji wykonywalnych na stanach była ograniczona w przypadku analiz przedstawionych w rozprawie doktorskiej i wokół niej do klasy operacji LOKK. Wydaje się , że główny watek rozprawy doktorskiej dotyczył problemu trudnej odróżnialności stanów kwantowych bezpiecznych dla implementacji QKD od stanów separowalnych.

Przedstawiona rozprawa habilitacyjna której główne wyniki są opublikowane w siedmiu (przedstawionych subiektywnie i niekompletnie przeze mnie z powodów oczywistych) poniżej artykułach (Artykuł 1-Artykuł 7) napisanych we współpracy z wieloma innymi badaczami (w sumie naliczyłem ich czternastu) stanowi owoc (a właściwie jego cześć wyselekcjonowaną przez dra Karola Horodeckiego)prawie dziesięcioletnich badań nad rozszerzeniem i pogłębieniem wyników badan realizowanych wokół rozprawy doktorskiej o których wspomniałem w poprzednim akapicie .Jeden z ważniejszych elementów tego rozszerzenia to dołączenie do badań w sposób bardziej wyrazisty jednego z najważniejszych przejawów kwantowości jakim jest niewątpliwie zasób związany z nielokalnością Bella i to na poziomie zachowań pod-świetlnych , ale poza-kwantowych .Inny zasób kwantowy który odgrywa ważną role w przedstawionej dysertacji to ciągle jeszcze budzący wiele kontrowersji [R.B. Griffiths, Quantum Measurements and Contextuality , arxivv:1902.05633v2]zasób zwany kontekstualnością kwantowa i tez jego rozszerzenia na poziom Zachowań pod-świetlnych ,ale niewantowych . Wypracowanie adekwatnych definicji miar rozszerzonych , nowych zasobów kwantowych i poza-kwantowych wymagało wiele wysiłków i czasu . Przedstawione , w większości przypadków nowe konstrukcje ilościowych miar dla badanych zasobów oraz ich dualnych miar w postaci miar kosztów ich uzyskania wydaja się być najważniejszymi wynikami przedstawionej dysertacji. Nie było to łatwe zadanie tak z punktu widzenia matematyki jak i spełnienia wielu naturalnych wymagań jakie stawia teoria kwantowa tego rodzaju miarom.

Ażeby dać pewien posmak poziomu wyrafinowania przedstawionej dysertacji przedstawię poniżej , bardzo subiektywny i wybiorczy przegląd treści i najważniejszych wyników stanowiących treść przedstawionej dysertacji .

Artykuł 1.

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 63, NO. 9, SEPTEMBER 2017

On Distinguishing of Non-Signaling Boxes viaCompletely Locality Preserving Operations

By : **Karol Horodecki**

W tej pracy ,napisanej samodzielnie pan dr Karol Horodecki analizuje pewne ważne konceptualnie aspekty Zachowań pod-świetlnych (hipotetycznych ! bo ciągle nie znamy rzeczywistych układów fizycznych które zachowują się taki sposób i są różne od znanych układów kwantowych) układów typu (2,2,2). W szczególności Autor wprowadził pewna klasę odwzorowań na przestrzeni Zachowań ,nazwanych (w analogii to sytuacji znanych na poziomie Zachowań kwantowych jako odwzorowania Zupełnie Dodatnie) odwzorowaniami Zupełnie Zachowującymi Lokalność (klasa CLP) jako te które przekształcają wielościan Zachowań Bella w siebie i spełniających dodatkowo warunek matematyczny ze iloczyn tensorowy tej operacji z identycznością zachowuje tez warunki lokalności i realizmu Bella. Główny wątek pracy skoncentrowany był na zadaniu (probabilistycznej)

odróżnialności Zachowań pod-świetlnych , poza- kwantowych za pomocą operacji klasy CLP. To zadanie zostało sprowadzone do problemu numerycznego Programowania Liniowego za specjalnie skonstruowana do tego zadania liniowa funkcja kosztów , który to problem numeryczny w pewnych , specjalnych sytuacjach zostały pomyślnie zrealizowany i wyniki obliczeń w przypadku małej ilości rozkładów pod-świetlnych , izotropowych opisujących układy typu (2,2,2) przedstawione detalicznie.

Artykuł 2.

PHYSICAL REVIEW A **92**, 032104 (2015) ,**Axiomatic approach to contextuality and nonlocality** , By :Karol Horodecki, Andrzej Grudka, Pankaj Joshi, Waldemar Kłobus, and Justyna Łodyga

W tej pracy zaproponowano podejście aksjomatyczne do (ciągle jeszcze , zobacz np. [R.B. Griffiths, Quantum Measurements and Contextuality , arxivv:1902.05633v2] ,chociaż o tradycji sięgającej początków teorii kwantowej) zjawiska kontekstowości kwantowej zinterpretowanego jako zasób kwantowy . W analogii do analizy z tegoż punktu widzenia zachowań pod-świetlnych wprowadzano nowa klasę operacji z pomocą których wprowadzona została pewna metryka na przestrzeni rozważanych Zachowań która spełnia wszystkie naturalne oczekiwania z nią związane .Skonstruowana metryka posłużyła do udowodnienia asymptotycznej ciągłości , wprowadzonej w tym artykule (ale także w Artykule 5 tej serii) miary ilości kontekstualności w topologii wyznaczonej przez te właśnie metrykę. Wprowadzona miara kontekstualności została skonstruowana w oparciu o pewne analogie ze znanymi , bazującymi na pojęciu entropii względnej miarami splatania stanów kwantowych . Wiele rozważań i wyników zostało uzyskane w drodze dedukcji z zaproponowanego podejścia aksjomatycznego do rozwazanego zasoby kontekstualności i z tego powodu zawiera spory potencjał na ciekawe zastosowania do badania w oparciu o niego inne , mniej znane zasoby czysto kwantowe.

Artykuł 3.

PHYSICAL REVIEW A 92, 010301(R) (2015)Bounds on quantum nonlocality via partial transposition, **Karol Horodecki** and Gl´aucia Murta

Analizowany jest związek pomiędzy poziomem łamania nierówności Bella a trudnością odróżnienia od siebie dwóch stanów kwantowych za pomocą wybranej , ograniczonej klasy operacji typu LOKK . W pracy podano bardzo ciekawe oszacowanie górne na poziom łamania nierówności Bella w zależności od stopnia trudności odróżnienia od siebie dwóch stanów kwantowych za pomocą operacji wybranej klasy. Na bazie tych rozważań wprowadzono pojecie asymptotycznej entropii nielokalności i udowodniono ciekawe oszacowania górne na jej wartość . W szczególności dla stanów splatanych typu PPT otrzymano oszacowanie górne w terminach względnej entropii splatania stanu częściowo transponowanego .Otrzymane wyniki z zastosowano w kontekście bezpieczeństwa klucza w ramach schematów bazujących o DI-QKD protokół.

<u>Artykuł 4.</u>

Nature Communication DOI: 10.1038/ncomms7908,Limitations on quantum key repeaters ,Stefan Ba¨uml ,Matthias Christandl, **Karol Horodecki**, Andreas Winter.

Jak dobrze wiadomo jednym z głównych elementów sukcesu związanego z implementacja rzeczywista klasycznych sieci rozległych są różnego rodzaju techniki odszumiania i wzmacniania przesyłanych sygnałów klasycznych. W przypadku klasycznym istnieje wiele rozwiązań dotyczących pośrednich wzmacniaczy sygnałów tzw. klasycznych Powtarzaczy (repeaterow , wzmacniaczy)).Z drugiej strony pojawienie się kwantowych protokołów transferu kluczy kryptograficznych (gwarantujących absolutne bezpieczeństwo transferu w wersji teoretycznej) jak np. protokol BB84 czy też protokół Eckerta E91 spowodowało ogromne zainteresowanie i ogromna aktywność w obszarze kwantowej komunikacji. Znane z początków Kwantowej Informatyki wyniki typu No Cloning [W.K. Wooters, W.H. Zurek ,"A single quantum cannot be cloned ". Nature 299 (1982),str. 802-803] sugerowały ,że ażeby przezwyciężyć jeden z podstawowych defektów implementacji protokołów typu QKD (mianowicie ich krotki zasięg ze względu na szumy kwantowe)czyli skonstruować kwantowe odpowiedniki klasycznych Powtarzaczy będzie trzeba dokonać swoistego przełomu :

W. Dür, H.-J. Briegel, J. I. Cirac i P. Zoller. „Quantum repeaters based on entanglement purification". *Phys. Rev. A* 59 (1999), s. 169–181. arXiv: quant-ph/9808065.

.Jak wiadomo typowy kwantowy powtarzacz sygnału powinien mieć zaimplementowany w swojej konstrukcji oprócz odpowiedniego protokołu wymiany splatania (entanglement swapping) pomiędzy węzłami się

komunikującymi mieć także zaimplementowany protokół teleportacji do transferu kwantowej informacji. Inna słabością znanych dzisiaj protokołów QKD jest niemożność ich absolutnie sterylnego fizycznego urzeczywistnienia. Na dzień dzisiejszy wiadomo ,że wszystkie implementacje technologiczne znanych protokołów QKD są narażone na ataki. Nawet próby ominięcia tej trudności w postaci protokołów w ramach tzw. Device Independent ideologii bazującej na detekcji łamania nierówności Bella czy tez jej mniej wymagającej technicznie odmianie Semi- Device Independent protokołów QKD nie dały satysfakcjonujących wyników dających należyty poziom bezpieczeństwa transferów kluczy.Artykuł współautorstwa dra K. Horodeckiego jest teoretycznym studium na temat możliwości z zastosowania stanów mieszanych (z których będzie otrzymany klucz metoda destylacji splątania)w protokołach typu QKD i możliwości udanej implementacji kwantowych powtarzaczy w nich .Wyniki przeprowadzonej analizy są raczej negatywne i potwierdzają wcześniej znane wyniki dotyczące ogólnie twierdzeń typu No Cloning na przypadek transferowania i kopiowania nielokalności.

ARTYKUŁ 5.

PRL 112, 120401 (2014) PHYSICAL REVIEW LETTERS 28 MARCH 2014
Quantifying Contextuality ,A. Grudka, **K. Horodecki**, M. Horodecki, P. Horodecki, R. Horodecki, P. Joshi, W. Kłobus, and A. Wójcik

Jednym z ważniejszych zadań związanych z analiza pojęcia kontekstualności kwantowej jest skonstruowanie odpowiednich ilościowych miar kontekstualności i ich miar dualnych , miar kosztów badanej kontekstualności . Bazując na uderzającym podobieństwie zjawiska kwantowej kontekstualności zjawiska kwantowej nielokalności wprowadzono definicje bazująca na pomysłach entropijnych tak zwana względna entropię kontekstualności oraz miarę dualna do niej jako koszt kontekstualności .Pokazano naturalne własności wprowadzonych Miat , takie jak np. ich addytywność czy też monotoniczność. Drugie podejście do problemu za punkt wyjścia obiera pewne gry kwantowe gdzie kontekstualność a raczej jej ilość staje się naturalnie zdefiniowana i jak pokazali Autorzy pokrywa się ze wcześniejszą definicja bazująca na rozważaniach entropijnych .Podano także przykład explicite ,związany z dwiema grami kwantowymi rozważanej klasy gdzie możliwe było porównanie zasobów kontekstualności poprzez ich dokładne obliczenia w oparciu o zaproponowane definicje .

Artykuł 6.

Quantum Information and Computation, Vol. 13, No. 7&8 (2013) 0567{0582
c Rinton Press ,NO-BROADCASTING OF NON-SIGNALLING BOXES
VIA OPERATIONS WHICH TRANSFORM LOCAL BOXES INTO LOCAL ONES
P. JOSHIA , M.HORODECKI ,R. HORODECKI, A. GRUDKA ,**K. HORODECKI** ,P. HORODECKI

Bardzo ważnym problemem przy badaniu eksperymentalnym nielokalności Zachowań układów kwantowych jest poradzenie sobie z defektami transferu jakim są np. procesy absorpcji pojedynczych fotonów niosących sygnały kwantowe .W tym właśnie celu została zaproponowana metoda zwana rozglaszaniem (heralding)transferowanego fotonu. W artykule dyskutuje się problem (nie) –rozgłaszalności splątania kwantowego (bardzo ważnego mechanizmu w eliminacji luk związanych z badaniem łamania nierówności Bella czyli nielokalności) w przypadku transmisji związanej z pod-świetlnymi , nielokalnymi pudełkami o dwóch wejściach binarnych i dwóch wyjściach (hipotetyczne układy typu (2,2,2)).Główny wynik pracy to dowód że za pomocą operacji zachowujących wielościan lokalnych i realistycznych Zachowań nie da się rozgłosić transferu takiego nielokalnego pudełka .Czyli otrzymano wynik za taki zasób kwantowy jak nielokalność nie daje się za pomocą prostych operacji rozgłosić.

Artykuł 7.

PHYSICAL REVIEW A **85**, 012330 (2012)Q ,**Quantum privacy fitness,**Konrad Banaszek ,**Karol Horodecki**, Paweł Horodecki.

W analogii do koncepcji świadków splatania czy tez świadków nielokalności wprowadzono pojecie świadka prywatności czyli świadka bezpiecznego (względem ataków kwantowych) klucza kryptograficznego . W terminach skonstruowanego świadka prywatności podane zostały oszacowania od dołu na wielkość destylowanego (w danym scenariuszu)klucza destylowanego z danych stanów splątanych . Tego rodzaju wynik może być ważnym przyczynkiem do optymalizacji wielu technicznych implementacji (s)DI-QKD protokołów. Oszacowanie od dołu wielkości destylowalnego klucza sprowadza problem bezpieczeństwa klucza do małej ilości pomiarów dających oszacowania od

dołu na wielkość drugiego świadka prywatności , tzw. klucza bezpieczeństwa. Redukcja ilości niezbędnych pomiarów na stanie uzyskana dzięki tym oszacowaniom w stosunku do ilości pomiarów dla przeprowadzenia kompletnej tomografii badanego stanu splatanego jest znaczna i może to być zastosowane w praktyce . Podano przykład stanu 4-qubitowego gdzie przestawiona metoda redukuje problem oceny klucza destylowanego z 81 pomiarów (pełna tomografia) do zaledwie 6ciu pomiarów prostych obserwabli.

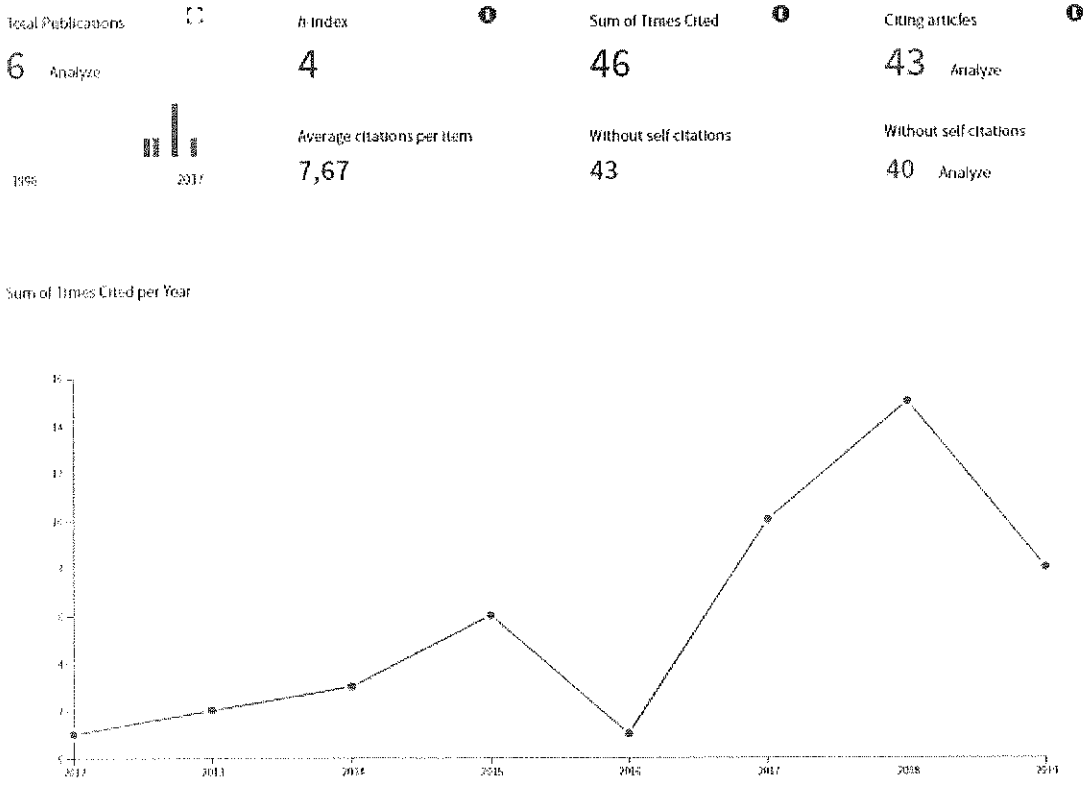
W podsumowaniu :

W przedstawionej serii publikacji zostało osiągniętych szereg bardzo ważnych i nietrywialnych wyników dotyczących wielu fundamentalnych problemów informatyki kwantowej jak też interdyscyplinarnych wyników na polach wspólnych z Fizyka Kwantowa .Wiele z tych wyników może (potencjalnie) znaleźć zastosowanie do realizacji i analiz ważnych projektów technologicznych takich jak np. Konstrukcja Internetu kwantowego.

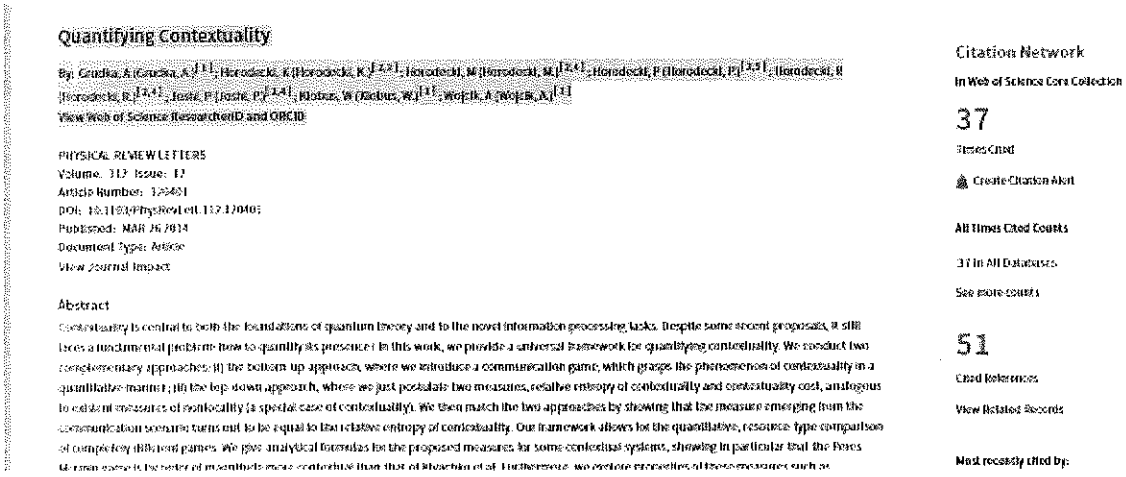
Do wniosku habilitacyjnego zostały dołączone certyfikowane oświadczenia wszystkich współautorów dotyczące ich wkładów w przedstawione publikacje . Z tych oświadczeń wynika jednoznacznie iż wkład do nich dra Karola Horodeckiego w zdecydowanej większości opublikowanych artykułów stanowiących przedstawiona dysertacje jest dominujący , a w pozostałych większościowy lub bardzo istotny. Aczkolwiek ,w wersji w której każdy ze współautorów (oprócz Autora wniosku) opisuje szczegółowo swój wkład merytoryczny do artykułu powoduje ,że recenzent chcący wydestylować rzeczywisty wkład dra K. Horodeckiego do każdego z przeglądanych artykułów stanowiących osiągnięcie habilitacyjne musi wykonać sporą dodatkową pracę . Ułatwieniem dla recenzenta byłaby sytuacja gdyby to Autor wniosku zamieścił potwierdzoną przez innych współautorów informację na temat swojego , osobistego wkładu w konkretny artykuł .

O wartości naukowej przedstawionej dysertacji habilitacyjnej dra Karola Horodeckiego świadczy niezbicie jakość czasopism w których przedstawione osiągnięcia badawcze zostały opublikowane . Prace te są chętnie czytane i (mimo ich „młodego wieku")cytowane .Poniżej przytaczam w dowód tego dane z bazy Web of Science na temat prac tworzących cykl będący dysertacja .

Rys.**1 Dane biblio-metryczne dotyczące 6-ciu publikacji cyklu (bez Artykułu 5)na bazie Web of science.**



Rys . 2 Praca „ Artykuł 5", najczęściej cytowana praca cyklu tworzącego dysertacje .



4. Podsumowanie dorobku naukowego.

Całe życie naukowe dra Karola Horodeckiego jest związane z aktywnością grupy badaczy skupionej wokół prof. Ryszarda Horodeckiego , grupy której aktywność naukowa , a zwłaszcza pionierskie i fundamentalne wyniki w wielu obszarach Informatyki Kwantowej są znane na całym Świecie . Pan Karol Horodecki ukończył studia magisterskie na Uniwersytecie Gdańskim uzyskując dyplom magistra matematyki (ze specjalnością informatyka i metody numeryczne) w roku 2004. Doktoryzował się na Wydziale Matematyki , Informatyki i Mechaniki Uniwersytetu

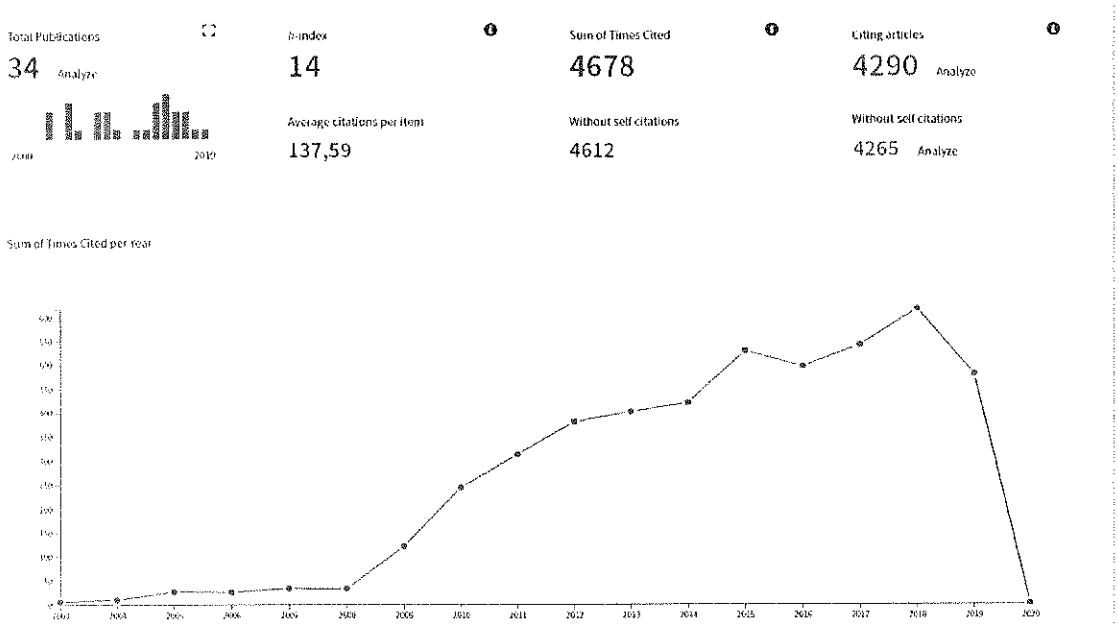
Warszawskiego w roku 2009 na podstawie przedstawione rozprawy doktorskiej dotyczącej ważnych zagadnień dotyczących wielu teoretycznych aspektów Kryptografii Kwantowej .Jednym z najważniejszych wątków badawczych tego okresu jego aktywności naukowej był bardzo ważny problem bezpieczeństwa (względem ataków kwantowych)transmisji klucza prywatnego w protokołach typu DI – QKD w zależności od poziomu (ilości splatania)splatania przetwarzanych stanów kwantowych.

Inny ciekawy wątek tego okresu dotyczy zagadnienia odróżnialności od siebie nieznanych stanów kwantowych za pomocą operacji typu LOKK. Warto jeszcze , omawiając aktywność naukową pana K. Horodeckiego w tym okresie zwrócić uwagę na wkład pana Karola Horodeckiego do jednej z najczęściej cytowanych w obszarze Informatyki Kwantowej pracy przeglądowej dotyczącej zjawiska kwantowego splatania [zobacz rys. 4 poniżej]napisanej w grupie prof. Ryszarda Horodeckiego. O wynikach zawartych w rozprawie doktorskiej tj . przede wszystkim analizie bezpieczeństwa klucza prywatnego w protokołach DI- QKD wspominałem już wcześniej.

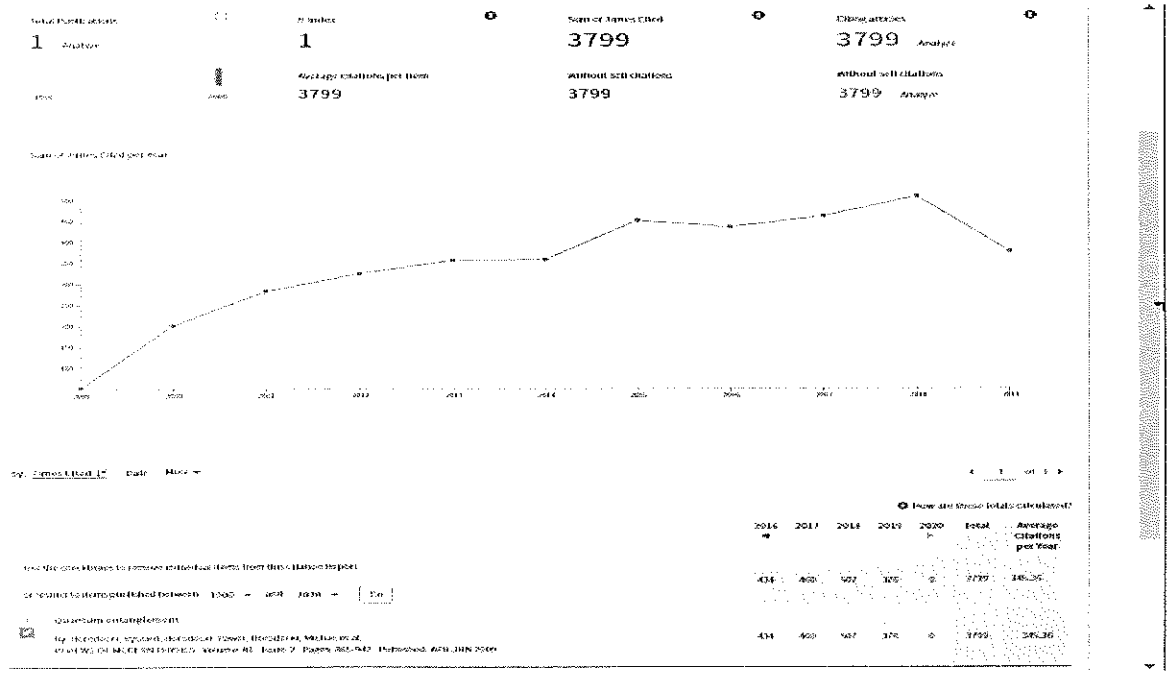
W sumie aktywność przed i wokół rozprawy doktorskiej zaowocowała jak podaje Autor autoreferatu opublikowaniem 14 ważnych artykułów , we współpracy z wieloma innymi badaczami dotyczących ważnych zagadnień Informatyki Kwantowej.

W okresie po doktoracie aktywność badawcza dra K. Horodeckiego koncentrowała się w dalszym ciągu głównie wokół zagadnienia związku bezpieczeństwa klucza prywatnego w zależności od ilości splatania .Pojawiły się w tym okresie także ważne badania dotyczące rożnych aspektów związanych z nielokalnością stanów kwantowych w oparciu o nierówności Bella . Nie sposób tutaj wymienić wszystkich osiągnięć w tym zakresie które nie znalazły swojego miejsca w przedstawionej dysertacji habilitacyjnej ,a które same w sobie stanowią bardzo interesujące wyniki. Także wiele ciekawych artykułów dotyczących kwantowej kontekstualności nie znalazło się w materiale dysertacji ale warto je mieć na uwadze .Aktywność badawcza dra Karola Horodeckiego zaowocowała ,we współpracy z wieloma innymi badaczami opublikowaniem dalszych dwudziestu ważnych artykułów naukowych .Warto podkreślić , że wszystkie artykuły naukowe wchodzące w skład osiągnięć dra Karola Horodeckiego zostały opublikowane w czasopismach specjalistycznych o bardzo wysokich indeksach wpływu , Prace te są w środowisku specjalistów w tych obszarach jak wyżej ,bardzo cenione o czym świadczą częste ich cytowania . Na dowód tego przytaczam pewne dane pozyskane z Web of Science .

Rys.3 Dane dotyczące publikacji pana dra K. Horodeckiego (źródło : Web of Science)



rys. 4 Praca w dorobku dra Karola Horodeckiego najczęściej cytowana (źródło : Web of Science) :



4 . Wnioski końcowe

Pan dr Karol Horodecki jak wynika z moich poprzednich wywodów i argumentów jest niewątpliwie bardzo kreatywnym badaczem o uznanej renomie światowej w środowisku zajmującym się (w szerokim sensie) Informatyka Kwantowa . Jakkolwiek jego badania i uzyskane wyniki maja charakter zdecydowanie teoretyczny (czasami zbyt abstrakcyjny jak na

wymagania dotyczące możliwości ich praktycznego zastosowania) ,a nawet wręcz dotyczą badania teoretycznego zachowań się układów o których nie wiadomo czy w ogóle istnieją w Świecie rzeczywistym (np. poza-kwantowe układy pod-świetlne) to stanowią one ważne wyniki z punktu widzenia poznawczego.

Problematyka jego badan ma charakter interdyscyplinarny lokując się na przecięciu tego co nazywamy Informatyką Kwantową w szerokim sensie a Fizyką Kwantowa (ale o posmaku czysto teoretycznym , a wręcz matematyzującym) i z tego powodu można zaliczyć przedstawioną rozprawę habilitacyjna jako rozprawę dotyczącą Fizyki – a wniosek dra Karola Horodeckiego jest adresowany w celu uzyskania stopnia naukowego doktora habilitowanego w dziedzinie Nauk Fizycznych , dyscyplinie Fizyka .

Rys 5. Spektrum tematyczne publikacji dra Karola Horodeckiego (źródło : Web of Science)

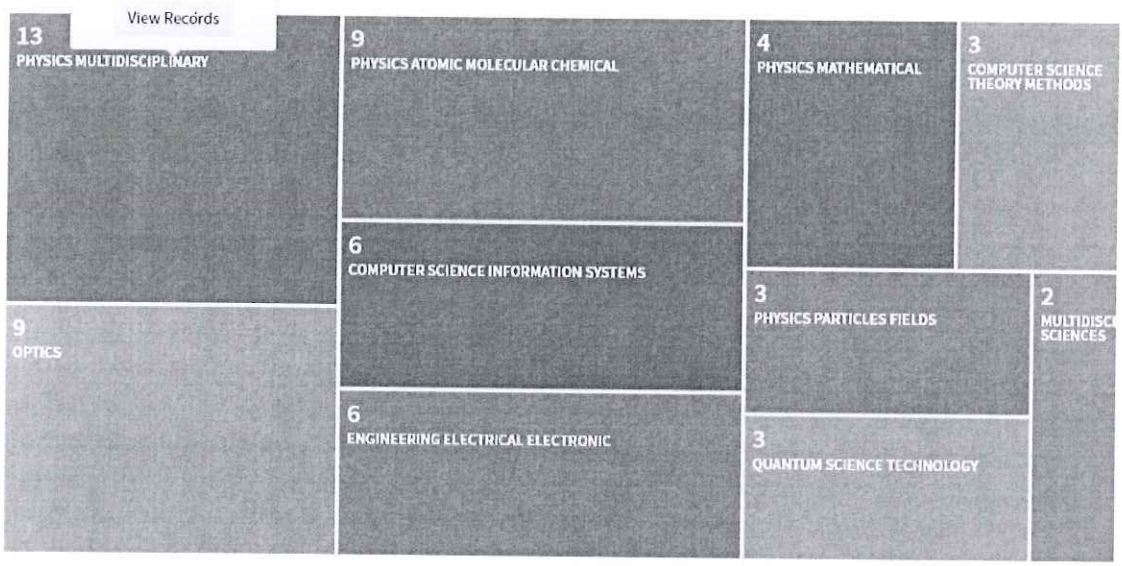
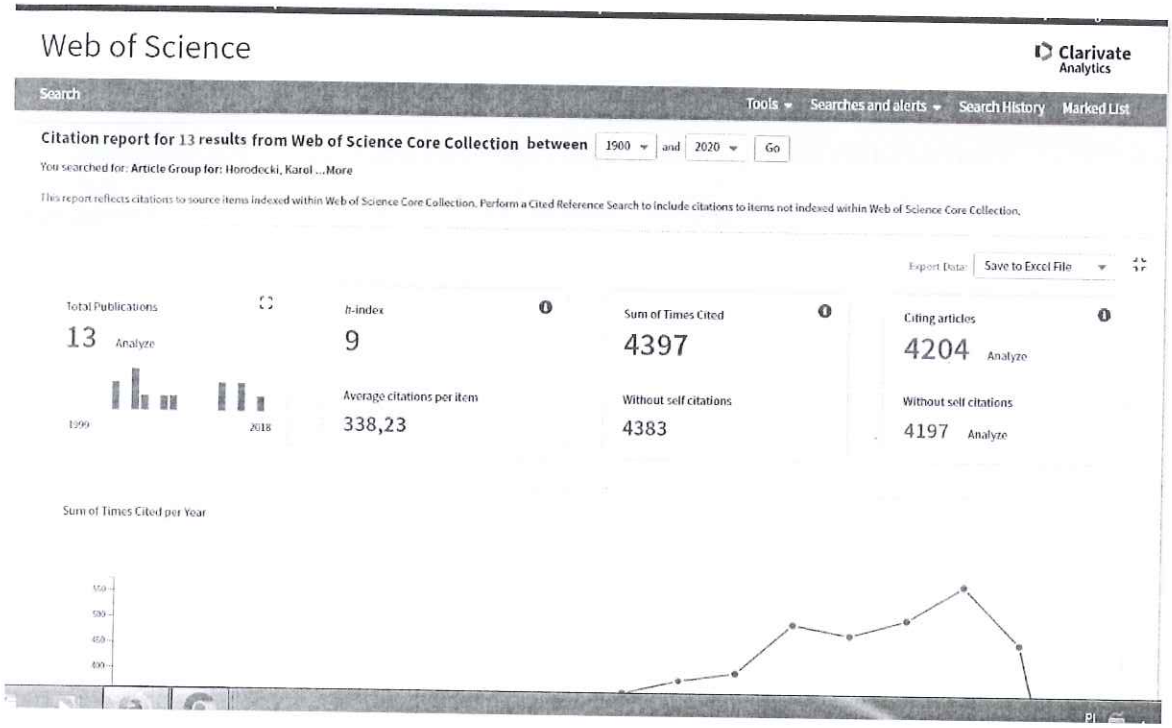


Tabela 6. Statystyka tematów obecnych w dorobku naukowym dra K. Horodeckiego (źródło : Web of Science)

Select	Field: Web of Science Categories	Record Count	% of 34	Bar Chart
☐	PHYSICS MULTIDISCIPLINARY	13	38.235 %	
☐	OPTICS	9	26.471 %	
☐	PHYSICS ATOMIC MOLECULAR CHEMICAL	9	26.471 %	
☐	COMPUTER SCIENCE INFORMATION SYSTEMS	6	17.647 %	
☐	ENGINEERING ELECTRICAL ELECTRONIC	6	17.647 %	
☐	PHYSICS MATHEMATICAL	4	11.765 %	
☐	COMPUTER SCIENCE THEORY METHODS	3	8.824 %	
☐	PHYSICS PARTICLES FIELDS	3	8.824 %	
☐	QUANTUM SCIENCE TECHNOLOGY	3	8.824 %	
☐	MULTIDISCIPLINARY SCIENCES	2	5.882 %	



Konkluzje końcowe :

Wczytując się w treść artykułu 16 Ustawy z dnia 14.03. 2003 r. o stopniach naukowych i tytule naukowym ...(Dz.U. 2003 Nr 65 poz. 595) nie mam wątpliwości ze przedstawione osiągnięcie naukowe **"Wybrane, wzajemne relacje miedzy nielokalnością Bella , kontekstualnością , kluczem kryptograficznym bezpiecznym względem kwantowego adwersarza i kwantowym splątaniem"** (współ)-autorstwa dra Karola Horodeckiego (i będącego monotematycznym cyklem publikacji) oraz jego pozostały dorobek naukowy (przedstawiony we wniosku o nadanie mu stopnia naukowego doktora habilitowanego w Dziedzinie Nauk Fizycznych , dyscyplina Fizyka) wypełniają **z nawiązką** wszystkie wymagania stawiane tego rodzaju wnioskom i wnioskuję o nadanie mu stopnia doktora habilitowanego w Dziedzinie Nauk Fizycznych , dyscyplina Fizyka .

Prof. dr hab. Roman Gielerak