Zielona Góra , 10.04.2018

Recenzja osiągnięcia habilitacyjnego będącego monotematycznym cyklem publikacji i zatytułowanym **'Kody swobodnego dostępu w informatyce kwantowej '** (współ)-autorstwa dra Marcina Pawłowskiego oraz jego dorobku naukowo-dydaktycznego i organizacyjnego .

Recenzje wykonano na zamówienie Centralnej Komisji ds. Stopni i Tytułów postanowieniem (zmiana postanowienia z dnia 11.01.2018) z dnia 08.02 2018.

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

Zapotrzebowanie na losowość najwyższej próby w technologiach informatycznych jest w czasach dzisiejszych trudna do przeszacowania . Zwrócę uwagę tutaj na dwie płaszczyzny na których procesy generacji liczb losowych odgrywają role wręcz fundamentalną . Jak wiadomo , wielkoskalowe obliczenia i symulacje komputerowe , zwłaszcza symulacje układów kwantowych są realizowane (na superkomputerach) w oparciu o różne typy algorytmów zwanych algorytmami Monte Carlo . Dobrze są znane z literatury przypadki użycia zbyt "słabych „ generatorów liczb (pseudo)-losowych do implementacji programów obliczeniowo/symulacyjnych w oparciu o algorytmikę Monte Carlo które zakończyły się zupełna „klapą" ,tzn. wyniki symulacji stawały w sprzeczności albo z rzeczywistością fizyczną albo z matematyką ,co było oczywiście równoważne z ich dyskredytacją .Algorytmika typu Monte-Carlo wymaga perfekcyjnej losowości co w ramach klasycznych technologii tzw. klasycznych Generatorów Liczb Losowych (C -RNG)jest nie do uzyskania !! Z tego właśnie powodu wyniki obliczeń/symulacji komputerowych w oparciu o techniki Monte Carlo powinny zawsze być przyjmowane z pewna ostrożnością .Poprawienie jakości obliczeń /symulacji zatem jest związane z poprawą technologii tworzenia RNG o wyższych parametrach jakościowych: poziom losowości , wydajność,..

Inny ,niezmierne ważny dla czasów współczesnych obszar to zagadnienia bezpieczeństwa transferu informacji związane z masowa komunikacja oraz bezpieczna akwizycja informacji. Zbyt słaby poziom losowości stosowany do implementacji (tutaj ciągle dominują techniki oparte o generacje pseudolosowa ,tzw. generatory liczb pseudolosowych pRNG) typowych protokołów kryptograficznych używanych powszechnie w masowej komunikacji (sieci ,np. Internet)może grozić skutecznymi atakami na podstawowe składowe tych protokołów jak np. sam proces generacji (pseudo)-losowych kluczy oraz samych transferów tych kluczy , tzw. problem dystrybucji kluczy (KD problem).Znane są liczne i udane ataki na współcześnie stosowane protokoły stosowane w sieciach publicznych (typu Internet)których sukces był /jest spowodowany zbyt słabej jakości losowością używaną w implementacji tych protokołów.Jak wiadomo standard bezpieczeństwa jaki zapewniają nam dzisiejsze protokoły bezpieczeństwa w sieci Internet jest konsekwencja implementacji technicznej tych protokołów , a przy założeniu sterylności implementacji bezpieczeństwo ma charakter warunkowy i bazuje na założeniu ze pewne zadania obliczeniowe związane z atakiem (np. w przypadku RSA jest to problem faktoryzacji lub równoważnie obliczeń okresów w grupach modularnych) są zadaniami o zbyt dużej złożoności obliczeniowej dla współczesnych maszyn (czego dowodów matematycznych tak naprawdę nie posiadamy).Świętym Graalem dzisiejszej inżynierii bezpieczeństwa jest wygenerowanie protokołów dających tzw. absolutne bezpieczeństwo informatyczne niezależnie od potencjału obliczeniowego strony atakującej. Przy założeniu sterylności implementacji taki poziom bezpieczeństwa zapewni nam znany od roku 1917 tzw. protokół one-time pad , tzw. Protokół Vernama i kwantowe protokoły o których jest mowa w pracach Pana Pawłowskiego .Jeżeli chodzi o protokół Vernama, to już Shanon w roku 1946 podał matematyczny dowód jego absolutnego bezpieczeństwa przy założeniu jego sterylnej implementacji która obejmuje następujące założenia (zobaczymy ze to są ciągle (te same !) wymagania którym chcemy sprostać czy to na poziomie klasycznej krypto-inżynierii czy tez kwantowej) :

V (1) ciąg bitów (klucza) jest **perfekcyjnie losowy**

V(2) ciąg bitów klucza jest tej samej długości co ciąg bitów wiadomości (**wydajność !!**)

V(3) klucz jest **transferowany bezpiecznie** do adresata (bezpieczeństwo KD ! : szumy , podsłuchujący ,..)

V(4) niepowtarzalność klucza (czyli znowu V (1) i V(2))

Chociaż pierwszy kwantowy protokół dystrybucji kluczy pojawił się w literaturze już w roku 1984 [BB84]Bennett, C.H., and G. Brassard (1984), "Quantum cryptography: Public key distribution and coin tossing," Proceedings of the IEEE International Conference on Computers,Systems and Signal Processing, Bangalore, India , 175.(w wersji one-way transfer

),a następnie w wersji opartej o użycie stanów splątanych [Ekert, A.K. (1991), "Quantum cryptography based on Bell's theorem," Physical Review Letters 67 (6), 661–663.]to dopiero po pojawieniu się kwantowego algorytmu Shora aktywność dotycząca technologicznej implementacji protokołów kwantowej dystrybucji klucza (QKD) wzrosła w tempie eksponencjalnym. Jakkolwiek z punktu widzenia czysto informatycznego można udowodnić absolutne bezpieczeństwo znanych protokołów QKD to jednak podobnie jak w przypadku protokołu Vernama w każdej rzeczywistej implementacji tych protokołów użyta technologia fizyczna łamie jakieś/któreś z założenia/n dowodu twierdzeń o bezpieczeństwie . Na dzień dzisiejszy sytuacja jest taka ,iż nie istnieje żadna , nawet komercyjna implementacja znanych protokołów QKD która jest odporna na ataki'w 100%' [Zheng, Y., and T. Matsumoto (1997), "Breaking real-world implementations of cryptosystems by manipulating their random number generation," in *Proceedings of the 1997Symposium on Cryptography and Information Security ,Fukuoka, Japan*, pp. 6B1–6, Zhao, Y., C.-H.F. Fung, B. Qi, C. Chen, and H.-K. Lo (2008),"Quantum hacking: Experimental demonstration of timeshiftattack against practical quantum-key-distribution systems, Physical Review A 78, 042333, Li, H.-W., Z.-Q. Yin, S. Wang, Y.-J. Qian, W. Chen, G.-C.Guo, and Z.-F. Han (2015), "Randomness determines practicalsecurity of BB84 quantum key distribution," Scientific Reports 5, 16200.]Przyglądając się implementacjom proponowanych protokołów QKD [Bennett, C.H., and G. Brassard (1984), "Quantum cryptography: Public key distribution and coin tossing," Proceedings of the IEEE International Conference on Computers,Systems and Signal Processing, Bangalore, India , 175.],[E91,Ekert, A.K. (1991), "Quantum cryptography based on Bell'stheorem," Physical Review Letters 67 (6), 661–663],[Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden (2002),"Quantum cryptography," Reviews of Modern Physics74 (1), 145–195.],],[Lo, H.-K., M. Curty, and K. Tamaki (2014), "Secure quantumkey distribution," Nature Photonics 8 (8), 595–604,2014],[Scarani, V., H. Bechmann-Pasquinucci, N.J. Cerf, M. Du˘sek,N. Lutkenhaus, and M. Peev (2009), "The security of practical quantum key distribution," Reviews of Modern Physics 81, 1301–1350.],można zauważyć , ze stanowią one w zasadzie bardzo wyrafinowane wersje generatorów liczb losowych o strukturze rozciągłej (przestrzennie) która zawiera mechanizmy (kwantowe) generowania entropii (losowości) oraz mechanizmy podwyższania poziomu losowości (tzw. Randomness amplification algorithms).Widziane z takiej perspektywy implementacje protokołów QKD doczekały się rożnego rodzaju (często udanych w 100%) ataków wzorowanych na atakach na standardowe implementacje pRNG lub tez ataków bezpośrednio na bloki generujące losowość w zadanej implementacji (Stipcevic, M., and C, .K. Ko, (2014), "True Random, Number Generators," Open Problems in Mathematics and Computational Science (Springer International Publishing, Switzerland), pp. 275–315. 2014].Najbardziej udane ataki na istniejące komercyjne implementacje infrastruktury QKD są opisane np. w : [Gerhardt, I., Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer,and V. Makarov (2011), "Full-field implementation of a perfect eavesdropper on a quantum cryptography system."Nature Communications 2 (2027), 349.],[Lydersen, L., C. Wiechers, C. Wittmann, Dominique Elser,J. Skaar, and V. Makarov (2010), "Hacking commercial quantum cryptography systems by tailored bright illumination,"Nature Photon 4 (686), 5.], [Z.Zhao, Y., C.-H.F. Fung, B. Qi, C. Chen, and H.-K. Lo (2008),"Quantum hacking: Experimental demonstration of time Shift attac against practical quantum-key-distributions systems,"Physica lReview A 78, 042333], [Li Li, H.-W., S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y.Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao,and Z.-F. Han (2011), "Attacking a practical quantum key-distribution system with wave length-dependent beam Splitter and Multi wave length sources," Physical Review A84, 062308.].We wszystkich znanych atakach na protokoły QKD prawie zawsze zródłem sukcesu były ataki rożnego rodzaju na same układy kwantowe (urządzenia działające w oparciu o prawa fizyki kwantowej)realizujące zaimplementowany protokół transferu .Dlatego tez w reakcji na to zaproponowane zostały nowe warianty protokołów QKD , tzw. protokoły niezależne od samych implementacji sprzętowych i działające w oparciu o prawa fizyki kwantowej tzw. protokoły typu DI QKD i DI RNG (patrz poniżej)[D. Mayers and A. Yao, Quantum Inf. Comput. 4, 273(2004),....] .Ich bezpieczeństwo absolutne ,w wersjach opartych o zjawisko splątania stanów kwantowo mechanicznych i w oparciu o łamanie nierówności korelacyjnych Bella w takich stanach (ciągle jeszcze dyskutowane na gruncie eksperymentalnym , eksperyment Aspecta) jest w zasadzie udowodnione przy wielu założeniach dotyczących zastosowanej implementacji fizycznej.

Prace Pana dra Pawłowskiego , napisane we współpracy z wieloma osobami dotyczą dwóch zasadniczych wątków związanych z kwantowymi protokołami komunikacyjnymi a dokładnie dotyczą głownie zastosowań. kwantowych wersji tzw. kodów swobodnego dostępu (Q-RAC (m.n, p)) do technologii generowania liczb losowych (Q-RNG), zwłaszcza do ich certyfikacji w oparciu o protokoły kwantowej komunikacji typu one- way. Drugi wątek w przedstawionej przez Pana Pawłowskiego rozprawie habilitacyjnej opartej o monotematyczny cykl publikacji to zagadnienia sformułowania wersji protokołów QKD typu one-way transfer, a opartych o koncepcje możliwości weryfikacji (certyfikacji)kwantowego charakteru pracy systemu kwantowego w sytuacji gdy nie mamy korelacji typu Bella związanych z stanami splątanymi). Prace te zostaną omówione bardziej dokładnie w następnym paragrafie .

2. Omówienie głównych wyników osiągnięcia habilitacyjnego dra Marcina Pawłowskiego.

W klasycznej informatyce znany jest problem implementacji określonego zadania komunikacji(np. transfer klucza , innych danych ...)w oparciu o wykorzystanie minimalnych zasobów informatycznych (ilość bitów)oraz jednoczesne zapewnienie możliwie najwyższego poziomu bezpieczeństwa (np. odporność na zaszumienie kanału , atak ,..) .Klasa zadań polegających na transferze skończonego ciągu bitów nosi nazwę zadania transmisji kodu o swobodnym dostępie . Istotnym parametrem jest to określenie minimum prawdopodobieństwa poprawnego odczytu wszystkich transferowanych bitów . Jeżeli p=1 to transfer jest deterministyczny .Dla sukcesu takiej transmisji w sytuacji ogólnej musimy zapewnić p >½. Każdy protokół realizujący transfer n bitów za pomocą m bitów z prawdopodobieństwem sukcesu p nazywamy klasycznym protokołem transferu kodu o dostępie swobodnym (C-RAC)) a dokładniej protokołem C-RAC (m,n ,p). Kwantowe wersje takich zadań tzw. protokoły Q-RAC (m,n,p) sa badane od wielu lat w Kwantowej Informatyce i wiadomo , ze przy założeniu $n \leq 4^m - 1$ istnieją protokoły realizujące taki transfer n bitów za pomocą m qubitów z prawdopodobieństwem sukcesu p > ½.

Przedstawiona przez Pana Pawłowskiego seria dziesięciu wspólnych publikacji (z łącznie 25 -cioma współautorami !) dotyczy zastosowań technik analizy protokołów typu Q-RAC (m,n,p) do badania rożnych zagadnień związanych z certyfikacja bezpieczeństwa protokołów semiDI- typu one –way QKD.A także , co jest związane z bezpieczeństwem protokołu transmisji , certyfikacji kwantowego mechanizmu generowania losowości w oparciu o protokoły semiDI–RNG. Poniżej przedstawię krótki opis najważniejszych wyników uzyskanych w zamieszczonych pracach.

Wykaz publikacji stanowiących osiągnięcie naukowe (o którym mowa w art. 16 ust. 2 ustawy A) Monotematyczny cykl publikacji pt.

Kody swobodnego dostępu w informatyce kwantowej.

[P1] M. Pawłowski, N. Brunner, "Semi-device-independent security of one-way quantum key distribution", Phys. Rev. A 84, 010302(R) (2011).

Wcześniej było wiadomo [D. Mayers and A. Yao, Quantum Inf. Comput. 4, 273(2004),....] ze można sformułować bezpieczne (przy założeniu sterylności ich implementacji) protokoły DI –QKD w oparciu o komunikacje oparta na współdzieleniu splatania kwantowo- mechanicznego przez obie strony komunikujące się a następnie sprawdzenie poziomu losowości za pomocą badania tzw. Macierzy Korelacji Danych otrzymywanych w kolejnych rundach protokołu. Wyrocznią w tych protokołach jest poziom łamania odpowiednich nierówności Bella przez porównanie jej obserwowanego łamania z tą która przewiduje teoria kwantowa .Tego rodzaju implementacja jest jednak bardzo wymagająca od strony technicznej i z tego powodu znacznie narażona na różne odstepstwa od perfekcji. W tejpracyAutorzy,za pracami [S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N.Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A.Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).[9] Y.-C. Liang, T.V´ertesi, and N. Brunner,Phys. Rev. A **83**, 022108(2011) rozważają protokoły typu semi- DI QKD w kontekście Q-QRG i w miejsce nierówności Bella wprowadzili jako wyrocznie tzw. Świadki Wymiaru (wprowadzone w pracy [R. Gallego, N. Brunner, C. Hadley, and A. Acin, Phys. Rev. Lett.**105**, 230501 (2010).]), pewne liniowe formy w elementach Macierzy Korelacji Danych] . To umożliwiło przeniesienie znanych mechanizmów certyfikacji losowości i bezpieczeństwa dla protokołów DI Q-RNG do ich wersji „one-way transfer" a wiec znacznie mniej wymagającej a dającej poziom bezpieczeństwa porównywalny do tego jaki uzyskuje się dla protokołów DI QKD (Q-RNG).Istotna obserwacją było zauważenie , ze jeden z użytych Świadków Wymiaru , Swiadek S jest prawie identyczny z prawdopodobieństwem uzyskania sukcesu w znanych scenariuszach realizacji protokołu Q-RAC (1,2,p).To pozwoliło na zastosowanie metod analitycznych wypracowanych przy analizie protokołów typu Q-RAC (m,n,p) do analizy zagadnień certyfikacji generowanej losowości czy tez oceny bezpieczeństwa w przedstawionych protokołach semi-DI QNG czy tez odpowiednio semi-DI QKD.
Powiazanie metod analitycznych wypracowanych w kontekście analizy protokołów Q-RAC do analizy bezpieczeństwa w protokołach semiDI QKD czy tez certyfikacja semiDI QNG pojawi się w następnych publikacjach cyklu .
Wkład Pana Pawłowskiego :„*Mój wkład w powstanie tej pracy polegał na: wymyśleniu zagadnienia badawczego, dyskusjach nad zagadnieniem, obliczeniach i edycji manuskryptu. Mój udział procentowy szacuję na: 50%.*"

[P2] M. Pawłowski, A. Winter,","Hyperbits: the information quasiparticles". ' Phys. Rev. A 85, 02233 1 (2012)

.Podstawowe jednostki informatyczne stosowane w rożnych zadaniach natury obliczeniowej czy tez komunikacyjnej to bity informacji oraz qubity .Przez analogie do sytuacji jakie mamy w zagadnieniach fizyki układów wielociałowych Autorzy proponują wprowadzić pojecie tzw. hiperbitu jako nowej jednostki informacyjnej w terminach której niektóre zagadnienia informatyczne w pewnych określonych kontekstach można by uprościć jak to robi wprowadzenie pojęcia quasicząstek w układach fizycznych. Definicja hiperbitu pojawia się w kontekście ciekawego twierdzenia mówiącego ze z punktu widzenia protokołów komunikacyjnych sytuacja gdzie pojawia się standardowa konfiguracja :nadawca-

odbiorca którzy współdzielą ze sobą pewna ilość splatania i mogą w kanale klasycznym transferowac 1 bit klasycznej informacji jest dokładnie z punktu widzenia komunikacji równoważna sytuacji kiedy nadawca może przesłać jeden hiperbit ale odbiorca hiperbitu może przesłać zwrotnie tylko klasyczny bit . Już w tym punkcie widać ze hiperbit jest jednostką typu artificial, w analogii do rożnego rodzaju quasicząstek w fizyce układów wielocalowych (polarony , magnony ,..). Użyteczność tej nowej koncepcji została zademonstrowana przez Autorów w kontekście analizy pewnych aspektów typowych protokołów kwantowej komunikacji.

Wkład Pana Pawłowskiego: *„Mój wkład w powstanie tej pracy polegał na: wymyśleniu zagadnienia badawczego, dyskusjach nad zagadnieniem, obliczeniach i edycji manuskryptu. Mój udział procentowy szacuję na:75%."*

[P3] H-W. Li, M. Pawłowski,Z-Q. Yin, G-C, Guo, Z-F. Han,"Semi-device independent random number expansion protocol with n to 1 quuntum random access codes", Phys. Rev. A 85, 052308 (20 1 2).

Ta praca jest rozszerzeniem wyników uzyskanych w pozycji [P1]. Podobnie jak w tamtej pracy podaje się protokół certyfikacji losowości generowanej przez semi-DI QNG . Nowością w stosunku do poprzedniej pracy jest użycie do generowania i certyfikowania otrzymywanej losowości protokołów komunikacyjnych typu Q- RAC (1,n,p) dla n >2.Ciekawy wynik tej pracy to pokazanie ,z e ilość losowości generowanej przez użycie protokołów Q-RAC(1,n,p) dla kolejnych wartości rosnących n (ale wtedy przecież p dąży do zera) nie zachowuje się w sposób monotoniczny w n i przyjmuje wartość maksymalna dla n=3.

Wkład dra Pawłowskiego: *„Mój wkład w powstanie tej pracy polegał na: wymyśleniu zagadnienia badawczego, dyskusjach nad zagadnieniem, obliczeniach i edycji manuskryptu. Mój udział procentowy szacuję na: 40%."*

[P4] H.-W. Li, P. Mironowicz, M. Pawłowski, Z.-Q. Yin, Y.-C. Wu. S. Wang, W. Chen, H.-G. Hu, G.-C. Cuo, Z.-F. Han, "Relationship between semi- and fully-device-independent protocols". Phys. Rev. A 87, 020302(R) (20l3)

W tej pracy Autorzy analizują związek jaki zachodzi pomiędzy protokołami certyfikacji losowości typu DI-QRG a protokołami typu semi-DI i jak w poprzednich pracach [1,3,4} scenariuszu komunikacji (2,2, 2).Podstawowy mechanizm badania poziomu bezpieczeństwa w protokołach DI QKD i DI RNG opiera się na stosowaniu nierówności korelacyjnych Bella w obserwowanej /mierzonej Macierzy Korelacji Danych .Natomiast w przypadku systemów semi-DI QKD i semi-DI QRNG (dyskutowanych w pracach { 1,2, 3) podstawowe narzędzie do certyfikacji losowości to Świadki Wymiaru. W bieżącej pracy udowodniono pewnego rodzaju równoważność obu scenariuszy certyfikacji przez pokazanie ze z każda nierównością Bella można związać pewnego Świadka Wymiaru i odwrotnie , z każdym Swiadkiem Wymiaru można powiązać pewna nierówność korelacyjna Bella .Jako ciekawy wynik można zacytować to ze narzędzia optymalizacyjne przygotowane do użycia w kontekście nierówności korelacyjnych Bella mogązostać zaadoptowane do badan zagadnień optymalizacji związanych ze Świadkami Wymiaru.

Wkład dra Pawłowskiego *:'Mój wkład w powstanie tej pracy polegał na: koordynacji projektu, dyskusjach nad zagadnieniem, obliczeniach i edycji manuskryptu. Mój udział procentowy szacuję na:35%"*

[P5] J. Ahrens, P. Badziąg, M. Pawłowski. M. Żukowski, M. Bourennane,"Experimental Tests of Classical and Quantum Dimensions", Phys. Rev. [,ett. 112, 140401 (2014).

Podano scenariusz eksperymentu demonstrującego użyteczność wprowadzonej w [N. Brunner, S. Pironio, A. Acin, N. Gisin, A. Méthot, and V. Scarani, Phys. Rev. Lett. 100, 210503 (2008) koncepcji Świadka Wymiaru , koncepcji której to użyteczność w sensie teoretycznym została zademonstrowana we wcześniejszych pracach P1-P5 przedstawionego cyklu publikacji. Sam eksperyment został osadzony w ramach implementacji wcześniej analizowanych protokołów semiDI QRNG i jego głównym zadaniem była eksperymentalna demonstracja możliwości odróżnienia klasycznego procesu generowania losowości od mechanizmu kwantowego poprzez porównanie odpowiednich wartości oczekiwanych Świadka Wymiaru. Eksperyment zrealizowano dla przypadków kiedy transferowana informacja jest zapisana albo w kubicie (d=2) , qutricie (d=3) oraz przypadku quartsów o wymiarze d=4.Jako ciekawy wynik pośredni można podkreślić iż , niejako przy okazji uzyskano precyzyjne górne oszacowania dla używanych Swiadków Wymiaru.

Wkład dra Pawłowskiego: *'Mój wkład w powstanie tej pracy polegał na wykonaniu większości obliczeń oraz dowodów a takze ustaleniu efektywności dystrybucji klucza oraz generacji losowości przy zastosowaniu badanych protokołów. Mój udział procentowy szacuję na:30%"*

[P6] P. Mironowicz, H.-W. Li, M. Pawłowski. "Properties of dimension witnesses and their semi-definite programming relaxations". Phys. Rev, A 90,022322 (2014).

W tej publikacji próbuje się rozszerzyć/zastosować metody wypracowane dla oszacowań ilości certyfikowanej losowości (mierzonej za pomocą funkcji typu min-entropy) w protokołach DI Q-RNG (gdzie certyfikacja losowości odbywa się przez pomiar głębokości łamania odpowiednich nierówności Bella) do przypadku protokołów typu semiDI , gdzie certyfikacja odbywa się badanie wartości średnich odpowiednich Świadków Wymiaru. We wcześniejszej publikacji [P4] podano odpowiedniość pomiędzy nierównościami Bella a Świadkami wymiaru co umożliwia w kontekście tej pracy przypisanie użytym Świadkom Wymiaru odpowiednich układów DI i odpowiednich nierówności Bella dla których to sytuacji jest znany aparat numeryczny służący do szacowania ilości certyfikowanej losowości a głębokością łamania nierówności Bella. W oparciu o to okazało się możliwe powiazanie ilości certyfikowanej losowości w semiDI protokołach Q-RNG z wartościami średnimi Świadków Wymiaru.Ciekawy produkt tej analizy to procedury konstrukcji nowych Świadków Wymiaru które są wstanie „wydać" certyfikat losowości większej jej ilości niż do tej pory stosowane Świadki we wcześniejszych publikacjach cyklu.

Wkład dra Pawłowskiego :*'Mój wkład w powstanie tej pracy polegał na wymyśleniu zagadnienia badawczego, kierowaniu projektem, uczestnictwie w dyskusjach i edycji manuskryptu. Mój udział procentowy szacuję na: 50%."*

[P7]A. Grudka, K. Horodecki, M. Horodecki, W. Kłobus, M. Pawłowski, "Whe Ar Popescu-Rohrlich Boxes and Random Access Codes Equivalent'? ", Phys. Rev. Lett. 113, l0040l (2014).

Z punktu widzenia fundamentalnych praw związanych z STW podstawowy postulat jaki powinna spełniać Macierz Korelacji Danych w najogólniejszych protokołach komunikacji czy to klasycznej czy też kwantowej to postulat pod-świetlności , który mówi ,że odpowiednie wartości prawdopodobieństw warunkowych zapisane w tej Macierzy nie mogą umożliwić transferu informacji z prędkościami większymi niż prędkość światła (dokładniej: bez uprzedniej komunikacji fizycznej) .Oczywiste jest, że wszystkie schematy klasycznego transferowania informacji , i te oparte o fizyka kwantową spełniają ten postulat . Zbiory dopuszczalnych Macierzy Korelacji Danych maja bardzo ciekawe struktury z punktu widzenia geometrii .I tak np. wiadomo ze zbiór wszystkich Macierzy Korelacji Danych spełniających warunek pod-świetlności stanowi zbiór wypukły o strukturze polotypu w przestrzeni R^N , gdzie N zależy od szczegółów protokołu. Jego punkty ekstremalne nazywa się boksami PR .Ten polotyp zawiera w szczególności zbiór kwantowo-mechanicznych Macierzy Korelacji Danych który jest wypukły , ale nieliniowy . Zbiór kwantowych Macierzy Korelacji zawiera w sobie polotyp złożony z klasycznych Macierzy Korelacji , a granice rozdziału definiują tutaj nierówności korelacyjne Bella. Z koleimaksymalne łamania nierówności Bella, jeszcze mocniejsze niż pozwala na to mechanika kwantowa ale ciągle jeszcze zgodne z STW to właśnie boksy PR.W tej pracy jest analizowana typowa 8 wymiarowa sytuacja (2,2,2).PR boks jest zdefiniowany jako PR boks łamiący maksymalnie nierówność korelacyjna Clausera-Horna-Shimona-Holta, ale ciągłe jeszcze pod-świetlny czyli zgodny z STW.O tym boksie wiadomo ze za jego pomocą idodatkowej informacji jednobitowej można wiernie symulować działanie protokołu Q-RAC (1,2,p) jak opisanego we wcześniejszych pracach tego cyklu. Autorzy postawili pytanie jakie minimalne wzbogacenie Q_RACu jak wyżej pozwoliłoby symulować PR jak wyżej. W tym celu wprowadzone zostało pojęcie rac-Boksu jako uzupełnienie Q-RACu o jeden bit informacji . Następnie pokazano , ze istnieją podświetlne rac-Boksy umożliwiające symulacje działania PR- boksu a także pokazano istnienie nadświetlnych rac-Boksow za pomocą których nie da się symulować działania PR-boksu.

Wkład dra Pawłowskiego :*'Mój wkład w powstanie tej pracy polegał na uczestnictwie w dyskusjach oraz dowodach twierdzeń. Mój udział procentowy szacuję na: 40%".*

[P8] S. Muhammad, A.Tavakoli, M. Kurant, M. Pawłowski. M. Żukowski. M. Bourennane,"Quantum bidding in Bridge", Phys. Rev. X 4.021041 (2014).

Jak wiadomo każdą grę klasyczną można „skwantować" , jakkolwiek kanoniczne procedury dla takich „kwantowań" nie istnieją w ogólności. Przedmiotem tej publikacji jest pewna wersja kwantowa popularnej gry w karty , gry w brydża

, wersja która została nazwana Kwantowym Brydżem .W pracy pokazano iż sformułowany Kwantowy Brydż jest w zasadzie równoważny z dobrze znana gra kwantową Clausera-Horna-Shimona-Holta o której z kolei wiadomo ze jest ona równoważna z Q-RACkiem (1,2,p) w wersji jak opisanej we wcześniejszych publikacjach tego cyklu. Praca jest ciekawą demonstracja faktu iż , w niektórych zadaniach komunikacyjnych zastosowanie technologii kwantowej pozwala na znaczne obniżenie poziomu złożoności komunikacyjnej w porównaniu do technologii klasycznych .

Wklad dra Pawłowskiego :*'Mój wkład w powstanie tej pracy polegał na wymyśleniu zagadnienia badawczego, kierowaniu projektem, uczestnictwie w dyskusjach, przeprowadzeniu obliczeń zawartych w pracy oraz edycji manuskryptu. Mój udział procentowy szacuje na:70%."*

[P9] M. Dall'Arno. E,. Passaro, R. Gallego, M. Pawłowski. A. Acin, "Attacks on semi-device independent quantum protocols". QIC 15, 0037 (2015).

Protokoły dla Q-RNG , QKD czy tez Q-RAC w wersji DI czy tez semi-DI są narażone na rożnego rodzaju ataki w rzeczywistych implementacjach. Najbardziej znane ataki to ataki związane z atakiem na rzeczywista efektywność procesów przygotowywania przesyłanej informacji (zarówno wkanale kwantowym jaki klasycznym w przypadku klasycznego protokołu) czy tez procesu mierzenia po stronie odbiorcy . Są to ataki znane w literaturze pod nazwa ataków 'detection loop-hole attacks „ (ataki typu DL) . W tej pracy Autorzy dyskutują szczegółowo scenariusz takiego ataku i jego możliwości zafałszowania korelacji zawartych w odpowiedniej Macierzy Korelacji Danych . Jak wiadomo istota stosowania protokołów o których jest mowa jest to , ze można odseparować losowość generowana przez sama naturę kwantowości od losowości generowanej w sposób klasyczny w tych protokołach. Powstaje zatem pytanie czy można sfałszować na tyle Macierz Korelacji Danych ażeby np. nie można było wykorzystać stosowanych Wyroczni , czyli w przypadku semi-DI protokołów Świadków Wymiaru. Okazuje się że przy pewnych założeniach ataki tego typu nie są wstanie (np. w przypadku semi-DI QNG) zapobiec uniemożliwieniu odseparowania klasycznych korelacji od kwantowych niezależnie od poziomu ingerencji we wskazniki efektywności po obu stronach łącza.

Wkład dra Pawłowskiego :*„Mój wkład w powstanie tej pracy polegał na dyskusjach nad projektem oraz otrzymaniu wyników zawartych w sekcji 4. Mój udział procentowy szacuję na: 15%"*

[Pl0] H.-W. Li. Z.-Q. Yin, M. Pawłowski. G.-C. Guo. Z.-F. Han."Detection efficiency and noise in a semi-device-independent randomness-extraction protocol", Phys. Rev. A 91" 032305 (20l 5).

Jak zwykle , w każdej fizycznej implementacji protokołów kwantowej komunikacji pojawiają się problemy związane z nie perfekcyjnością i nie sterylnością pewnych komponent takich implementacji. Problemy tego rodzaju pojawiły się już na poziomie próby implementacji tzw. Eksperymentu Aspecta I są znane pod nazwą „detection loophole" [P. Pearle, Phys. Rev. D2, 1418 (1970). D. Mermin, Ann. N.Y. Acad. Sci. 480, 422 (1986),..] .I do dzisiaj są źródłem kontrowersji rożnego rodzaju. W bieżącej publikacji cyklu podjęto próbę przeanalizowania wpływu nie perfekcyjności działania używanych detektorów (określana za pomocą ich efektywności) na prawidłowy przebieg funkcjonowania wcześniej analizowanych protokołów semiDI QNG oraz semiDI QKD, protokołów w istocie identycznych z protokołami typu Q-RAC(1,2,p). W pracypodano oszacowanie na tzw. wartości krytyczne poziomu efektywności mierników stosowanych przez Boba zarówno w przypadku symetrycznych (przy założeniu ze ich efektywności sa jednakowe) a także w przypadku asymetrycznym. Zamodelowano tez wpływ zaszumienia kwantowego kanału transmisji qubitu za pomocą białego szumu i obliczono krytyczne wartości zaszumienia umożliwiające sukces w realizowanym protokole .

Wkład dra Pawłowskiego : *„Mój wkład w powstanie tej pracy polegał na dyskusjach nad projektem, kierowaniu obliczeniami i edycji manuskryptu. Mój udział procentowy szacuję na: 40%."*

Podsumowanie wyników :

Wyniki uzyskane w przedstawionym cyklu dotyczą fundamentalnych zagadnień związanych z możliwościami skonstruowania wydajnych protokołów generacji liczb losowych i certyfikowania samego mechanizmu losowości w oparciu o kwantowe kody dostępu swobodnego w wersji przedstawionej jak w przedstawionych artykułach. Przedstawione konstrukcje mogą także być zastosowane także w implementacjach odpornych na standardowe ataki na transfer kluczy kryptograficznych kanałach klasycznych czy też kwantowych, aczkolwiek jak widać droga do zaimplementowania w pełni odpornego protokołu QKD wydaje się być ciągle jeszcze odległa i najeżona wieloma trudnościami. Prace stanowiące rdzeńdorobku habilitacyjnego zostały wszystkie co do wyjątku opublikowane w

topowych czasopismach o bardzo wysokich współczynnikach wpływu i spotkały się z żywym środowiska badaczy. Poniżej przytaczam , za portalem Web of Science wskaźniki bibliometryczne związane z przedstawionych cyklem prac.

Wyniki przedstawionego cyklu publikacji zostały przedstawione w bardzo lakonicznym autoreferacie , niestety w sposób bardzo oszczędny , a na dodatek trochę niechlujnie (mowa o jego wersji polskojęzycznej) od strony edycyjnej (dużo literówek , przekłamań gramatycznych ,niejasności , pomyłek w oznaczeniach ,...e.t.c.).Oczywiście poprzednia uwaga nie ma znaczenia w ocenie zwartości merytorycznej przedstawionego cyklu prac ale ....W wielu artykułach cyklu wiele naturalnych pytań i problemów , jak to zawsze sie dzieje w badaniach naukowych zostało przeznaczonych do dalszych badan i analiz .Juz po złożeniu wniosku habilitacyjnego pojawiło się sporo dodatkowego materiału naukowego i nowych publikacji związanych z nierozwiązanymi w przedstrawionym cyklu problemami rożnej natury, zobacz uwagi poniżej. Na podstawie tego co zostało napisane powyżej z całym przekonaniem formułuje następująca opinię :

W mojej opinii przedstawiony w cyklu monotematycznym 'Kody swobodnego dostępu i ich zastosowania w informatyce kwantowej' zbiór osiągnieć badawczych uzyskanych przez dra Pawłowskiego we współpracy z wieloma współautorami z ***nadwyżką*** *wypełnia oczekiwania zawarte w stosownych treściach ustawy stopniach i tytułach naukowych (zobacz paragraf 4 poniżej) i wnioskuje o przyjęcia tego cyklu jako ekwiwalentu rozprawy habilitacyjnej w Dziedzinie Nauk Fizycznych , dyscyplina Fizyka.*

3. Podsumowanie aktywności naukowo- dydaktycznej i organizacyjnej dra Pawłowskiego przed i po uzyskaniu stopnia doktora.

Rozpocznę od przytoczenia danych bibliometrycznych odnośnie aktywności naukowo- badawczej Pana Pawłowskiego uzyskanych za portalem Web of Science a wiec baza danych zawierającym informacje tego typu na bazie uznawanych czasopism (z listy JRC) oraz innych certyfikowanych najwyższym poziomem naukowej rzetelności źródeł .Pełna lista opublikowanych materiałów naukowych jest znacznie dłuższa i dołączona do tego wniosku habilitacyjnego przez Pana Pawłowskiego

Przeglądając listy jego publikacji naukowych łatwo zauważyć że właściwie cala jego aktywność naukowo badawcza od okresu przed uzyskaniem doktoratu aż do dnia dzisiejszego jest związana z zastosowaniem podstaw teorii kwantowej w obszarze informatyki. Nie jest to bynajmniej dziwne biorąc pod uwagę dominujące od wielu lat trendy badawcze w środowisku trójmiejskich fizyków kwantowych.

3.1 .Aktywność naukowo –badawcza związana z rozprawą doktorska .

Przed doktoratem dominujący wątek aktywności naukowo-badawczej obejmuje badania nielokalności Świata na poziomie kwantowym w protokołach komunikacyjnych.I tak np. w pracy [M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, M. Zukowski, "Information Causality as a Physical Principle ", Nature 461,110l (2009).] wyprowadzono maksymalne łamanie nierówności CHSH korzystając wyłącznie z podstawowych założeń teorii informacji które musza być spełniane przez wszystkie układy fizyczne. Ta praca była kontynuowana w artykule [J, Allcock, N. Brunneą M. Pawłowski, V. Scarani, "Recovering part of the quantum boundary front information causality" , Phys. Rev. A 80, 040103(R) (2009).] gdzie wyprowadzono dodatkowe ograniczenia oraz w[D. Manzano, M. Pawłowski, C, Brukner "The speed of quantum and classical learning for performing the k-th root of XIOT", New J. Phys. l1, l l3018 (2009).] gdzie uogólniono podstawowe narzędzia wykorzystane we wcześniejszych artykułach , jak powyżej.Główne zamierzenie przytoczonych prac miało na celu dowiedzenie się więcej o maksymalnym kwantowym łamaniu nierówności Bella. W innych pracach badano jak dopuszczenie komunikacji wpływa na ograniczenia klasyczne. I tak np. w |22] rozważano ilość i typ informacji jakie są wymagane przez klasyczne modele wspomagane jednokierunkową komunikację pomiędzy stronami aby osiągnąć maksymalną dopuszczalna przez teorię kwantową wartość łamania CHSH.

Stopień doktora nauk fizycznych został nadany panu Pawłowskiemu przez Radę Wydziału Matematyki, Fizyki i Informatyki Uniwersytetu Gdańskiego w dniu 18.11.2010 na podstawie złożonej i obronionej rozprawy doktorskiej " Fizyczna teoria informacji" .

W swoim doktoracie pan Pawłowski skupił się na badaniach związku pomiędzy podstawowymi pojęciami fizyki a protokołami przetwarzania informacji i badania nierówności Bella na podstawie prac przytoczonych powyżej. Innym aspektem nierówności Bella poruszanym w obronionym doktoracie była ich monogamia.To określenie odnosi się do faktu. ze jeśli pomiary jednej ze stron mogą zostać użyte do złamania nierówności Bella razem z pewną grupą innych stron, silniejsze ograniczenie nakładane jest na możliwość użycia tych samych pomiarów do złamania ich z inną grupa. W [14] wyprowadzono ilościowe ograniczenie na monogamię każdej dwuosobowej nierównościBella. W [21] udało się pokazać. że do wyprowadzenia bezpieczeństwa kryptografii kwantowej, używanie jej pełnego formalizmu jest zbędne a założenie wyłącznie, że obowiązują ograniczenia monogamii jest wystarczające.

3.2 Aktywność naukowo-badawcza Pana Pawłowskiego po uzyskaniu stopnia doktora .

3.2.1 **Główne watki i osiągnięcia badawcze nie wchodzące w skład przedstawionego cyklu habilitacyjnego**

Watek 1:Badanie nierówności korelacyjnych typu Bella, w szczególności jej monogamiczności.
W serii prac [24,33,30,36,37,38 39] dr Pawłowicz wraz z **wieloma** współpracownikami kontynuował badania nad łamaniem nierówności Bella i obecnej w ich procesie zasadzie monogamii . W szczególności uzyskał nowe wyniki odnośnie tych zagadnień .Nowe wyniki i paralelne w stosunku do przedstawionego cyklu są zawarte w następujących przykładowych publikacjach :
R. Augusiak, T. Fritz, N,L Kotonski. N[. Kotornski, M. Pawłowski, M. Lewenstein, A. Acin,Tight Bell inequalities with no quantum violation from qubit unextendible product bases,Phys. Rcv. A 85, 0.12113 (2012).P.Horodecki,M.Pawłowski, R.Horodecki. Intrinstic asymmetry with respect to adversary : New feature of Bell inequalities. J. Phys. A: Math. Theor. 47, 424016 (2014). R. Augusiak, M.Demianowicz. M. Pawłowski. J. Tura. A. Acin, Elemental and tight monogamyrclations in nonsignalling theories. Phys. Rev. A 90, 052323 (201,1).[36] Ł. Czekaj, M. Pawłowski, T. Vertesi, A. Grudka, M. Ilorodecki, R. Horodecki, Quantum advantage for distributed computing without communication, Phys. Rev. A S2.032122 (2015).[37] D. Saha, M. Pawłowski, Structure of quantum and broadcasting nonlocal correlations, Phys.Rev. A 92 062129 (2015).|38] A. Tavakoli, S. Zohren, ,M.Pawłowski, Maximal Non-Classicality multi-setting Bell Inequalities, J. Phys. A: Math. and Theor. 49, 14530l (2016).[39] M. Pivoluska. M. Pawłowski, M. Plesh, Tight bound on the classical value of generalized Clauser-Horne-Shirnony-Holt games, Phys. Rev. A 94.022338 (2016).

Watek 2 Badania nad losowością kwantowo-mechaniczną

Uzyskano szereg ważnych wyników dotyczących ważnych zagadnień certyfikacji , a zwłaszcza amplifikacji słabo wydajnego źródła losowości. Reprezentatywne publikacje dla tych wyników to :P. Mironowicz, M .Pawłowski, Robustness of quantum randomness expansion protocols in the presence of noise, Phys. Rev. A 88, 0323l9 (2013). A. Grudka, K. Horodecki, M. Horodecki. P. Horodecki ,M. Pawłowski. R. Ramanathan. Free randomness amplification using bipartite chain correlations. Phys. Rev,. A 90.032322 (2014).[32] J. Bouda, M. Pawłowski, M. Pivoluska, N. Plesch. Device-independent randomness extraction for arbitrarily weak min-entropy source. Phys. Rev. A 90,032313 (2014), P. Mironowicz, R. Gallego, M.Pawłowski. Robust amplification of Santha-Vazirani Sources with three devices. Phys. Rev. A 91, 032317 (2015).,[45] P. Mironowicz. A. Tavakoli, A. Harneedi, B. Marques, M. Pawłowski, M. Bourennarre. Increased Certification of Semi-device Independent Random Numbers using Many Inputs and More Postprocessing, New J. Phys, 18, 065004 (20l6), H. Wojewodka. F'.G.S.L. Brandao. A. Grudka, M. Horodecki, K. Horodecki. P. Horodecki, M. Pawłowski, R.. Ramanathan. Amplifying the randomness of weak sources correlated with devices. IEEE Transactions of Information Theory, 63, 7592 (2017).

Watek 3. Zagadnienia QKD

Uzyskano szereg wyników dotyczący implementacji protokołów QKD i ich bezpieczeństwa. Reprezentatywne wyniki są zawarte w publikacjach: M. Pawłowski. Security proof for cryptographic protocols based only on the monogamy of Bell's inequality violations, Rev. A 82, 032313 (2010),M. Pawłowski, Reply to "Comment on Security proof for cryptographic protocols based only on the monogamy of Bell's inequality violations'", Phys.Rev. A 82.032313 (2010),M. Huber, M. Pawłowski, Weak randomness in device independent quantum key distribution and the advantage of using high dimensional entanglement, Phys. Rev. A 88, 032309 (2013), R. Rahaman, G. Parker, P. Mironowicz. M. Pawłowski. Dimensional discontinuity in quantum communication complexity at dimension seven, Phys. Rev. A 92. 062304 (2015),E. A. Aguilar, R. Ramanathan. J. Kofler. M. Pawłowski. Completely Device Independent Quantum Key Distribution, Phys. Rev. A 94.022305 (2016)

Inne wątki :-badanie protokołów teleportacji warunkach zaszumionych kanałów transmisji

-badanie złożoności komunikacyjnej wybranych protokołów komunikacji

Reprezentatywne publikacje w tym wątkach to :A. Grudka, K. Horodecki, M. Horodecki. P. Horodecki, M. Pawłowski, R. Ramanathan, "Free randomness amplification using bipartite chain correlations", Phys. Rev. A90, 032322 (2014),A. Chaturvedi, M. Pawłowski, K. Horodecki."Random access codes and non-local resources", Phys. Rev. A96,022125 (2011).

3.2.2 Kierowanie międzynarodowymi i krajowymi projektami badawczymi

-udział w charakterze **kierownika projektu:**

-Fizyczne podstawy przetwarzania informacji" finansowany przez UK EPSRC kwotą 233.503 GBP w latach 20l I-2014

-Jakościowe i ilościowe badanie losowości wyników pomiarów mechanice kwantowej" finansowany przez Narodowe Centrum Nauki kwotą 994.500 PLN w latach 2013-2016

-Kwantowe przetwarzanie danych przy silnie ograniczonej pamięci i komunikacji" finansowany przez Narodowe Centrum Nauki kwotą 1.991.129 PLN w latach 2015-2020

-Kryptografia z samotestującymi urządzeniami kwantowymi" finansowany przez Fundację na rzecz Nauki Polskiej kwotą 1 .425.411 PLN w latach 2016-2019

udział w charakterze wykonawcy:

-Informatyka i inżynieria kwantowa" (PBZ-MIN-008/P03/03), Ministerstwo Nauki i Szkolnictwa Wyższego, 2003-001

- Qubit Applications (QAP)", Komisja Europejska (F'P7-ICT), 2005-2009

-Scalable Quantum Computing with Light and Atoms (SCALA)", Komisja Europejska (I,-P6-ICT) 2005-2009

-Quantum Interfaces, Sensors, and Communication based on Entanglement (Q-ESSENCE)". Komisja Europejska (FP7-ICT) 20 1 0-20 l 3

-Quantum States: Analysis and Realizations (QUASAR)" (program CHIST:ERA), Narodowe Centrum Badań i Rozwoju, 2012-2014

-Quantum resources: conceptuals and applications (QOLAPS)", (European ResearchCouncilAdvanced Grant), 2013-2015

-Kwantowa informacja i kwantowa komunikacja" (Polsko - Austriacki program współpracy naukowo technicznej), Ministerstwo Nauki i Szkolnictwa Wyższego, 2003-2009

-Kwantowe przetwarzanie informacji" (Polsko - Austriacki program współpracy naukowo - technicznej), Ministerstwo Nauki i Szkolnictwa Wyższego, 2010-201 1

- Nieklasyczne korelacje i ich struktura w układach wielopoziomowych. Nowe źródła i metody analizy" (grant Sonata Bis, 2012105lElSTzl02352), Narodowe Centrum Nauki, 2008-2011

-Technologies for information transfer and processing based on phenomena of a strictly quantum nature" (project TEAM), Fundacja na rzecz Nauki Polskiej, 2012-20 l 5

3.2. Aktywność dra Pawłowskiego w sferze dydaktyki i popularyzacji Nauki.

3.2.0*INFORMACJE O DOTYCHCZASOWYM ZATRUDNIENIU W JEDNOSTKACH NAUKOWYCH/ARTYSTYC ZNYCH*

05.05.2010 - 31.12.2010: asystent techniczny,. Instytut Fizyki Teoretycznej i Astrofizyki. Uniwersytet Gdański

01.11.2010 - 30.04.2011: asystent. Schoo1 of Mathematics, University of Bristol ,

l6.07.2012 - 30.04.20l3: asystent techniczny, Instytut Fizyki Teoretycznej_ i Astrofizyk,. Uniwersytet Gdanski

. 01.05.2013 - 30.06.2015: specjalista naukowo-badawczy Instytut Fizyki Teoretycznej i Astrofizyki. Uniwersytet Gdanski ,

od 01.07.2015; adiunkt. Instytut Fizyki Teoretycznej i Astrofizyki. Uniwersytet Gdański

3.2.l.**Działalność podstawowa**-Mechanika Kwantowa (ćwiczenia), Politechnika Gdańska – 2010,

-Algorytmy Graficzne (wykłady). Politechnika Gdańska – 2010

-Obliczenia Symboliczne (ćwiczenia), Politechnika Gdańska -2010

-Technologie informacyjne (wykłady),UniwersytetGdański - 2012-3

:-Rachunek różniczkowy (ćwiczenia), University of Bristol - 2012-3:

Mechanika (ćwiczenia). University of Bristol - 20l5-6:

Analiza matematyczna II (ćwiczenia), Uniwersytet Gdański - 2015-6:

Matematyka dyskretna i algebra liniowa (ćwiczenia i wykłady), Uniwersytet Gdański - 2015-6:

Nieliniowe układy dynamiczne i chaos (laboratoria). Uniwersytet Gdański. .

3.2.2 . Inne :

-Nauka fizyki i fizyki po angielsku w III L.O. w Gdańsku. (3 semestry) 2006-2007]. .

- wykłady popularnonaukowe dla uczniów szkół średnich: "wielki zderzacz hadronów" i "winda lv kosmos",20l0.

. -opublikowanie artykułu popularnonaukowego: M. Pawłowski, M. Zukowski, "Głębia oczywistości", Świat Nauki. 228, 48 (2010).

-Prowadzenie zajęć na kółku fizycznych w III L.O. w Gdyni. (2 spotkania) 20l4-2015.

.- Cykl wykładów na ,,VI Summer School on Optics and Photonics" w Concepcion (Chile),20l6.

-wykłady na nocy naukowców organizowanej przez centrum Eksperyment w Gdańsku, 20l7.

3.2.3 Dyplomy :

a) Opieka naukowa nad studentami zagranicznymi

1)AtminTavakoli (University of Sztokholm) - zewnętrzny promotor pracy licencjackiej;

2)Anubhav Chaturvedi (IIIT Hyderabad) - opiekun stażu naukowego (2014):,zewnętrzny promotor pracy magisterskiej.;

3)Maharshi Ray ([IIT Hyderabad) - opiekun stażu naukowego (2014).

3.2.4 Opieka naukowa nad doktorantami w charakterze opiekuna naukowego 1ub promotora pomocniczego:

o Arijit Dutta - promotor pomocniczy; Rozprawa ,,Quantumness of states and their transfer" obroniona w 2016.

o doktorant : Piotr Mironowicz - promotor pomocniczy; Rozprawa ,Applications of semi-definite optimization in quantum information protocols" obroniona w 2016.

-Doktorant :Ryszard Veynar - promotor pomocniczy, planowana data obrony: XII 2017 .

-Nieformalna opieka nad doktorantami będącymi wykonawcami projektów pod moim kierownictwem: Edgar Aguilar, Debashis Saha, Anubhav Chaturuedi, Mate Farkas i Jan Jakub Baz.

3.3.Aktywnosc Pana Pawłowskiego w obszarze organizacyjnym i współpraca międzynarodowa .

3.3.1 Kierowanie pracami zespołu badawczego w ramach realizacji licznych grantów **międzynarodowych** i krajowych : patrz punkt 3.2.2.

3.3.2 Udział w komitetach organizacyjnych międzynarodowych i krajowych konferencji naukowych

o NATO Advanced Research Workshop "Quantum Communication and Security", 2006, Gdańsk (Polska), redakcja materiałów po - konferencyjnych

o NATO Advanced Research Workshop ,.Quantum Cryptography and Computing: Theory and Implementations", 2009. Gdańsk (Polska)" członek komitetu organizacyjnego i redakcja materiałów pokonferencyjnych

o DimWit Meeting 20l3. Sopot (Polska), przewodniczący komitetu organizacyjnego.

o 13th Asian Quantum Information Science Conference,20l3 Chennai, (Indie), członek komitetu programowego

o DimWit Meeting 2014. Sopot (Polska)., przewodniczący komitetu organizacyjnego.

o Quantum Information Processing 201Ą,Barcęlona (Hiszpania), członek komitetu, programowego

o 1Sth Asian Quantum Information Science Conference. 2015 Seul. (Korea Południowa), członek komitetu programowego

o 1Oth Doctoral Workshop on Mathematical and Engineering Methods in Computer Science 2015 Telcz (Czechy). Członek komitetu programowego

3.3.3 Udział w międzynarodowych konferencjach jako "invited speaker" :

o M. Pawłowski. .."Information Causality", Workshop on Quantum Correlations, Singapur (2009)

o M, Pawłowski, ,"Information Causalily", CIFAR Quantum Information Processing Meeting, Toronto, ON, Kanada (20l0)_

o M. Pawłowski. "Security proof for cryptographic protocols based only on the monogamy of Bell's inequality relations". Nordita Workshop on Quantum Cryptography, Sztokholm. Szwecja (2010)

M. Pawłowski,.,Simplicity as an axiom", ESF-PESC Strategic Workshop on Signatures of Quantumness In Complex Systems. Nottingham, Wielka Brytania (2011)

.- M. Pawłowski. ,..Nonlocality detection scheme for realistic sources". IISympozjum KCIK. Sopot. Polska (2011)

. -M. Pawłowski, .."Information Causality",Workshop on Quantum Correlations, Contextuality and All That. Natal. Brazylia (2013)
O M.Pawłowski, P. Mironowicz,. "Amplification of arbitrary weak randomness",Sympozjum KCIK, Sopot, Polska (2013)
-M. Pawłowski. "Monogamy of nonlocal correlations - a review", Phys .Info'i 3,Paryż, Francja (20 13)
I- M. Pawłowski,"R 4C-boxes", Quantum Contextuality: Trick or Treat, Singapur (2014)
o M. Pawłowsk ,Device Independent Quantum Key Distribution without Random Number Generator's", Randomness ,III Quantum Physics And Beyond. Barcelona,Hiszpania (2015)
o M. Pawłowski ,.Device Independent Quantum Key Distribution, without Random Number Generators", VI Sympozium KCIK, Sopot, Polska (2015)
o M. Pawłowski, "Quantum random access codes and mutually unbiased bases and other random Access code-based games ", Workshop on Quantum Correlations, Contextuality and All That ,Again , Natal. Brazylia (2015)
o M. Pawłowski, "Relation between randomness and monogamy of nonlocal correlations", workshop on the Foundations of Randomness. Stellenbosch. RPA (2015)
-M. Pawłowski, "Exotic random access codes", Workshop on Quantum Nonlocality, Causal Structures and Device-independent Quantum Information. Tainan. Tajwan (20l 5)
-M. Pawłowski, "Detection efficiency loophole in tests of quantumness", 2nd International Conference on Quantum Foundations, Patna. Indie (2016).
.-M. Pawłowski. "Quantum Random Access Codes and Mutuaily Unbiased Bases" , II International Conference on Mathematical Modelling, Gdańsk, Polska (2017).
o M. Pawłowski. "Information Causality", Lejda, Holandia (2017).

3.3.4 Referaty wygłoszone na konferencjach międzynarodowych : W sumie wygłoszono kilkadziesiat referatów i przedstawiono kilkanaście plakatów

3.3.5. Uczestnictwo w programach europejskich oraz innych programach międzynarodowych i krajowych

o ,,Informatyka i inżynieria kwantowa" (PBZ-MIN-008iP03/03), Ministerstwo Nauki i Szkolnictwa Wyższego, 2003 -2007, wykonawca
o,,Qubit Applications (QAP)", Komisja Europejska(FP7-ICT), 2005-2009, wykonawca
o "Scalable Quantum Computing with Light and Atorns (SCALA)", Komisja Europejska (FP6-ICT) 2005-2009, wykonawca
o "Quantum Interfaces, Sensors, and Communication based on Entanglement (Q-ESSENCE)", Komisja Europejska (FP7-ICT),, 201 0-20 l3, wykonawca
o „Quantum States: Analysis and Realizations (QUASAR)" (program CHiST:ERA) , Narodowe Centrum Badań i Rozwoju, 20I2-2014, wykonawca
"Quantum resources: conceptuals and applications (QOLAPS)", (European Research Council Advanced Grant), 2013-2015, wykonawca
o ,.Kwantowa informacja i kwantowa komunikacja" (polsko - austriacki program współpracy naukowo -technicznej), Ministerstwo Nauki i Szkolnictwa Wyższego, 2003-2009, wykonawca
.,Kwantowe przetwarzanie infornlacji" (Polsko - Austriacki program współpracy naukowo - technicznej),Ministerstwo Nauki i Szkolnictwa Wyższego ,2010-2011, wykonawca
. , Nieklasyczne korelacje i ich struktura w układach wielopoziomowych. Nowe źrodła i metody analizy" (grant Sonata Bis. 2012105lElSTzl0ż352). Narodowe Centrum Nauki, 2013-2017, wykonawca
o ,,Technologies for information transfer and processing based on phenomena of a strictly quantum nature"(project TEAM), Fundacja na rzecz Nauki Polskiej, 2012-2015, wykonawca

3.3.6 Członkostwo w międzynarodowych i krajowych organizacjach oraz towarzystwach naukowych:
o Członek Rady Naukowej Krajowego Centrum Informatyki Kwantowej w Gdańsku (od 2015).

4 Konkluzje końcowe

Podstawy prawne do sformułowanej konkluzji końcowej:

1) Ustawa z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki - Dz.U. 2003 nr 65 poz. 595

2) Ustawa z dnia 18 marca 2011 r. o zmianie ustawy - Prawo o szkolnictwie wyższym, ustawy o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki oraz o zmianie niektórych innych ustaw - Dz. U. 2011 nr 84 poz. 455

3) Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 1 września 2011 r. w sprawie kryteriów oceny osiągnięć osoby ubiegającej się o nadanie stopnia doktora habilitowanego - Dz. U. 2011 nr 196 poz. 1165

4) Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 22 września 2011 r. w sprawie szczegółowego trybu i warunków przeprowadzania czynności w przewodach doktorskich, w postępowaniu habilitacyjnym oraz w postępowaniu o nadanie tytułu profesora - Dz. U. 2011 nr 204 poz. 1200

Na podstawie przytoczonego materiału obrazującego aktywność pana dra Marcina Pawłowskiego w trzech podstawowych płaszczyznach aktywności zawodowej : płaszczyźnie naukowo- badawczej , płaszczyźnie dydaktycznej i płaszczyźnie organizacyjnej wnioskuje , ze jego dorobek zawodowy , zwłaszcza na płaszczyźnie naukowo-badawczej jako najważniejszej dla konsekwencji tego rodzaju opinii jest imponujący i wypełnia wszystkie założenia odpowiednich ustaw i rozporządzeń jak wyżej . Dorobek naukowy dra Marcina Pawłowskiego wybiega , w mojej opinii znacznie poza średni poziom naukowy wniosków o wszczęcie procedur habilitacyjnychw w Polsce .Wyniki naukowe dra Marcina Pawłowskiego dotyczą fundamentalnych zagadnień związanych zarówno z fizyka kwantowa jak tez ich zastosowań do kwantowej informatyki.Wyniki te są szeroko znane i cenione w Świecie i często cytowane w światowej literaturze przedmiotu, a sam ich Autor jest osobą szeroko znana i rozpoznawalna w obszarze Informatyki Kwantowej.

Na podstawie przeprowadzonej i przedstawionej analizy dorobku zawodowego pana dra Marcina Pawłowskiego z pełnym przeświadczeniem wnioskuję o nadanie panu drowi Marcinowi Pawłowskiemu stopnia doktora habilitowanego Nauk Fizycznych , dyscyplinie Fizyka.

Prof. dr hab. Roman Gielerak

Instytut Sterowania i Systemów Informatycznych

Wydział Informatyki ,Elektrotechniki i Automatyki

Uniwersytet Zielonogórski