

ПРИМЉЕНО:		19. 09. 2025	
Рад.јед.	б р о ј	Арх.шифра	Прилог
6801	1585/1		

Научном већу Института за физику у Београду

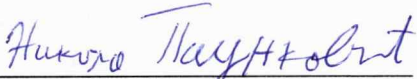
Молба за покретање поступка за избор у звање научни саветник

Молим научно веће Института за физику у Београду да у складу са Правилником о стицању истраживачких и научних звања Министарства науке, технолошког развоја и иновација Републике Србије покрене поступак за мој избор у звање научни саветник (по правилима за повратнике из иностранства, и уз прескакање звања научни сарадник и виши научни сарадник).

У прилогу уз молбу достављам:

1. Мишљење руководиоца лабораторије са предлогом чланова комисије
2. Биографске податке
3. Преглед научне активности
4. Приказ елемената за квалитативну оцену научног доприноса
5. Приказ елемената за квантитативну оцену научног доприноса
6. Списак објављених радова и њихове копије
7. Податке о цитираности
8. Решење о нострификацији докторске дисертације
9. Додатке

У Београду, 16.09.2025.


др Никола Паунковић

Научном већу Института за физику у Београду

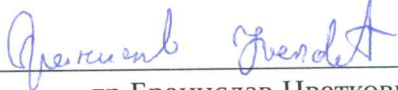
Мишљење руководиоца лабораторије о избору др Николе Паунковића у звање научни саветник

Др Никола Паунковић је рођен 1973. године у Загребу, Хрватска. Дипломирао је 1998. године на Физичком факултету Универзитета у Београду. Докторску тезу из области квантна информатика и рачунарство брани 2004. године на Универзитету Оксфорд, Уједињено Краљевство, под заједничким менторством проф. др Артура Екерта и др Влатка Ведрала. Током 2005. прелази на Институт за научну размену у Торину, Италија, као постдок под вођством др Паола Занардија. Током 2007. ради свој други постдок на Департману за математику Техничког универзитета у Лисабону у Групи за логику и рачунарство, под менторством проф. др Паула Матеуша. Од 2008. ради као истраживач на Институту за телекомуникације у Лисабону, у оквиру Групе за сигурност и квантну информатику. У периоду 2009-2014. члан је Центра за физику фундаменталних интеракција Универзитета у Лисабону, а од 2015. до 2019. Центра за Физику и инжењерство напредних материјала Универзитета у Лисабону. Учесник је 13 међународних пројеката, а додатно је био руководиоца једног међународног пројекта. Аутор је преко 40 научних публикација, и био је ментор за 6 докторских дисертација на Универзитету у Лисабону.

Имајући у виду да др Никола Паунковић, као повратик из иностранства, испуњава све услове предвиђене Правилником о стицању истраживачких и научних звања Министарства науке, технолошког развоја и иновација Републике Србије, препоручујем Научном већу Института за физику у Београду да др Паунковићу одобри покретање поступка за избор у звање научни саветник, уз прескакање звања научни сарадник и виши научни сарадник. Коначно, предлажем следеће чланове комисије за избор:

1. др Марко Војиновић, научни саветник, Институт за физику у Београду,
2. др Бранислав Цветковић, научни саветник, Институт за физику у Београду,
3. проф. др Мирољуб Дугић, редовни професор Природно-математичког факултета Универзитета у Крагујевцу.

У Београду, 26.09.2025.



др Бранислав Цветковић
научни саветник

руководилац Групе за гравитацију, честице и поља
Института за физику у Београду

Материјал уз захтев за избор др Николе Паунковића у звање научни саветник

1. ПОДАЦИ О КАНДИДАТУ

Име и презиме: **Никола Паунковић**

Година рођења: **1973.**

Радни статус: **запослен**

Назив институције у којој је запослен: **Институт за телекомуникације, Лисабон, Португалија (Instituto de Telecomunicações, Lisboa, Portugal)**

Претходна запослења:

2006-2007 Постдок истраживач, Департман за математику Техничког универзитета у Лисабону (Departamento de Matemática, IST, Universidade Técnica de Lisboa)

2005-2006 Постдок истраживач, Институт за научну размену, Торино, Италија (Research Fellow, Institute for Scientific Interchange, Turin, Italy)

1999-2000 Сарадник у настави, Физички факултет Универзитета у Београду

1998-2000 Истраживач приправник, Институт за физику у Београду

Образовање

Основне академске студије: **1992-1998, Физички факултет Универзитета у Београду**

Одбрањен мастер или магистарски рад:

Одбрањена докторска дисертација: **07.02.2005, Универзитет у Оскфорду, Уједињено Краљевство (Oxford University, UK)**

Постојеће научно звање:

Научно звање које се тражи: **научни саветник** (уз прескакање звања научни сарадник и виши научни сарадник)

Датуми избора у стечена научна звања (укључујући и постојеће)

научни сарадник:

виши научни сарадник:

Област науке у којој се тражи звање: **природно-математичке науке**

Грана науке у којој се тражи звање: **физика**

Научна дисциплина у којој се тражи звање: **Квантна механика, квантно рачунарство и квантна оптика**

Назив матичног научног одбора којем се захтев упућује: **МНО за физику**

Стручна биографија

Никола Паунковић је рођен 1973. године у Загребу, Хрватска. Основну школу, Математичку гимназију и Физички факултет завршио је у Београду. Дипломирао је 1998. године на смеру Теоријска физика са просеком 9,39. Исте године постаје истраживач приправник у оквиру групе проф. др Звонка Марића на Институт за физику, и започиње магистарске студије у оквиру програма „Класична, квантна и математичка физика“. У исто време ради као сарадник у настави на Физичком факултету. Магистарске студије прекида 2000. године да би започео докторске студије на Универзитету Оксфорд, Уједињено Краљевство. Докторску тезу из области квантна информација и рачунарство, под насловом „Улога неразличивости идентичних честица у обради квантне информације“ (“The role of indistinguishability of identical particles in quantum information processing”), брани 2005. године под заједничким менторством проф. др Артура Екерта (Artur Ekert) и др Влатка Ведрала. Током 2005. прелази на Институт за научну размену (Institute for Scientific Interchange) у Торину, Италија, као постдок под вођством др Паола Занардија (Paolo Zanardi). Током 2006.-2007. ради свој други постдок на Департману за математику Техничког универзитета у Лисабону (Departamento de Matemática, IST, Universidade Técnica de Lisboa) у Групи за логику и рачунарство (Group for Logic and Computation) под менторством проф. др Паула

Матеуша (Paulo Mateus). Од 2008. ради као истраживач на Институту за телекомуникације (Instituto de Telecomunicações) у Лисабону, у оквиру Групе за безбедност и квантну информацију (Security and Quantum Information Group). У периоду 2009.-2014. члан је Центра за физику фундаменталних интеракција (Centro de Física das Interações Fundamentais), а од 2015. до 2019. Центра за Физику и инжењерство напредних материјала (Centro de Física e Engenharia de Materiais Avançados) Универзитета у Лисабону. Учесник је 13 међународних пројеката, а додатно је био руководилац једног међународног пројекта.

2. ПРЕГЛЕД НАУЧНЕ АКТИВНОСТИ

Кандидат се бави теоријом квантне информације у оквиру научне гране физика. Испод наводимо три главна правца истраживања кандидата. Бројеви референци одговарају оним из главе 5 овог Материјала за избор у звање.

Правца 1: Квантна теорија информације и квантна криптографија

Главни фокус истраживања су ОТ (Oblivious Transfer) и ВС (Bit Commitment) протоколи који омогућују извршење протокола безбедног вишекомпонентног рачунања (Secure Multiparty Computation). Експериментална демонстрација и до сада први пуни доказ безбедности практичног ОТ протокола су дати у [1]; видети исто [24] као и студије ОТ протокола [12,13,34] и ВС протокола [14,35,36]. Додатно, анализирани су протоколи за квантну размену кључа [7,10,42], потписивање уговора [15,27], као и извршавање криптографских задатака коришћењем идеалних (tamper-proof) уређаја [43]. Напоследку, анализирана је квантна Колмогоровљева комплексност [5], разни протоколи за обраду информација [9,32,40,41] и рану карактеризацију података временских серија (earliness of time-series data) [25].

Већина радова из овог правца је теоријског типа, али има и експерименталних, [1,7], као и нумеричких радова (као репрезентативни издвајамо [40]).

Правца 2: Информациона геометрија и примене на теорију вишечестичних система

Кандидат је био коаутор рада [3] који је засновао целу област истраживања фазних прелаза коришћењем фиделити функције (норма скаларног производа између два вектора квантних стања; скаларни производ индукује појмове норме и растојања, и омогућава примену техника из диференцијалне геометрије). Овај рад је до сада цитиран преко 700 пута. У протеклих двадесет година, овај метод је привукао пажњу великог броја, у почетку само теоријских, а у последње време и експерименталних физичара, доживео огроман развој, и постао етаблирани модерни поглед на *ојшћу теорију* фазних прелаза – превазилазећи Ландау-Гинзбургов приступ, као и остале дотадашње парцијалне приступе. Након иницијалног рада, објављеног 2006. године, кандидат је у оквиру овог правца објавио и читав низ даљих радова [2,11,16,17,22,23,28,29,31,33,39].

Радови из ове области су примарно теоријског типа, али готово сваки садржи и нумеричке симулације.

Правца 3: Квантна механика, информација и гравитација

Овај правац повезује квантну теорију информације са теоријом гравитације кроз анализу последица суперпозиције различитих квантних стања поља гравитације и материје. Показано је да гејџ симетрија теорије оставља простор само за уплетена (entangled) стања гравитације и материје [30]. Затим, показано је квантно нарушење Ајнштајновог слабог принципа еквиваленције, као и једнакости инерцијалне и гравитационе масе [26], што је даље анализирано у [38]. У [8] се анализира могућност постојања неодређених (indefinite) каузалних поредака. Такође, показано је да се интеракција апаратуре са вакуумом мора третирати на исти начин као и са физичким системом, дакле као квантна операција [6].

Поред анализе суперпозиција у гравитацији, предложен је операциони начин за верификацију основних особина класичног просторвремена – димензионалности и топологије [4].

Радови из ове области су примарно теоријског типа, али [4] и [30] такође садрже и нумеричке симулације.

3. ПРИКАЗ НАЈЗНАЧАЈНИЈИХ РЕЗУЛТАТА

Ниже је наведено пет најзначајнијих радова кандидата са сажетим описом одговарајућих резултата остварених у оцењиваном периоду који кандидата квалификују за избор у предложено научно звање у научној грани и дисциплини наведеној у извештају.

1. M. Lemus, P. Schiansky, M. Goulão, M. Bozzio, D. Elkouss, **N. Paunković**, P. Mateus and P. Walther, “Performance of Practical Quantum Oblivious Key Distribution”, *PRX Quantum* **6**, 040308 (2025). 36 pages. IF = 9.3
DOI: 10.1103/j8mt-c124

Безбедно вишекомпонентно рачунање (SMC) представља значајни алат за анализу података који штити приватност. SMC омогућује решавање великог броја криптографских проблема, од којих ћемо овде само навести електронско гласање и безбедно рударење података (secure data mining). С друге стране, ОТ протокол представља једног од главних кандидата за практичну имплементацију SMC протокола. У раду се предлаже практична реализација квантног рандомизованог ОТ протокола (Randomised Oblivious Transfer – ROT), за који је познато да омогућује реализацију ОТ протокола. Користећи само симетричне криптографске протоколе за имплементацију ОТ протокола, у раду је конструисан рачунарски безбедан ROT протокол без коришћења криптографије базиране на дељењу јавног кључа (public-key cryptography) и без претпоставки које намећу ограничења на уређаје коришћене за пресретање и декодирање размењених информација. Доказано је да протокол задовољава захтев сигурности базиране на неразличивости (indistinguishability-based notion of security). *Ово је посебно значајан резултат, јер представља први јуни доказ безбедности једног ОТ протокола реализованог у реалистичним условима применом данашње технологије.* Додатно, демонстрирана је експериментална имплементација предложеног ОТ протокола у циљу даљег тестирања његових перформанси у реалистичним условима. Коначно, безбедност и перформансе предложеног протокола су затим упоређене са квантним и класичним алтернативама, показујући потенцијалне предности у односу на постојећа решења заснована на употреби неидеалних квантних меморија са ограниченим временом складиштења информација (noisy storage model), као и решења заснована на криптографији јавног кључа.

Кандидат је учествовао у свим теоријским фазама израде рада (конкретно, у креирању протокола и у изради доказа његове безбедности), као и у обради експерименталних резултата.

2. F. Massa, P. Yadav, A. Moqanaki, W. O. Krawec, P. Mateus, **N. Paunković**, A. Souto and P. Walther, “Experimental semi-quantum key distribution with classical users”, *Quantum* **6**, 819 (2022). 27 pages. IF = 7.599
DOI: 10.22331/q-2022-09-22-819

У овом раду је предложен нови протокол који омогућава да два класична корисника деле тајни кључ користећи помоћ непоузданог, потенцијално непријатељски настројеног, квантног сервера. Конкретно, наш протокол захтева од Алисе и Боба (корисника који желе да размене тајни кључ) да изврше само две класичне операције, детекцију или рефлексију једног фотона, и стога поставља још мање ограничења корисницима него претходни протоколи ове природе, захтевајући само мерење једног фотона, без препарирања квантног стања фотона. *Ово је први рад у коме се показује да су њихви минимални захтеви, са стираних корисника, довољни за генерисање тајног кључа.* Сложеност сервера је такође смањена у поређењу са претходном литературом, јер сервер само препарира и мери појединачне квантне битове (фотоне). Додатно, у раду је дат информационо-теоријски доказ безбедности протокола под претпоставком практичних уређаја, први за протоколе такве природе (претходни радови на тему квантних протокола за размену тајног кључа са класичним корисницима у присуству квантног сервера били су ограничени на сценарије идеалних квантних битова), и израчуната је брзина размене тајног кључа у неасимптотском случају коначног броја извршавања основног протокола. Коначно, протокол

је експериментално демонстриран у реалистичним условима са присуством шума, коришћењем реалистичне апаратуре доступне на данашњем тржишту. Методи развијени у овом раду могу бити широко применљиви и на друге вишекомпонентне протоколе (протоколе са два и више корисника) у практичним условима.

Кандидат је учествовао у свим теоријским фазама израде рада (конкретно, у креирању протокола и у изради доказа његове безбедности), као и у обради експерименталних резултата.

3. P. Zanardi and **N. Paunković**,
“Ground state overlap and quantum phase transitions”,
Physical Review E **74**, 031123 (2006). 6 pages. IF = 2.438

У овом раду је предложена карактеризација квантних фазних прелаза коришћењем фиделити (fidelity) функције (функције преклапања између два основна квантна стања многочестичног система, добијена за две различите вредности спољашњих параметара Хамилтонијана система). На примерима Дикеовог (Dicke) и XY модела, показано је да су региони критичности система (regions of criticality) означени екстремним тачкама фиделити и фиделити суцептибилности функција. Даље, разматрана је веза између овог приступа и Андерсонове катастрофе ортогоналности (Anderson orthogonality catastrophe), као и са динамичком студијом Лошмитовог одјека (Loschmidt echo) за критичне системе. *Овај рад је од посебне важности, јер је остворио целу једну поделу теоријској, а касније ће се испоставити и експерименталној, правца у физици – анализа фазних прелаза и макроскопских особина многочестичних система базирана на фиделити функцији и информационој геометрији простора квантних стања.*

Кандидат је самостално написао прву верзију целокупног чланка. Додатно, оба коаутора рада су сваки самостално извршили целокупан теоријски рачун. Разлог томе је био да кандидат, као тада млади истраживач који је управо одбранио докторску тезу, стекне пуну самосталност у научном раду. Додатно, овиме је поверење у крајњи исход истраживачког рада повећано, јер су оба коаутора независно добила идентичне резултате.

4. B. Mera, C. Vlachou, **N. Paunković** and V. R. Vieira,
“Uhlmann connection in fermionic systems undergoing phase transitions”,
Physical Review Letters **119**, 015702 (2017). 6 pages. IF = 8.839
DOI: 10.1103/PhysRevLett.119.015702

У овом раду се анализира понашање Улманове (Uhlmann) конекције код фермионских система у близини региона фазних прелаза. Конкретно, анализирају се неки од парадигматских случајева једнодимензионалних тополошких изолатора и суперпроводника, као и BCS теорија суперпроводљивости у три димензије. У раду се показује да Улманова конекција сигнализира фазне прелазе у којима се мења својствени базис квантног стања система, док је за анализу фазних прелаза код система код којих је својствени базис фиксан (и до прелаза долази само услед промене својствених вредности), неопходно користити општије функције фиделити и фиделити суцептибилности, резултат који је први пут наговештен у [2]. Користећи етаблирани приступ анализи фазних прелаза базиран на фиделити функцији, и проучавањем ивичних стања (edge states), показује се одсуство термалних фазних прелаза у случају 1D тополошких изолатора и суперпроводника. Додатно, показује се да Улманова геометријска фаза разматрана у простору импулса није адекватна за анализу ових фазних прелаза, јер је само део информације садржане у Улмановој холономији. Заиста, као функција температуре, ова холономија је глатка, стога се не очекује феномен сличан фазном прелазу. *Ово је посебно важан резултат, јер побија ранији закључак о постојању фазног прелаза на основу анализе понашања само Улманове геометријске фазе.*

Иста анализа је извршена за 3Д случај BCS суперпроводника који, за разлику од претходних система, имају термалне фазне прелазе, који су потврђени понашањем како фиделити (суцептибилности), тако и Улмановом конекцијом. Ово показује да се, при промени температуре, оператор мешаног стања мења и на нивоу свог спектра и на нивоу својих својствених вектора. Поред тога, проучавање Мајорана модова на коначној температури отвара могућност конструкције стабилних квантних меморија у реалистичним условима. Коначно, анализа различитог понашања Улманове конекције за случајеве BCS

модела и Китајевљевог спинског ланца, сугерише да би у реалним сценаријима процеп (gap) тополошких суперпроводника такође, генерички, могао бити зависан од температуре.

Кандидат је дао иницијалну идеју за цео пројекат (из кога је произашао још један рад, [33]). Преко свог дугогодишњег сарадника проф. др Витора Роше Виеире (Vítor Rocha Vieira), стручњака у области теорије кондензованог стања, повезао је свог студента докторских студија Хришулу Влашу (Chrysoula Vlachou) са Бруном Мером (Bruno Mera), студентом проф. др Виеире. Кандидат је учествовао у свим фазама израде рада, који представља један од кључних резултата у изради докторских теза оба кандидата (као интердисциплинарни пројекат, овај рад се уклапао и у тезу Х.В. из области теорије информације, и у тезу Б.М. из области теорије кондензованог стања).

5. **N. Paunković** and M. Vojinović,

“Causal orders, quantum circuits and spacetime: distinguishing between definite and superposed causal orders”,

Quantum **4**, 275 (2020). 29 pages. IF = 6.777

DOI: 10.22331/q-2020-05-28-275

У раду се проучава појам каузалних поредака код (класичних и квантних) кола и за случај скупа просторвременских догађаја. Показано је да свако коло може бити уроњено у класично просторвреме, очувајући компатибилност између две каузалне структуре. Главни фокус рада је анализа недавно предложеног протокола под именом квантни прекидач. Користећи формализам процес матрица (process matrix formalism), анализирани су реализације квантног прекидача користећи 4 и 3 просторвременска догађаја у класичном просторвремену са фиксираним каузалним поретком, и реализација гравитационог прекидача са само 2 просторвременска догађаја који садржи суперпозиције различитих конфигурација гравитационог поља и њихових одговарајућих каузалних поредака. Показано је да тренутне експерименталне имплементације квантног прекидача не садрже суперпозиције каузалних поредака између просторвременских догађаја и да се ове суперпозиције могу јавити само у контексту суперпонираних гравитационих поља. Такође, разматран је недавно уведени појам операционог догађаја, који дозвољава суперпозиције каузалних поредака у имплементацијама квантног прекидача у равном просторвремену, као последица чињенице да се реализације квантног прекидача користећи 4 и 3 просторвременска догађаја у класичним просторвременима могу описати помоћу само два операциона догађаја. Рад предлаже опсерваблу која може разликовати квантне реализације прекидача у класичним просторвременима и имплементације гравитационог прекидача у суперпонираним просторвременима, *без декохеренције система у прекидачу. Ово је посебно значајан резултат јер љубија раније шврдње да је шакко нешшо немоћуће, шврдње која је била један од главних аргумента у прилој значаја новоуведеној појма операционој догађаја.* Коначно, извршена је анализа резултата овог рада у светлу модерног релационистичког приступа физици.

Кандидат је учествовао у свим фазама израде рада, у коме су оба коаутора дала подједнак допринос.

4. ПОКАЗАТЕЉИ УСПЕХА У НАУЧНОИСТРАЖИВАЧКОМ РАДУ

4.1. Утицајност

Др Никола Паунковић је у свом досадашњем раду објавио 50 научних публикација, међу којима 3 рада категорије M21a+, 18 радова категорије M21a, 16 радова категорије M21, 8 радова категорије M22, и 5 радова категорије M33.

Према бази података Web of Science, радови кандидата су цитирани укупно 1452 пута, од тога 1348 пута не рачунајући самоцитате. Према бази података Scopus, радови кандидата су цитирани укупно 1494 пута, од тога 1277 пута не рачунајући самоцитате и цитате коаутора. Хиршов индекс кандидата износи 14, како према бази Web of Science, тако и према бази Scopus. Релевантни подаци о цитираности из обе базе дати су у прилогу.

4.2. Међународна научна сарадња

Кандидат је провео укупно 25 година у иностранству (од тога 4 године на докторским студијама и 21 годину бавећи се научноистраживачким радом). Осим тога, сви радови кандидата представљају заједничке резултате категорија M21a+, M21a, M21 и M22 са колегама из разних земаља света. Осим сарадње коју је остварио са колегама из институција у којима је боравио као студент, односно истраживач, кандидат је током каријере имао сарадњу и са истраживачима из следећих институција (у загради су наведени бројеви одговарајућих радова као доказ, видети библиографију ниже):

- Vienna Center for Quantum Science and Technology (VCQ), Faculty of Physics, University of Vienna, Austria [1,7]
- Computer Science and Engineering Department, University of Connecticut, USA [7,10]
- Departments of Physics, Harvard University and MIT, Cambridge, Massachusetts, USA [31]
- School of Physics and Materials Science, Anhui University, Hefei, China [9,32]
- School of Electronic and Information Engineering, Hefei Normal University, China [9,32]
- Department of Computer Science, Sun Yat-sen University, Guangzhou, China [41]
- Networked Quantum Devices Unit, Okinawa Institute of Science and Technology Graduate University, Japan [1]
- QuTech, Delft University of Technology, Netherlands [1]
- Optical Quantum Communications Group, Instituto de Telecomunicações, Aveiro, Portugal [14,24,36]
- Institute of Physics Belgrade, University of Belgrade, Serbia [4,6,8,26,30,38]
- Lasige, Faculdade de Ciências da Universidade de Lisboa, Portugal [5,7,10,24,27,34]
- Faculty of Informatics, Masaryk University, Brno, Check Republic [15,43]
- Institute for Theoretical Physics, Heinrich-Heine-Universität Düsseldorf, Germany – Колаборација иницирана заједничком радионицом између групе у Дизелдорфу и групе у Лисабону коју је представљао кандидат са своја два бивша студента (Chrysoula Vlachou, Mariano Lemus). Веб страна радионице као и сертификат о предавању кандидата дати су у прилогу.

4.3. Руковођење пројектима и потпројектима (радним пакетима)

Кандидат је био руководилац португалског научноистраживачког тима за међународни пројект категорије VI, са називом “Noise and measurement errors in multi-party quantum security protocols”, из програма билатералне сарадње између Португалије и Србије, финансиран од стране португалске Фондације за науку и технологију (Fundação para a Ciência e a Tecnologia, FCT) и Министарства просвете, науке и технолошког развоја Републике Србије. Период реализације пројекта је 2015/2016.

У прилогу се налази писмо директора Департамента за међународне односе (DRI) португалске Фондације за науку и технологију, у коме се кандидат обавештава да је његов пројект одобрен за финансирање и имплементацију. Такође прилажемо и превод писма са португалског на српски језик, ради комплетности.

Додатно, кандидат учествује као члан управног одбора (Management Committee member) за две COST акције, CA23115 (“Relativistic quantum information”) и CA23130 (“Bridging high and low energies in search of quantum gravity”). У прилогу се налази слика званичних интернет страница обе акције, на којима се види да је кандидат члан управних одбора.

4.4. Уређивање научних публикација

Кандидат је био гостујући уредник (Guest Editor) за следеће часописе:

- Током 2021. године у часопису *Entropy* (ISSN 1099-4300, категорија M22), за специјално издање под називом “Information Geometry of Classical and Quantum States and Applications”. (a)

- Током 2022. године у часопису *Applied Sciences* (ISSN 2076-3417, категорија M21), за специјално издање под називом “Recent Development and Application of Quantum Communication and Security Protocols”. (б)
- Током 2022. године у часопису *Symmetry* (ISSN 2073-8994, категорија M21), за специјално издање под називом “Quantum Information and Condensed Matter Physics”. (в)

У прилогу се налазе сертификати за гостујућег уредника, као и копије званичних интернет страна специјалних издања часописа, на којима се види да је кандидат у случају првог специјалног издања био самостални гостујући уредник, док је у случају другог и трећег специјалног издања био први, односно други, гостујући уредник.

(а) https://www.mdpi.com/journal/entropy/special_issues/Information_Geometry_Quantum_States

(б) https://www.mdpi.com/journal/applsci/special_issues/Quantum_Communication_Security_Protocols

(в) https://www.mdpi.com/journal/symmetry/special_issues/Quantum_Information_Condensed_Matter_Physics

4.5. Предавања по позиву (осим на конференцијама)

Кандидат је током 2006. године био у посети групи Часлава Брукнера на Факултету за физику Универзитета у Бечу, Аустрија, и одржао предавање о примени метода из области квантне информације на решавање проблема у физици многочестичних система. У прилогу се налази позивно писмо др Брукнера од 16. фебруара 2006. године.

Током 2008. године кандидат је поново био у посети групи Часлава Брукнера на Факултету за физику Универзитета у Бечу, Аустрија, и одржао предавање под насловом “Macroscopic distinguishability between quantum states defining different phases of matter”. У прилогу се налазе позивно писмо др Брукнера од 17. јула 2007 и потврдно писмо од 29. октобра 2008. године.

Током 2017. године кандидат је био у посети групи Маркуса Хубера на Институту за квантну оптику и квантне информације Аустријске Академије Наука у Бечу, Аустрија, и одржао предавање под насловом “Quantum contract signing” (*). У прилогу се налази потврдно писмо др Хубера од 13. децембра 2017. године.

(*) <https://www.iqoqi-vienna.at/detail/event/invitation-to-a-talk-nikola-paunkovic-friday-nov-10th-2017-1430h-at-the-iqoqi-seminar-room>

4.6. Рецензирање пројеката и научних резултата

Кандидат је био рецензент за два национална научна пројекта (један пројект за Велс, Уједињено Краљевство, и један пројект за Пољску). У прилогу се налазе позиви и потврде о извршеним рецензијама за оба пројекта.

Такође, кандидат је током своје каријере био рецензент за велики број (преко стотину) научноистраживачких радова који су објављени у реномираним међународним научним часописима, па издавамо само најрепрезентативније часописе:

- *PRX Quantum*,
- *Physical Review Letters*,
- *Physical Review A*,
- *Physical Review B*,
- *Physical Review E*,
- *npj Quantum Information*,
- *Quantum*.

У прилогу се налазе позивна писма и писма захвалнице уредника горњих часописа за извршене рецензије.

4.7. **Образовање научних кадрова**

Кандидат је у току своје каријере био ментор односно коментор за шест студената докторских студија на Универзитету у Лисабону. По правилима Универзитета у Лисабону, један од коментора увек мора да има наставно звање на Универзитету, па је због тога кандидат у пет случајева коментор са још једним истраживачем са Универзитета, а у једном случају коментор са још два истраживача са Универзитета.

Будући да је на Универзитету у Лисабону процедура израде и одбране докторске дисертације у потпуности организована електронски, не постоје папирни документи којима би се доказало менторство кандидата. Уместо тога, једини докази који кандидат има да је радио у својству коментора су: званична интернет страница одбрањене докторске дисертације кандидата на сајту матичне институције кандидата (Instituto Superior Técnico, Universidade de Lisboa), насловна страна тезе, и заједнички радови које кандидат има са студентима.

Ниже је дат хронолошки списак студената и информације о њиховим дисертацијама, укључујући и бројеве радова који су заједнички за кандидата и студента (бројеви одговарају радовима у библиографији кандидата датом ниже). Такође, у прилогу су дате званичне интернет странице, као и насловне стране дисертација.

- (1) João Paulo do Amaral de Jesus Rodrigues,
“Quantum oblivious transfer”
Instituto Superior Técnico, Universidade de Lisboa, 07.04.2017.
Ментори: Paulo Alexandre Carreira Mateus, **Nikola Paunković**
Интернет страна:
<https://scholar.tecnico.ulisboa.pt/records/cBDLP-wzyZgmmYx-LAgdckTjba4a0-5CFxZt>
Заједнички радови кандидата и студента: [34,40,42]
- (2) Chrysoula Vlachou,
“Quantum walks in cryptography and finite-temperature topological phase transitions”
Instituto Superior Técnico, Universidade de Lisboa, 07.09.2018.
Ментори: Paulo Alexandre Carreira Mateus, **Nikola Paunković**
Интернет страна:
<https://scholar.tecnico.ulisboa.pt/records/U35zmFxH7NAWQqfN7ebx8UwFMHpcoR1XriYp>
Заједнички радови кандидата и студента: [10,11,29,31,33,42]
- (3) Syed Tahir Amin,
“Tracking topological phase transitions using quantum information geometric quantities”
Instituto Superior Técnico, Universidade de Lisboa, 28.02.2020.
Ментори: **Nikola Paunković**, Vitor Rocha Vieira
Интернет страна:
https://scholar.tecnico.ulisboa.pt/records/W1mxqMS6keYGPzdlus1jF_O82wrPNN_YP1dp
Заједнички радови кандидата и студента: [22,29,39]
- (4) Preeti Yadav,
“Practical Quantum Privacy Protocols”
Instituto Superior Técnico, Universidade de Lisboa, 06.11.2020.
Ментори: Paulo Alexandre Carreira Mateus, **Nikola Paunković**, André Nuno Carvalho Souto
Интернет страна:
https://scholar.tecnico.ulisboa.pt/records/IHBmE_semaCn7JCFqOIRNaubyBU7JuDJ76Px2
Заједнички радови кандидата и студента: [7,27]

(5) Mariano José Lemus Hernández,
“Asymmetric Quantum Cryptography and Multipartite Correlations”
Instituto Superior Técnico, Universidade de Lisboa, 16.03.2022.
Ментори: Paulo Alexandre Carreira Mateus, **Nikola Paunković**
Интернет страна:
<https://scholar.tecnico.ulisboa.pt/records/w6VWWC3joK1utlZwXNebQb4mGvRF7vAV5xSd>
Заједнички радови кандидата и студента: [1,5,24,25]

(6) Ricardo André Faleiro Miguel,
“Nonlocality and Contextuality: Concepts and Applications in Quantum Information”
Instituto Superior Técnico, Universidade de Lisboa, 04.03.2022.
Ментори: Paulo Alexandre Carreira Mateus, **Nikola Paunković**
Интернет страна:
https://scholar.tecnico.ulisboa.pt/records/xyvDikbyMVTC18SDiqp1LMozJ_2NsRm3DlcE
Заједнички радови кандидата и студента: [6]

4.8. Награде и признања

Кандидат није био добитник награда и признања у смислу члана 27 Правилника о стицању истраживачких и научних звања Министарства науке, технолошког развоја и иновација Републике Србије.

4.9. Допринос развоју одговарајућег научног правца

У току протеклих 20 година након одбране докторске тезе, кандидат је остварио изражену самосталност и у великој већини публикација дао значајан допринос. Стога ћемо овде навести само скраћени списак репрезентативних радова, који нису у вези са докторском дисертацијом, нити су рађени у колаборацији са коменторима. Велики број ових радова је рађен у оквиру докторских студија кандидативних студената, чија се имена по правилу наводе испред имена кандидата у списку аутора. Такође, у неким радовима аутори су поређани абecedним редом. Коначно, у радовима експерименталног карактера редослед аутора је следећи: на почетку студенти, затим постдокови, старији сарадници, и на крају руководицац експерименталног тима.

Из области квантне криптографије се посебно издвајају радови [1,24] који се баве реализацијом практичног ОТ протокола и доказом његове безбедности, и [7] у коме се анализира протокол у коме два класична корисника деле тајни кључ уз помоћ квантног сервера. Радови [1] и [7] представљају прва два значајна резултата из главе 3 овог документа. Поред њих, значајни су и радови [14,35,36] у којима се анализира једна врста ВС протокола. Треба истаћи да је у раду [36] представљена прва експериментална реализација неког квантног криптографског протокола у Португалији. Такође, значајни су и радови [15,27] у којима се анализирају два протокола за фер потписивање уговора, један базиран на размени чистих квантних стања, други на размени уплетених. Оба протокола је предложио кандидат, и учествовао у њиховој безбедоносној анализи.

Из области квантне теорије информације, значајан је скорији рад [5] који се бави квантном Колмогоровљевом комплексношћу и квантним корелацијама. Такође, значајни су и радови [9,32] у којима је кандидат са колегама из Кине анализирао два протокола за креирање и манипулацију уплетених стања.

Као коаутор рада [3] (трећи значајни резултат из главе 3) који је покренуо област проучавања фазних прелаза на основу анализе фиделити функције, кандидат је био коаутор укупно 12 радова и у сваком од њих је имао значајну улогу. Међу њима, поред [3], посебно се истиче [2], у коме је показана директна веза између фиделити суспенцибилности и термодинамичке суспенцибилности у Стонер-Хабардовом моделу магнетизма. Такође, значајан је и рад [11] (и са њим повезан рад [33]) који представља четврти значајни резултат из главе 3. Додатно, требало би посебно поменути [23], у коме се *ајсџиракџи*

механизам нарушења симетрије (за разлику од познатог Ландау-Гинзбурговог механизма нарушења локалне симетрије) доводи у везу са фиделити приступом анализи фазних прелаза, и [31] у коме се разматра нова врста такзованих динамичких фазних прелаза.

Напоследку, кандидат је у свих 6 радова на тему укрштања теорије информације и гравитације [4,6,8,26,30,38] имао значајну улогу. Као посебно значајан треба издвојити рад [8] који представља пети значајни резултат из главе 3. Такође, вредни посебног помена су и радови у којима се показује нарушење слабог принципа еквиваленције [26] и даје једно опште објашњење за постојање класичног лимеса [30] у присуству суперпонираних стања гравитационог поља.

5. БИБЛИОГРАФИЈА КАНДИДАТА

Напомена: с обзиром да кандидат до сада никада није био биран у научно звање, публикације нису подељене у скупове пре односно након избора у претходно научно звање. На основу члана 18. став 3. Правилника о стицању истраживачких и научних звања Републике Србије, научни резултати кандидата приказују се каријерно (комплетна научна продукција) у погледу оцењиваног периода.

Публикације категорије M21a+

[1] M. Lemus, P. Schiansky, M. Goulão, M. Bozzio, D. Elkouss, **N. Paunković**, P. Mateus and P. Walther, “Performance of Practical Quantum Oblivious Key Distribution”, *PRX Quantum* **6**, 040308 (2025). 36 pages. IF = 9.3
DOI: 10.1103/j8mt-c124

[2] **N. Paunković** and V. R. Vieira, “Macroscopic distinguishability between quantum states defining different phases of matter: Fidelity and the Uhlmann geometric phase”, *Physical Review E* **77**, 011129 (2008). 14 pages. IF = 2.438
DOI: 10.1103/PhysRevE.77.011129

[3] P. Zanardi and **N. Paunković**, “Ground state overlap and quantum phase transitions”, *Physical Review E* **74**, 031123 (2006). 6 pages. IF = 2.438
DOI: 10.1103/PhysRevE.74.031123

Публикације категорије M21a

[4] **N. Paunković** and M. Vojinović, “Operational verification of the existence of a spacetime manifold”, *Quantum* **9**, 1753 (2025). 17 pages. IF = 7.2
DOI: 10.22331/q-2025-05-22-1753

[5] M. Lemus, R. Faleiro, P. Mateus, **N. Paunković**, A. Souto, “Quantum Kolmogorov complexity and quantum correlations in deterministic-control quantum Turing machines”, *Quantum* **8**, 1230 (2024). 29 pages. IF = 7.9
DOI: 10.22331/q-2024-01-18-1230

[6] R. Faleiro, **N. Paunković** and M. Vojinović, “Operational interpretation of the vacuum and process matrices for identical particles”, *Quantum* **7**, 986 (2023). 15 pages. IF = 7.9
DOI: 10.22331/q-2023-04-20-986

[7] F. Massa, P. Yadav, A. Moqanaki, W. O. Krawec, P. Mateus, **N. Paunković**, A. Souto and P. Walther, “Experimental semi-quantum key distribution with classical users”, *Quantum* **6**, 819 (2022). 27 pages. IF = 7.599
DOI: 10.22331/q-2022-09-22-819

- [8] **N. Paunković** and M. Vojinović,
 “Causal orders, quantum circuits and spacetime: distinguishing between definite and superposed causal orders”,
Quantum **4**, 275 (2020). 29 pages. IF = 6.777
 DOI: 10.22331/q-2020-05-28-275
- [9] L. Ju, M. Yang, **N. Paunković**, W.-J. Chu and Z.-L. Cao,
 “Creating photonic GHZ and W states via quantum walk”,
Quantum Information Processing **18**, 176 (2019). 12 pages. IF = 2.433
 DOI: 10.1007/s11128-019-2293-7
- [10] C. Vlachou, W. Krawec, P. Mateus, **N. Paunković** and A. Souto,
 “Quantum key distribution with quantum walks”,
Quantum Information Processing **17**, 288 (2018). 37 pages. IF = 2.337
 DOI: 10.1007/s11128-018-2055-y
- [11] B. Mera, C. Vlachou, **N. Paunković** and V. R. Vieira,
 “Uhlmann connection in fermionic systems undergoing phase transitions”,
Physical Review Letters **119**, 015702 (2017). 6 pages. IF = 8.839
 DOI: 10.1103/PhysRevLett.119.015702
- [12] A. Souto, P. Mateus, P. Adão and **N. Paunković**,
 “Reply to ‘Comment on Bit-string oblivious transfer based on quantum state computational indistinguishability’”,
Physical Review A **92**, 046302 (2015). 4 pages. IF = 2.991
 DOI: 10.1103/PhysRevA.92.046302
- [13] A. Souto, P. Mateus, P. Adão and **N. Paunković**,
 “Bit-string oblivious transfer based on quantum state computational indistinguishability”,
Physical Review A **91**, 042306 (2015). 11 pages. IF = 2.991
 DOI: 10.1103/PhysRevA.91.042306
- [14] R. Loura, A. J. Almeida, P. S. André, A. N. Pinto, P. Mateus and **N. Paunković**,
 “Noise and measurement errors in a practical two-state quantum bit commitment protocol”,
Physical Review A **89**, 052336 (2014). 15 pages. IF = 3.042
 DOI: 10.1103/PhysRevA.89.052336
- [15] **N. Paunković**, J. Bouda and P. Mateus,
 “Fair and optimistic quantum contract signing”,
Physical Review A **84**, 062331 (2011). 11 pages. IF = 2.895
 DOI: 10.1103/PhysRevA.84.062331
- [16] P. D. Sacramento, **N. Paunković** and V. R. Vieira,
 “Fidelity spectrum and phase transitions of quantum systems”,
Physical Review A **84**, 062318 (2011). 12 pages. IF = 2.895
 DOI: 10.1103/PhysRevA.84.062318
- [17] **N. Paunković**, P. D. Sacramento, P. Nogueira, V. R. Vieira and V. K. Dugaev,
 “Fidelity between partial states as signature of quantum phase transitions”,
Physical Review A **77**, 052302 (2008). 10 pages. IF = 3.047
 DOI: 10.1103/PhysRevA.77.052302
- [18] Y. Omar, **N. Paunković**, L. Sheridan and S. Bose,
 “Quantum walk on a line with two entangled particles”,
Physical Review A **74**, 042304 (2006). 7 pages. IF = 3.047
 DOI: 10.1103/PhysRevA.74.042304

[19] S. Bose, A. Ekert, Y. Omar, **N. Paunković** and V. Vedral,
“Optimal state discrimination using particle statistics”,
Physical Review A **68**, 052309 (2003). 4 pages. IF = 2.986
DOI: 10.1103/PhysRevA.68.052309

[20] **N. Paunković**, Y. Omar, S. Bose and V. Vedral,
“Entanglement concentration using quantum statistics”,
Physical Review Letters **88**, 187903 (2002). 4 pages. IF = 7.323
DOI: 10.1103/PhysRevLett.88.187903

[21] Y. Omar, **N. Paunković**, S. Bose and V. Vedral,
“Spin-space entanglement transfer and quantum statistics”,
Physical Review A **65**, 062305 (2002). 4 pages. IF = 2.986
DOI: 10.1103/PhysRevA.65.062305

Публикације категорије M21

[22] B. Mera, **N. Paunković**, S. T. Amin and V. R. Vieira,
“Information geometry of quantum critical submanifolds: relevant, marginal and irrelevant operators”,
Physical Review B **106**, 155101 (2022). 10 pages. IF = 4.036
DOI: 10.1103/PhysRevB.106.155101

[23] H. Silva, B. Mera and **N. Paunković**,
“Interferometric geometry from symmetry-broken Uhlmann gauge group with applications to topological phase transitions”,
Physical Review B **103**, 095127 (2021). 12 pages. IF = 4.036
DOI: 10.1103/PhysRevB.103.085127

[24] M. Lemus, M. F. Ramos, P. Yadav, N. A. Silva, N. J. Muga, A. Souto, **N. Paunković**, P. Mateus and A. N. Pinto,
“Generation and distribution of quantum oblivious keys for secure multiparty computation”,
Applied Sciences **10**, 4080 (2020). 11 pages. IF = 2.736
DOI: 10.3390/app10124080

[25] M. Lemus, **N. Paunković**, A. M. Carvalho and P. Mateus,
“Information-theoretical criteria for characterizing the earliness of time-series data”,
Entropy **22**, 49 (2019). 22 pages. IF = 2.530
DOI: 10.3390/e22010049

[26] F. Pipa, **N. Paunković** and M. Vojinović,
“Entanglement-induced deviation from the geodesic motion in quantum gravity”,
Journal of Cosmology and Astroparticle Physics **09**, 057 (2019). 38 pages. IF = 5.524
DOI: 10.1088/1475-7516/2019/09/057

[27] P. Yadav, P. Mateus, **N. Paunković** and A. Souto,
“Quantum contract signing with entangled pairs”,
Entropy **21**, 821 (2019). 26 pages. IF = 2.530
DOI: 10.3390/e21090821

[28] P. D. Sacramento, B. Mera and **N. Paunković**,
“Vanishing k -space fidelity and the bulk-edge-bulk correspondence”,
Annals of Physics **401**, 40 (2019). 19 pages. IF = 2.367
DOI: 10.1016/j.aop.2018.11.021

[29] S. T. Amin, B. Mera, C. Vlachou, **N. Paunković** and V. R. Vieira,
“Fidelity and Uhlmann connection analysis of topological phase transitions in two dimensions”,
Physical Review B **98**, 245141 (2018). 19 pages. IF = 3.836
DOI: 10.1103/PhysRevB.98.245141

- [30] **N. Paunković** and M. Vojinović,
 “Gauge protected entanglement between gravity and matter”,
Classical and Quantum Gravity **35**, 185015 (2018). 27 pages. IF = 3.487
 DOI: 10.1088/1361-6382/aad7f1
- [31] B. Mera, C. Vlachou, **N. Paunković**, V. R. Vieira and O. Viyuela,
 “Dynamical phase transitions at finite temperature from fidelity and interferometric Loschmidt echo induced metrics”,
Physical Review B **97**, 094110 (2018). 15 pages. IF = 3.836
 DOI: 10.1103/PhysRevB.97.094110
- [32] X.-M. Li, M. Yang, **N. Paunković**, D.-C. Li and Z.-L. Cao,
 “Entanglement swapping via three-step quantum walk-like protocol”,
Physics Letters A **381**, 3875 (2017). 5 pages. IF = 1.772
 DOI: 10.1016/j.physleta.2017.10.022
- [33] B. Mera, C. Vlachou, **N. Paunković** and V. R. Vieira,
 “Boltzmann-Gibbs states in topological quantum walks and associated many-body systems: fidelity and Uhlmann parallel transport analysis of phase transitions”,
Journal of Physics A: Math. Theor. **50**, 365302 (2017). 17 pages. IF = 1.963
 DOI: 10.1088/1751-8121/aa820e
- [34] J. Rodrigues, P. Mateus, **N. Paunković** and A. Souto,
 “Oblivious transfer based on single-qubit rotations”,
Journal of Physics A: Math. Theor. **50**, 205301 (2017). 25 pages. IF = 1.963
 DOI: 10.1088/1751-8121/aa6a69
- [35] R. Loura, D. Arsenović, **N. Paunković**, D. B. Popović and S. Prvanović,
 “Security of two-state and four-state practical bit commitment protocols”,
Physical Review A **94**, 062335 (2016). 11 pages. IF = 2.925
 DOI: 10.1103/PhysRevA.94.062335
- [36] A. J. Almeida, A. Stojanovic, **N. Paunković**, R. Loura, N. Muga, N. Silva, P. Mateus, P. S. André and A. Pinto,
 “Implementation of a two-state quantum bit commitment protocol in optical fibers”,
Journal of Optics **18**, 015202 (2016). 9 pages. IF = 2.059
 DOI: 10.1088/2040-8978/18/1/015202
- [37] V. Božin, M. Hruška, **N. Paunković** and F. Herbut,
 “On statistical and deterministic quantum teleportation”,
Journal of Physics A: Math. Gen. **31**, 4403 (1998). 33 pages. IF = 1.545
 DOI: 10.1088/0305-4470/31/19/008

Публикације категорије M22

- [38] **N. Paunković** and M. Vojinović,
 “Equivalence principle in classical and quantum gravity”,
Universe **8**, 598 (2022). 16 pages. IF = 2.9
 DOI: 10.3390/universe8110598
- [39] S. T. Amir, B. Mera, **N. Paunković** and V. R. Vieira,
 “Information geometric analysis of long range topological superconductors”,
Journal of Physics: Condensed Matter **31**, 485402 (2019). 8 pages. IF = 2.711
 DOI: 10.1088/1361-648X/ab3c70

- [40] J. Rodrigues, **N. Paunković** and P. Mateus,
 “A simulator for discrete quantum walks on lattices”,
International Journal of Modern Physics C **28**, 1750055 (2017). 27 pages. IF = 1.195
 DOI: 10.1142/S0129183117500553
- [41] H. Situ, D. Qiu, P. Mateus and **N. Paunković**,
 “Secure N-dimensional simultaneous dense coding and applications”,
International Journal of Quantum Information **13**, 1550051 (2015). 25 pages. IF = 0.992
 DOI: 10.1142/S0219749915500513
- [42] C. Vlachou, J. Rodrigues, P. Mateus, **N. Paunković** and A. Souto,
 “Quantum walk public-key cryptographic system”,
International Journal of Quantum Information **13**, 1550050 (2015). 10 pages. IF = 0.992
 DOI: 10.1142/S0219749915500501
- [43] J. Bouda, P. Mateus, **N. Paunković** and J. Rasga,
 “On the power of quantum tamper-proof hardware”,
International Journal of Quantum Information **6**, 219 (2008). 22 pages. IF = 0.774
 DOI: 10.1142/S0219749908003542
- [44] L. Sheridan, **N. Paunković**, Y. Omar and S. Bose,
 “Discrete time quantum walk on a line with two particles”,
International Journal of Quantum Information **4**, 573 (2006). 11 pages. IF = 0.681
 DOI: 10.1142/S0219749906002006
- [45] Č. Brukner, **N. Paunković**, T. Rudolph and V. Vedral,
 “Entanglement-assisted orientation in space”,
International Journal of Quantum Information **4**, 365 (2006). 6 pages. IF = 0.681
 DOI: 10.1142/S0219749906001839

Публикације категорије M33

- [46] N. A. Silva, M. J. Ferreira, A. Carvalho, A. Souto, **N. Paunković**, P. Mateus, A. Teixeira and A. Pinto,
 “A network server for distributing quantum random numbers”,
 23rd International Conference of Transparent Optical Network (ICTON), Bucharest, Romania 2023.
IEEE Xplore digital library (2023). 4 pages.
 DOI: 10.1109/ICTON59386.2023.10207372
- [47] M. Lemus, P. Yadav, P. Mateus, **N. Paunković** and A. Souto,
 “On minimal assumptions to obtain a universally composable quantum bit commitment”,
 21st International Conference of Transparent Optical Network (ICTON), Angers, France 2019.
IEEE Xplore digital library (2019). 4 pages.
 DOI: 10.1109/ICTON.2019.8840386
- [48] **N. Paunković** and M. Vojinović,
 “Gravity-matter entanglement in Regge quantum gravity”,
 3rd International Symposium about Quantum Mechanics based on a “Deeper Level Theory”, Vienna, Austria,
 2015.
Proceedings of the EmQM15 conference, Journal of Physics: Conference Series **701**, 012035 (2016). 3 pages.
 DOI: 10.1088/1742-6596/701/1/012035
- [49] P. Mateus, **N. Paunković**, J. Rodrigues and A. Souto,
 “Enhancing privacy with quantum networks”,
 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, 2014.
Proceedings of CMS 2014, Lecture Notes in Computer Science, volume 8735, eds. B. de Decker and
 A. Zúquete, Springer (2014). 7 pages.
 DOI: 10.1007/978-3-662-44885-4_14

[50] A. Almeida, R. Loura, **N. Paunković**, N. Silva, N. Muga, P. Mateus, P. André and A. Pinto, "A brief review on quantum bit commitment", Second International Conference on Applications of Optics and Photonics, Aveiro, Portugal, 2014. *SPIE digital library*, Proceedings Volume 9286, page 92861C (2014). 8 pages. DOI: 10.1117/12.2063733

6. КВАНТИФИКАЦИЈА НАУЧНИХ РЕЗУЛТАТА КАНДИДАТА

Врста резултата	Вредност резултата (Прилог 2)	Укупан број резултата (укупан број резултата који подлежу нормирању)	Укупан број бодова (укупан број бодова након нормирања)
M21a+	20	3 (0)	60 (60)
M21a	12	18 (9)	216 (193.71)
M21	8	16 (5)	128 (116.39)
M22	5	8 (4)	40 (36.07)
M33	1	5 (4)	5 (4.20)
УКУПНО		50 (22)	449 (410.37)

Поређење са минималним квантитативним условима за избор у тражено научно звање

Диференцијални услов за оцењивани период за избор у научно звање: научни саветник (са прескакањем звања научни сарадник и виши научни сарадник)	Неопходно	Остварени нормирани број бодова
Укупно	$2 \times (16 + 50 + 70) = 272$	410.37
Обавезни: M11+M12+ M21+M22+M91+M92+M93	$2 \times (6 + 35 + 40) = 162$	406.17

Испуњени квалитативни критеријуми (за избор у звање научни саветник потребна су бар четири квалитативна услова са збирне листе А и Б, од којих бар један са листе А):

A1, A2, A4, Б1, Б2, Б4, Б5, Б6, Б7, Б9



Citation Report

Nikola Paunkovic (Author)

Analyze Results

Create Alert

Export Full Report

Publications

48

Total

From 1985 to 2025

Citing Articles

1,165

Total

1,130

Without self-citations

Times Cited

1,452

Total

1,348

Without self-citations

30.25

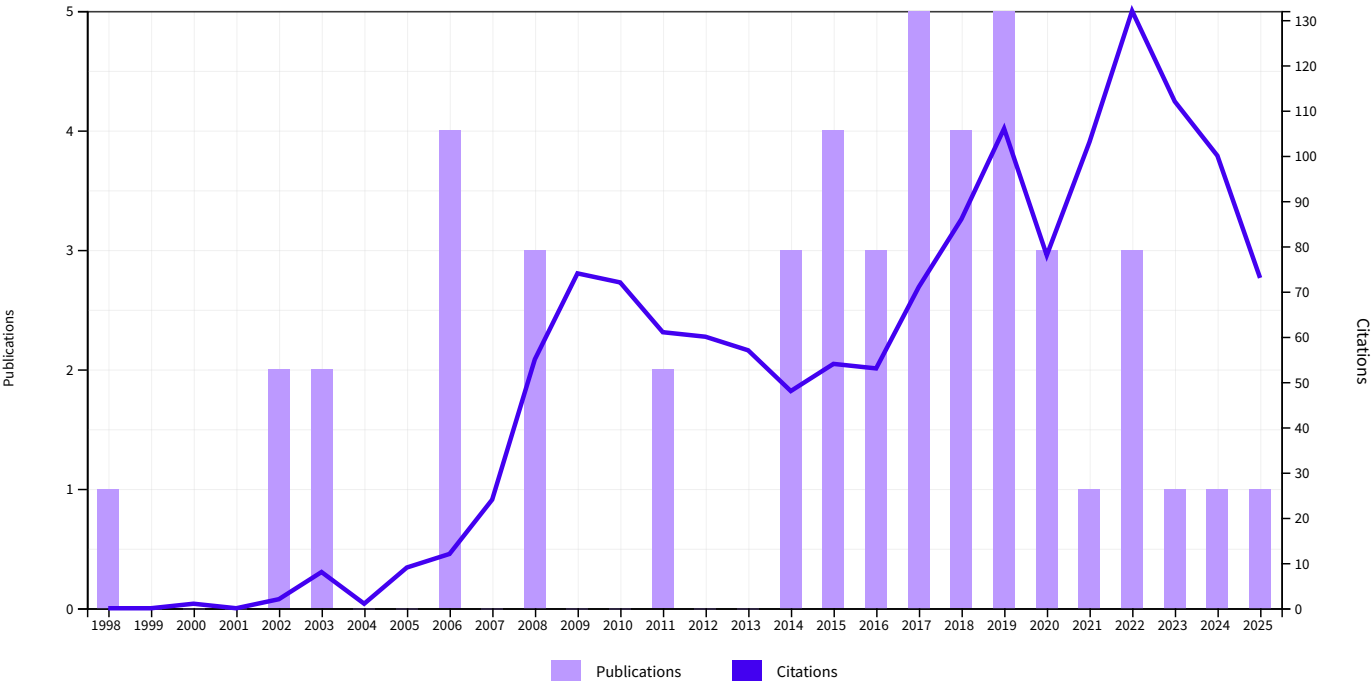
Average per item

14

H-Index

Times Cited and Publications Over Time

DOWNLOAD



48 Publications		Citations						
		Citations					Average per year	Total
		2021	2022	2023	2024	2025		
Total		103	132	112	100	73	55.85	1,452
1	Ground state overlap and quantum phase transitions Zanardi, P and Paunkovic, N Sep 2006 PHYSICAL REVIEW E 74 (3)	42	46	39	28	34	34.7	694
2	Quantum walk on a line with two entangled particles Omar, Y; Paunkovic, N; (...); Rose, S	4	6	3	5	4	5.65	113

⊖ 3	Fidelity between partial states as a signature of quantum phase transitions Paunkovic, N; Sacramento, PD; (...); Dugaev, VK May 2008 PHYSICAL REVIEW A ▾ 77 (5)	3	4	2	1	1	4	72
⊖ 4	Dynamical phase transitions at finite temperature from fidelity and interferometric Loschmidt echo induced metrics Mera, B; Vlachou, C; (...); Viyuela, O Mar 23 2018 PHYSICAL REVIEW B ▾ 97 (9)	10	8	9	11	2	7.5	60
⊖ 5	Quantum key distribution with quantum walks Vlachou, C; Krawec, W; (...); Souto, A Nov 2018 QUANTUM INFORMATION PROCESSING ▾ 17 (11)	9	11	4	7	1	5.38	43
⊖ 6	Uhlmann Connection in Fermionic Systems Undergoing Phase Transitions Mera, B; Vlachou, C; (...); Vieira, VR Jul 7 2017 PHYSICAL REVIEW LETTERS ▾ 119 (1)	4	3	5	4	1	4.22	38
⊖ 7	Macroscopic distinguishability between quantum states defining different phases of matter: Fidelity and the Uhlmann geometric phase Paunkovic, N and Vieira, VR Jan 2008 PHYSICAL REVIEW E ▾ 77 (1)	2	2	2	1	0	2.11	38
⊖ 8	Entanglement concentration using quantum statistics - art. no. 187903 Paunkovic, N; Omar, Y; (...); Vedral, V May 6 2002 PHYSICAL REVIEW LETTERS ▾ 88 (18)	1	3	3	0	0	1.5	36
⊖ 9	Causal orders, quantum circuits and spacetime: distinguishing between definite and superposed causal orders Paunkovic, N and Vojinovic, M May 23 2020 QUANTUM ▾ 4	3	10	7	9	4	5.83	35
⊖ 10	Quantum walk public-key cryptographic system Vlachou, C; Rodrigues, J; (...); Souto, A Oct 2015 INTERNATIONAL JOURNAL OF QUANTUM INFORMATION ▾ 13 (7)	4	3	3	4	7	2.82	31
⊖ 11	Spin-space entanglement transfer and quantum statistics - art. no. 062305 Omar, Y; Paunkovic, N; (...); Vedral, V Jun 2002 PHYSICAL REVIEW A ▾ 65 (6)	0	2	1	0	0	1.21	29
	Optimal state discrimination using particle statistics - art. no. 052309	0	2	1	0	0	0.87	26 0

12	Bose, S; Ekert, A; (...); Vedral, V Nov 2003 PHYSICAL REVIEW A ▾ 68 (5)							
13	Noise and measurement errors in a practical two-state quantum bit commitment protocol Loura, R; Almeida, AJ; (...); Paunkovic, N May 30 2014 PHYSICAL REVIEW A ▾ 89 (5)	2	1	0	1	1	1.58	19
14	Fidelity and Uhlmann connection analysis of topological phase transitions in two dimensions Amin, ST; Mera, B; (...); Vieira, VR Dec 26 2018 PHYSICAL REVIEW B ▾ 98 (24)	4	4	4	2	0	2.25	18
15	Boltzmann-Gibbs states in topological quantum walks and associated many-body systems: fidelity and Uhlmann parallel transport analysis of phase transitions Mera, B; Vlachou, C; (...); Vieira, VR Sep 8 2017 JOURNAL OF PHYSICS A-MATHEMATICAL AND THEORETICAL ▾ 50 (36)	2	0	1	1	0	1.44	13
16	Entanglement-assisted orientation in space Brukner, C; Paunkovic, N; (...); Vedral, V Apr 2006 INTERNATIONAL JOURNAL OF QUANTUM INFORMATION ▾ 4 (2) , pp.365-370	0	1	2	2	1	0.65	13
17	Secure N -dimensional simultaneous dense coding and applications Situ, H; Qiu, D; (...); Paunkovic, N Oct 2015 INTERNATIONAL JOURNAL OF QUANTUM INFORMATION ▾ 13 (7)	1	2	0	0	0	1.09	12
18	Bit-string oblivious transfer based on quantum state computational distinguishability Souto, A; Mateus, P; (...); Paunkovic, N Apr 8 2015 PHYSICAL REVIEW A ▾ 91 (4)	1	2	1	1	1	1.09	12
19	Fair and optimistic quantum contract signing Paunkovic, N; Bouda, J and Mateus, P Dec 29 2011 PHYSICAL REVIEW A ▾ 84 (6)	0	1	1	2	0	0.8	12
20	Fidelity spectrum and phase transitions of quantum systems Sacramento, PD; Paunkovic, N and Vieira, VR Dec 21 2011 PHYSICAL REVIEW A ▾ 84 (6)	1	1	1	0	0	0.8	12
21	Creating photonic GHZ and W states via quantum walk Ju, L; Yang, M; (...); Cao, ZL Jun 2019 QUANTUM INFORMATION PROCESSING ▾ 18 (6)	2	2	2	2	2	1.57	11

26

22	Implementation of a two-state quantum bit commitment protocol in optical fibers Almeida, AJ; Stojanovic, AD; (...); Pinto, AN Jan 2016 JOURNAL OF OPTICS ▾ 18 (1)	0	1	0	1	1	1.1	11
23	Interferometric geometry from symmetry-broken Uhlmann gauge group with applications to topological phase transitions Silva, H; Mera, B and Paunkovic, N Feb 19 2021 PHYSICAL REVIEW B ▾ 103 (8)	0	2	4	3	1	2	10
24	Generation and Distribution of Quantum Oblivious Keys for Secure Multiparty Computation Lemus, M; Ramos, ME; (...); Pinto, AN Jun 2020 APPLIED SCIENCES-BASEL ▾ 10 (12)	2	3	2	1	2	1.67	10
25	Quantum Contract Signing with Entangled Pairs Yadav, P; Mateus, P; (...); Souto, A Sep 2019 ENTROPY ▾ 21 (9)	0	4	3	2	0	1.29	9
26	Entanglement swapping via three-step quantum walk-like protocol Li, XM; Yang, M; (...); Cao, ZL Dec 13 2017 PHYSICS LETTERS A ▾ 381 (46) , pp.3875-3879	1	1	1	0	2	1	9
27	Oblivious transfer based on single-qubit rotations Rodrigues, J; Mateus, P; (...); Souto, A May 19 2017 JOURNAL OF PHYSICS A-MATHEMATICAL AND THEORETICAL ▾ 50 (20)	1	2	0	0	1	0.78	7
28	Security of two-state and four-state practical quantum bit-commitment protocols Loura, R; Arsenovic, D; (...); Prvanovic, S Dec 27 2016 PHYSICAL REVIEW A ▾ 94 (6)	0	0	0	1	0	0.7	7
29	Equivalence Principle in Classical and Quantum Gravity Paunkovic, N and Vojinovic, M Nov 2022 UNIVERSE ▾ 8 (11)	0	0	2	2	2	1.5	6
30	Information geometry of quantum critical submanifolds: Relevant, marginal, and irrelevant operators Mera, B; Paunkovic, N; (...); Vieira, VR Oct 3 2022 PHYSICAL REVIEW B ▾ 106 (15)	0	0	2	3	1	1.5	6

31	Vanishing k-space fidelity and phase diagram's bulk-edge-bulk correspondence Sacramento, PD; Mera, B and Paunkovic, N Feb 2019 ANNALS OF PHYSICS ▾ 401 , pp.40-58	2	0	1	1	1	0.86	6
32	On the power of quantum tamper-proof devices Bouda, J; Mateus, P; (...); Rasga, J Lisbon Quantum Computation, Information and Logic Meeting on Quantum Cryptography and Security Apr 2008 INTERNATIONAL JOURNAL OF QUANTUM INFORMATION ▾ 6 (2) , pp.281-302	0	1	0	0	0	0.33	6
33	Information geometric analysis of long range topological superconductors Amin, ST; Mera, B; (...); Vieira, VR Dec 4 2019 JOURNAL OF PHYSICS-CONDENSED MATTER ▾ 31 (48)	2	0	2	1	0	0.71	5
34	Entanglement-induced deviation from the geodesic motion in quantum gravity Pipa, F; Paunkovic, N and Vojinovic, M Sep 2019 JOURNAL OF COSMOLOGY AND ASTROPARTICLE PHYSICS ▾ (9)	0	2	1	2	0	0.71	5
35	Discrete time quantum walk on a line with two particles Sheridan, L; Paunkovic, N; (...); Bose, S International Workshop on Quantum Entanglement in Physical and Information Sciences Jun 2006 INTERNATIONAL JOURNAL OF QUANTUM INFORMATION ▾ 4 (3) , pp.573-583	0	0	1	0	0	0.25	5
36	Reply to "Comment on 'Bit-string oblivious transfer based on quantum state computational distinguishability' " Souto, A; Mateus, P; (...); Paunkovic, N Oct 30 2015 PHYSICAL REVIEW A ▾ 92 (4)	0	0	1	0	0	0.36	4
37	Gauge protected entanglement between gravity and matter Paunkovic, N and Vojinovic, M Sep 20 2018 CLASSICAL AND QUANTUM GRAVITY ▾ 35 (18)	0	1	0	1	0	0.38	3
38	Enhancing Privacy with Quantum Networks Mateus, P; Paunkovic, N; (...); Souto, A 15th Joint IFIP TC-6 and TC-11 International Conference on Communications and Multimedia Security (CMS) 2014 COMMUNICATIONS AND MULTIMEDIA SECURITY, CMS 2014 ▾ 8735 , pp.147-153	0	0	0	0	0	0.25	3
39	Operational interpretation of the vacuum and process matrices for identical particles Faleiro, B; Paunkovic, N and Vojinovic, M Apr 20 2023 QUANTUM ▾ 7	0	0	1	0	1	0.67	2
40	Information-Theoretical Criteria for Characterizing the Earliness of Time-Series Data	0	1	0	1	0	0.33	2



[← Back to author profile](#)

Citation overview

Paunković, Nikola

48

Documents

1,494

Citations

14

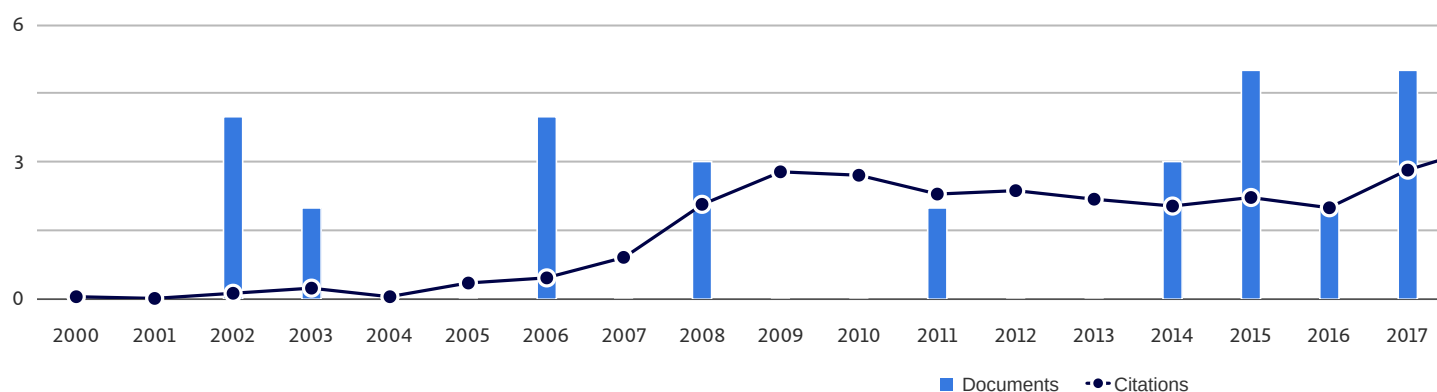
h-index

Date range: 2000 ▼ to 2025 ▼

Exclude citations ▾

☐ Hide documents with 0 citations Export

Documents



Sort by Cited by (highest) ▾

[illegible]

[illegible]

Documents		Year	<2000	2000	2001	2002	2003	2004	2005	2006	2007	2008	Total
Total			0	0	0	0	0	0	0	0	0	0	0
45	Entanglement Concentration Using Quant...	2002	0	0	0	0	0	0	0	0	0	0	2
46	On statistical and deterministic quantum t...	1998	0	1	0	0	0	0	0	0	0	0	2
47	Quantum Kolmogorov complexity and qua...	2024	0	0	0	0	0	0	0	0	0	0	1
48	Gravity-matter entanglement in Regge qu...	2016	0	0	0	0	0	0	0	0	0	0	1

Display [100 results](#) 

[Back to top](#)

About Scopus

[What is Scopus](#)

[Content coverage](#)

[Scopus blog](#)

[Scopus API](#)

[Privacy matters](#)

Language

[日本語版を表示する](#)

[查看简体中文版本](#)

[查看繁體中文版本](#)

[Просмотр версии на русском языке](#)

Customer Service

[Help](#)

[Tutorials](#)

[Contact us](#)

ELSEVIER

[Terms and conditions](#)  [Privacy policy](#)  [Cookies settings](#)

All content on this site: Copyright © 2025 [Elsevier B.V.](#) , its licensors, and contributors. All rights are reserved, including those for text and data mining, AI training, and similar technologies. For all open access content, the relevant licensing terms apply.

We use cookies to help provide and enhance our service and tailor content. By continuing, you agree to the [use of cookies](#) .



[← Back to author profile](#)

Citation overview

Paunković, Nikola

46

Documents

1,277

Citations

13

h-index

Date range:

2000

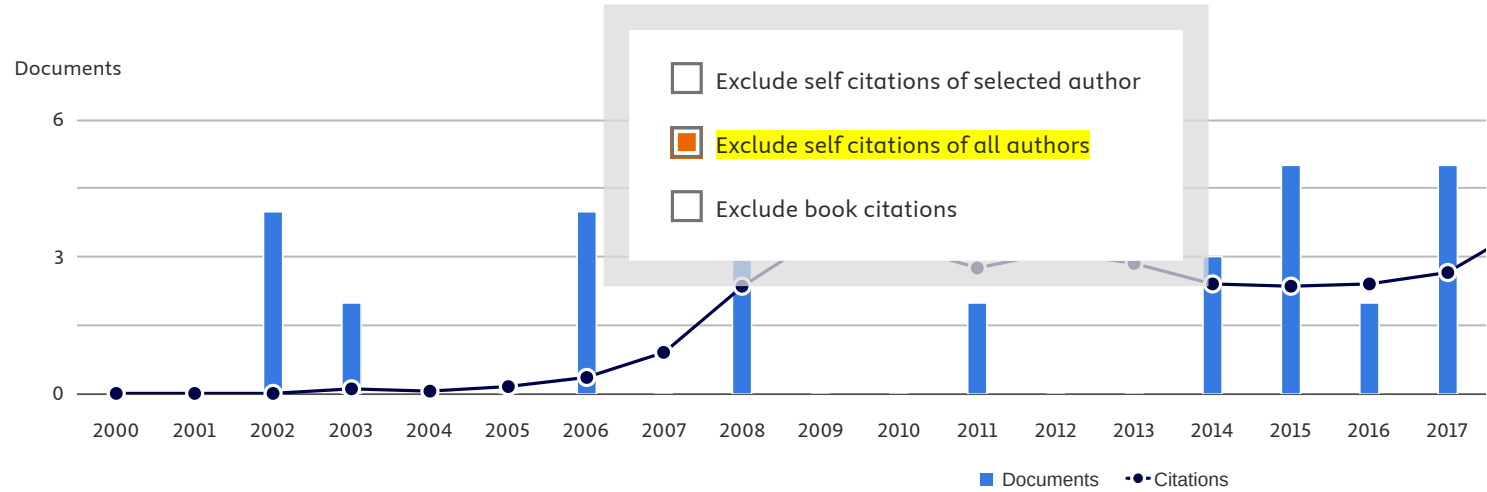
 to

2025

Exclude citations

☐ Hide documents with 0 citations

  Export



Sort by

Cited by (highest)

Documents		Year	<2000	2000	2001	2002	2003	2004	2005	2006	2007	2008	Total
Total			0	0	0	0	2	1	3	7	18		1,277
1	Ground state overlap and quantum phase ...	2006	0	0	0	0	0	0	0	2	14		666
2	Quantum walk on a line with two entangle...	2006	0	0	0	0	0	0	0	0	1		114
3	Dynamical phase transitions at finite temp...	2018	0	0	0	0	0	0	0	0	0		58
4	Fidelity between partial states as a signatu...	2008	0	0	0	0	0	0	0	0	0		57
5	Quantum walk public-key cryptographic s...	2015	0	0	0	0	0	0	0	0	0		35
6	Causal orders, quantum circuits and space...	2020	0	0	0	0	0	0	0	0	0		34
7	Quantum key distribution with quantum w...	2018	0	0	0	0	0	0	0	0	0		32
8	Uhlmann Connection in Fermionic Systems...	2017	0	0	0	0	0	0	0	0	0		28
9	Macroscopic distinguishability between qu...	2008	0	0	0	0	0	0	0	0	0		28
10	Entanglement concentration using quantu...	2002	0	0	0	0	0	0	1	1	0		23
11	Spin-space entanglement transfer and qua...	2002	0	0	0	0	2	1	1	3	3		21
12	Optimal state discrimination using particl...	2003	0	0	0	0	0	0	1	1	0		16

[illegible]

Documents		Year	<2000	2000	2001	2002	2003	2004	2005	2006	2007	2008	Total
Total			0	0	0	0							
44	Gauge protected entanglement between g...	2018	0	0	0	0	0	0	0	0	0		1
45	A brief review on quantum bit commitment	2014	0	0	0	0	0	0	0	0	0		1
46	Enhancing privacy with quantum networks	2014	0	0	0	0	0	0	0	0	0		1

Display [100 results](#) 

[Back to top](#)

About Scopus

[What is Scopus](#)

[Content coverage](#)

[Scopus blog](#)

[Scopus API](#)

[Privacy matters](#)

Language

[日本語版を表示する](#)

[查看简体中文版本](#)

[查看繁體中文版本](#)

[Просмотр версии на русском языке](#)

Customer Service

[Help](#)

[Tutorials](#)

[Contact us](#)

ELSEVIER

[Terms and conditions](#)  [Privacy policy](#)  [Cookies settings](#)

All content on this site: Copyright © 2025 [Elsevier B.V.](#) , its licensors, and contributors. All rights are reserved, including those for text and data mining, AI training, and similar technologies. For all open access content, the relevant licensing terms apply.

We use cookies to help provide and enhance our service and tailor content. By continuing, you agree to the [use of cookies](#) .





Република Србија
Агенција за квалификације

Број: 612-01-03-56/2019
Датум: 06.08.2019. године
Мајке Јевросиме 51
Београд
јк

На основу члана 38, члана 20. став 1. тачка 7 и члана 5. став 1. тачка 10. Закона о националном оквиру квалификација Републике Србије („Сл. гласник РС”, бр. 27/18), члана 131. став 1. Закона о високом образовању („Сл. гласник РС”, бр. 88/17, 27/18 – др. закон и 73/18), и члана 136. став 1. Закона о општем управном поступку („Службени гласник РС”, бр. 18/16 и 95/18 – аутентично тумачење), решавајући по захтеву **Николе Паунковића** из Београда, Република Србија, за признавање високошколске исправе издате у Уједињеном Краљевству Велике Британије и Северне Ирске, ради запошљавања, директор Агенције за квалификације доноси

РЕШЕЊЕ

1. Диплома издата 07.02. 2005. године од стране Универзитета у Оксфорду, колеџ Кебле (University of Oxford), Оксфорд, Уједињено Краљевство Велике Британије и Северне Ирске, на име **Никола Паунковић**, рођен 26.11.1973. године у Загребу, Република Хрватска, о завршеним докторским академским студијама високог образовања у четворогодишњем трајању, студијски програм: Физика, дисертација: “Улога неразличивости идентичних честица у обради квантне информације”, звање/квалификација: Doctor of Philosophy / Доктор наука, Доктор наука – физичке науке (на основу превода овлашћеног судског тумача за енглески језик), **признаје се** као диплома докторских академских студија трећег степена високог образовања (180 ЕСПБ), у оквиру образовно-научног поља: Природно-математичке науке, научна односно стручна област: Физичке науке, која одговара нивоу 8. НОКС-а, ради запошљавања.
2. Ово решење омогућава имаоцу општи приступ тржишту рада у Републици Србији, али га не ослобађа од испуњавања посебних услова за бављење професијама које су регулисане законом или другим прописом.
3. Превод звања/квалификације из тачке 1. диспозитива овог решења које је са оригиналне стране јавне исправе превео овлашћени судски тумач за енглески језик, не представља стручни, академски, научни односно уметнички назив који у складу са чланом 12. ставом 1. тачка 9. Закона о високом образовању, утврђује Национални савет за високо образовање.

Образложење

Агенцији за квалификације обратио се **Никола Паунковић** из Београда, Република Србија, захтевом од 27.05.2019. године за признавање дипломе Универзитета у Оксфорду, колеџ Кебле (University of Oxford), Оксфорд, Уједињено Краљевство Велике Британије и Северне Ирске, докторске академске студије високог образовања у четворогодишњем трајању, студијски програм: Физика, дисертација: “Улога неразличивости идентичних честица у обради квантне информације”, звање/квалификација: Doctor of Philosophy / Доктор наука, Доктор наука – физичке науке, ради запошљавања.

Уз захтев, подносилац захтева доставио је:

- 1) оверену копију дипломе издате 07.02. 2005. године од стране Универзитета у Оксфорду, колеџ Кебле (University of Oxford), Оксфорд, Уједињено Краљевство Велике Британије и Северне Ирске, студијски програм: Физика, звање/квалификација: Doctor of Philosophy;
- 2) оверени превод дипломе на српски језик;
- 3) примерак дисертације на изворном језику;
- 4) апстракт рада на енглеском језику;
- 5) листу објављених радова;
- 6) радну биографију;
- 7) оверене копије претходно стечене квалификације са документацијом;
- 8) пријавни формулар;
- 9) доказ о уплати таксе за професионално признавање.

Одредбом члана 136. став 1. Закона о општем управном поступку прописано је да се решењем одлучује о праву, обавези или правном интересу странке.

Одредбом члана 38. став 1. Закона о националном оквиру квалификација Републике Србије прописано је да захтев за професионално признавање заинтересовано лице подноси Агенцији. Ставом 2. наведеног члана прописано је да професионално признавање врши ENIC/NARIC центар, као организациони део Агенције, по претходно извршеном вредновању страног студијског програма, у складу са овим и законом који уређује високо образовање. Ставом 3. наведеног члана прописано је да решење о професионалном признавању посебно садржи: назив, врсту, степен и трајање (обим) студијског програма, односно квалификације, који је наведен у страног високошколској исправи – на изворном језику и у преводу на српски језик и научну, уметничку, односно стручну област у оквиру које је остварен студијски програм, односно врсту и ниво квалификације у Републици и ниво НОКС-а којем квалификација одговара. Ставом 4. наведеног члана прописано је да директор агенције доноси решење о професионалном признавању у року од 90 дана од дана пријема уредног захтева. Ставом 5. наведеног члана прописано је да решење из става 4. овог члана не ослобађа имаоца од испуњавања посебних услова за обављање одређене професије прописане посебним законом. Ставом 6. наведеног члана прописано је да је решење о професионалном признавању коначно. Ставом 7. наведеног члана прописано је да уколико није другачије прописано, на поступак професионалног признавања примењује се закон којим се уређује општи управни поступак. Ставом 8. наведеног члана прописано је да решење о професионалном признавању има значај јавне исправе. Ставом 9. наведеног члана прописано је да ближе услове у погледу поступка професионалног признавања прописује министар надлежан за послове образовања.

Одредбом члана 20. став 1. тачка 7. Закона о националном оквиру квалификација Републике Србије, директор Агенције за потребе давања стручног мишљења у поступку вредновања страног студијског програма именује комисију од најмање три рецензента са листе рецензента коју утврђује Национални савет за високо образовање, у складу са законом који уређује високо образовање и овим законом.

Одредбом члана 131. став 1. Закона о високом образовању, прописано је да се вредновање страног студијског програма врши на основу врсте и нивоа постигнутих компетенција стечених завршетком студијског програма, узимајући у обзир систем образовања у земљи у којој је високошколска исправа стечена, услове уписа, права која проистичу из стране високошколске исправе у земљи у којој је стечена и друге релевантне чињенице, без разматрања формалних обележја и структуре студијског програма.

Одредбом члана 5. став 1. тачка 10. Закона о националном оквиру квалификација Републике Србије, прописано је да се осми ниво стиче завршавањем докторских студија обима 180 ЕСПБ бодова (уз претходно завршене интегрисане академске, односно мастер академске студије).

Одлучујући о захтеву подносиоца, а након прибављеног мишљења комисије која је извршила вредновање страног студијског програма на основу врсте и нивоа постигнутих компетенција стечених завршетком студијског програма, узимајући у обзир систем образовања у земљи у којој је високошколска исправа стечена, услове уписа, права која проистичу из стране високошколске исправе у земљи у којој је стечена и друге релевантне чињенице, без разматрања формалних обележја и структуре студијског програма, одлучено је да се диплома Универзитета у Оксфорду, колеџ Кебле (University of Oxford), Оксфорд, Уједињено

Краљевство Велике Британије и Северне Ирске, може признати као диплома докторских студија трећег степена високог образовања (180 ЕСПБ), која одговара нивоу 8. НОКС-а.

Са напред наведених разлога директор Агенције је нашао да су у конкретном случају испуњени претходно наведени сви законом прописани услови да се призна диплома Универзитета у Оксфорду, колеџ Кебле (University of Oxford), Оксфорд, Уједињено Краљевство Велике Британије и Северне Ирске, као диплома докторских академских студија трећег степена високог образовања (180 ЕСПБ), у оквиру образовно-научног поља: Природно-математичке науке, научна односно стручна област: Физичке науке, која одговара нивоу 8 НОКС-а, ради запошљавања.

Такса за решење по захтеву, по тарифном броју 172. тачка 3, подтачка 4а) Закона о републичким административним таксама ("Службени гласник РС", бр. 43/03, 51/03-испр., 61/05, 101/05-др.закон, 5/09, 54/09, 50/11, 70/11- усклађени дин.изн., 55/12- усклађени дин.изн., 93/12, 47/13 - усклађени дин.изн, 65/13-др.закон, 57/14- усклађени дин.изн, 45/15- усклађени дин.изн, 83/15, 112/15, 50/16- усклађени дин.изн., 61/17- усклађени дин.изн., 113/17, 3/18, 50/18 и 95/18), плаћена је и поништена.

Сходно претходно наведеном, донета је одлука као у диспозитиву решења.

Упутство о правном средству: Ово решење је коначно у управном поступку и против истог може се покренути управни спор. Тужба се подноси Управном суду у року од 30 дана од дана пријема овог решења.

Решење доставити:

- Никола Паунковић, ул. Авијатичарски пут бр. 1, 11080 Београд;

- Архиви.





This is to certify that

Nikola Paunkovic

Keble College

having submitted a thesis entitled

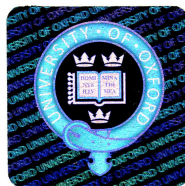
The Role of Indistinguishability of Identical Particles in Quantum Information Processing

and, having satisfied all the conditions prescribed by the Statutes of the University on 7 February 2005, was on 9 November 2013 admitted to the Degree of

DOCTOR OF PHILOSOPHY

University Offices,
Oxford.
9 November 2013

194926



Eva G. McKendrick

Registrar



[HHU](#) > [Math.-Nat. Fakultät](#) > [Physik](#) > [Arbeitsgruppe Prof. Bruß](#) > [Veranstaltungen](#) > **06 December 2023 -Lisbon-Düsseldorf Quantum Cryptography workshop**

Lisbon-Düsseldorf Quantum Cryptography workshop

Date: Wednesday, December 06, 2023

Time: 10:00 – 13:00

Place: seminar room 25.32.03.51

This short workshop aims to present an overview of the research conducted in Düsseldorf and Lisbon in the area of quantum cryptography.

Please contact [✉ glaucia.murta\(at\)hhu.de](mailto:glaucia.murta(at)hhu.de) if you would like to attend the workshop or if you are interested in a streaming option.

Schedule:

10:00 – 10:25 Federico Grasselli (Düsseldorf/Paris)

10:25 – 10:50 Mariano Lemus (Lisbon)

10:50 – 11:15 Giacomo Carrara (Düsseldorf)

11:15 – 11:45 Coffee break

11:45 – 12:10 Chrysoula Vlachou (Lisbon)

12:10 – 12:35 Anton Trushechkin (Düsseldorf)

12:35 – 13:00 **Nikola Paunkovic** (Lisbon)

Abstracts

Federico Grasselli

Title: Security proof for BB84-style QKD protocols without assumption of equal detection probabilities

A crucial security parameter in BB84-style QKD protocols is the so-called phase error rate. Most security proofs and relative implementations can easily estimate the phase error rate by assuming that the detection probability in the two measuring bases of Bob is equal, for any input state. In this case, the phase error rate reduces to the bit error rate that Alice and Bob observe in the test basis (i.e., the complementary basis to the key generation basis). However, there are certain QKD setups where the assumption on the equal detection probability is not justified experimentally. Our work aims at deriving a fully-analytical security proof for BB84-style QKD protocols, where the main challenge is estimating the phase error rate without relying on the assumption of equal detection probabilities.

Mariano Lemus

Title: Computationally Secure Oblivious Transfer in the Quantum Setting: Results from the QuantumPrime project.

Motivated by the usefulness of secure multiparty computation as a privacy-protecting data analysis tool, and identifying its

oblivious transfer as one of its main practical enablers, we propose a practical realization of quantum oblivious transfer, which uses cryptographic hash functions to implement commitments. The security of the resulting oblivious transfer is analyzed and compared to both quantum and classical alternatives. Furthermore, the protocol is implemented experimentally to measure its current real-world performance. The proposed version is shown to offer security advantages over existing classical solutions based on public key cryptography primitives in exchange for lower key generation rates. We will also explore potential of additional advantages that the protocol can provide that are subject to further exploring.

Giacomo Carrara

Title: Multipartite randomness extraction with almost unentangled states

Bell inequalities represent a fundamental tool for many quantum information tasks. In particular, past research has shown that the certification of the violation of a Bell inequalities allows the parties to extract perfectly random outcomes, which cannot be guessed by potential eavesdroppers. Moreover, the power of Bell inequalities has been shown in [Phys. Rev. Lett., 108, 100402 (2012)], where the authors show that the parties can extract perfect randomness even if the violation of the Bell inequality is achieved by a state which can be arbitrarily close to a separable state. In this work, we try to extend this result to the multipartite scenario. In particular, we analyze the amount of randomness that can be extracted from an multipartite Bell inequality, which is maximally violated by a state arbitrarily close to a fully separable multipartite state. In order to achieve this result, we aim to employ both standard numerical convex optimization and newly developed analytical methods, to obtain a better bound on the randomness extraction rate.

Chrysoula Vlachou

Title: Quantum Universally Composable Oblivious Linear Evaluation

Oblivious linear evaluation is a cryptographic primitive whereby two distrustful parties obliviously compute a linear function, $f(x) = ax + b$, i.e., each one provides their inputs that remain unknown to the other, in order to compute the output $f(x)$ that only one of them receives. From both a structural and a security point of view, oblivious linear evaluation is fundamental for arithmetic-based secure multi-party computation protocols. In the classical case, oblivious linear evaluation protocols can be generated using oblivious transfer, and their quantum counterparts can, in principle, be constructed as straightforward extensions using quantum oblivious transfer. Here, we present the first, to the best of our knowledge, quantum protocol for oblivious linear evaluation that, furthermore, does not rely on quantum oblivious transfer. Our protocol uses high-dimensional quantum states to obliviously compute $f(x)$ on Galois Fields of prime and prime-power dimension. Our construction utilizes the existence of a complete set of mutually unbiased bases in prime-power dimension Hilbert spaces and their linear behaviour upon the Heisenberg-Weyl operators. We prove the protocols to have static security in the framework of quantum universal composability.

Anton Trushechkin

Title: Problem of symmetric postprocessing in quantum conference key agreement

In the present-day quantum conference key agreement one party ('Alice') has a distinguished role: her bit string after finishing the quantum part and sifting is considered to be corrected, while discrepancies with the bit strings of are treated as errors on their sides. Alice announces information (e.g., error correction syndrome) for other parties in order to allow them to recover her string. Recently, F. Salek and A. Winter proposed to use the symmetric postprocessing, where each participant announces information that is enough for all other parties to recover his bit string. Then they merge their strings as a preliminary key and perform privacy amplification to it to obtain a final key. However, the question of which scheme (with the distinguished Alice or symmetric) is more efficient is open. This question will be discussed in the talk.

Nikola Paunkovic

Title: Quantum information at SQIG-IT — cryptography, prime number generation and causality

I will present part of the research in our group (SQIG-IT – Security and Quantum Information Group at Instituto de Telecomunicações) related to quantum information, in particular the results in cryptography developed within the QuantumPrime project. I will also present a measurement that distinguishes between definite and superposed causal orders and how to achieve quantum-mechanical closed timelike curves in the presence of the latter. Finally, I will briefly mention other interdisciplinary works on the gauge-protected gravity-matter entanglement, violation of the weak equivalence principle in the presence of superposed gravitational fields, operational emergence and verification of spacetime manifold, as well as applications of quantum information geometry to the study of phase transitions.

Heinrich-Heine-Universität Düsseldorf ✉ D-40204 Düsseldorf, Germany

Theoretische Physik III
Dr. Gláucia Murta
Telefon +49-211-81-11379
Telefax: +49 211 81-11613992
Gláucia.Murta@uni-duesseldorf.de

Sekretariat +49-211-81-13992
Cordula Hoffjan
sekretariat.tp3@uni-duesseldorf.de

Düsseldorf, 20th December, 2023

CERTIFICATE

Hereby we confirm the participation of

Nikola Paunkovic

from

SQIG – Instituto de Telecomunicações

in the Lisbon-Düsseldorf Quantum Cryptography workshop, which was held
at the Heinrich-Heine-Universität Düsseldorf, Germany, on December 06
2023, having presented the talk

**Quantum information at SQIG-IT — cryptography,
prime number generation and causality**

Further details of the event can be found on the url:

www.tp3.hhu.de/06-december-2023-lisbon-duesseldorf-quantum-cryptography-workshop

Yours sincerely,

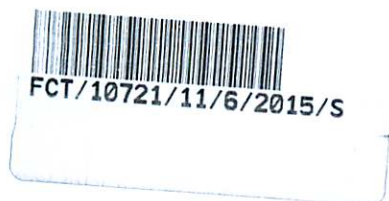

Dr. Gláucia Murta

Heinrich-Heine-Universität
Düsseldorf
Universitätsstraße 1
D-40225 Düsseldorf, Germany
Gebäude 25.32
Ebene 03 Raum 50
www.tp3.hhu.de



FCT Fundação para a Ciência e a Tecnologia

MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA



Exmo(a) Senhor(a)

Doutor(a)

Nikola Paunković

Instituto de Telecomunicações

SQIG – Security and Quantum Information Group

Torr Norte,

IST,

Av. Rovisco Pais 1,

1049-001 Lisboa

Proc.º 441.00 SERVIA

Assunto: Cooperação Científica e Tecnológica FCT/SERVIA - 2015/2016

Na sequência da reunião da Comissão Mista entre a Fundação para a Ciência e a Tecnologia (FCT) de Portugal e , tendo em vista a seleção de candidaturas ao concurso para o biénio 2015/2016, no âmbito do Acordo de Cooperação Científica e Tecnológica, informa-se V. Exa que o projeto intitulado "RUÍDO E ERROS DE MEDIÇÃO EM PROTOCOLOS DE SEGURANÇA QUÂNTICOS MULTIAGENTE" vai ser apoiado financeiramente, tendo-lhe sido atribuído, para o ano em curso, o montante de 2000€, destinado a custear as viagens dos investigadores portugueses a e as estadias dos investigadores a Portugal.

No final do corrente ano, deverá ser enviado ao Departamento das Relações Internacionais (DRI) da FCT um relatório científico/financeiro acompanhado pelos comprovativos das despesas enunciadas. O modelo do relatório está disponível no endereço: "http://www.fct.pt/apoios/cooptrans/#acordos_bilaterais".

O financiamento para o 2º ano do projeto só será confirmado após a avaliação do referido relatório.

Com os melhores cumprimentos

A Diretora do DRI,

Paula Elyseu Mesquita

Cooperação Transnacional

Concurso dos Acordos Bilaterais

Formulário

Nome do Acordo: Ano(s) de Execução 2014/2015**Responsável Português:****Nome:** Nikola Paunković**Responsável Estrangeiro****Nome:** Nikola Burić**Título:** PhD, Research fellow**Título:** PhD, Professor**E-Mail:** npaunkovic@gmail.com**E-Mail:** buric@ipb.ac.rs**Nome e endereço da instituição:**

Instituto de Telecomunicações
SQIG – Security and Quantum Information Group
Torre Norte, IST, Av. Rovisco Pais 1, 1049-001 Lisboa

Nome e endereço da instituição:

Institute of Physics, University of Belgrade
Scientific Computing Laboratory
Pregrevica 117, 11000 Beograd-Zemun, Serbia

PROJETO**Título em Português**

RÚÍDO E ERROS DE MEDIÇÃO EM PROTOCOLOS DE SEGURANÇA QUÂNTICOS MULTIAGENTE

Título em Inglês/Francês

NOISE AND MEASUREMENT ERRORS IN MULTI-PARTY QUANTUM SECURITY PROTOCOLS

FCT Фондација за науку и технологију
МИНИСТАРСТВО ПРОСВЕТЕ И НАУКЕ

Поштовани господине

Доктор

Никола Паунковић

Институт за телекомуникације

SQIG – Група за безбедност и квантне информације

Torr Norte,

IST,

Av. Rovisco Pais 1,

1049-001 Lisboa

Proc. 441,00 SERVIA

Предмет: Научна и технолошка сарадња FCT/SERVIA – 2015/2016

Након састанка Заједничког одбора између Португалске фондације за науку и технологију (FCT) и , у циљу избора пријава за двогодишњи позив 2015/2016, у оквиру Споразума о научној и технолошкој сарадњи, обавештавамо Вас да ће пројекат под називом „ШУМ И ГРЕШКЕ МЕРЕЊА У ВИШЕКОМПОНЕНТНИМ КВАНТНИМ БЕЗБЕДНОСНИМ ПРОТОКОЛИМА“ добити финансијску подршку, са 2.000 евра издвојених за текућу годину за покривање путних трошкова португалских истраживача и трошкова боравка истраживача у Португалу.

До краја ове године, Одељењу за међународне односе (DRI) FCT-а мора се доставити научни/финансијски извештај, заједно са доказом о наведеним трошковима. Шаблон извештаја је доступан на: http://www.fct.pt/apoios/cooptrans/#acordos_bilaterais.

Финансирање за другу годину пројекта биће потврђено тек након што се оцени горе поменути извештај.

Срдачан поздрав,

Директорка DRI-ја,

Паула Елисеу Мескита

CA23115 - Relativistic Quantum Information (RQI)

 Downloads

[Home](#) > [Browse Actions](#) > Relativistic Quantum Information (RQI)

Description

Management Committee

Main Contacts and Leadership

Working Groups and Membership

Action Details

 MoU - 028/24

 CSO Approval date - 17/05/2024

 Start date - 20/09/2024

 End date - 19/09/2028

How can I participate?

- Read the Action Description [MoU](#)
- Inform the Main Proposer/Chair of your interest ([email](#))
- [Apply](#) to join your Working Groups of interest
- Please note, Management Committee nominations are carried out through the [COST National Coordinators](#)

Management Committee

Country	MC Member
Albania	Dr Dolantina HYKA 
Albania	Prof Arban UKA 



Armenia	Dr Armen ALLAHVERDYAN	▼
Austria	Prof Caslav BRUKNER	▼
Austria	Dr Beatrix HIESMAYR	▼
Belgium	Dr Yves CAUDANO	▼
Belgium	Dr Ognyan ORESHKOV	▼
Cyprus	Prof Constantia ALEXANDROU	▼
Czech Republic	Prof Petr VASIK	▼
Finland	Dr Kimmo LUOMA	▼
France	Prof Thomas DURT	▼
France	Dr Alexandre MATZKIN	▼
Germany	Dr Albert ROURA	▼
Germany	Dr Dennis RÄTZEL	▼
Greece	Dr Andreas ZOUPAS	▼
Hungary	Prof Lajos DIÓSI	▼
Hungary	Dr Tamás KISS	▼
Ireland	Prof Felix BINDER	▼
Israel	Prof Eliahu COHEN	▼
Israel	Dr Boris KANTSEPOLSKY	▼
Italy	Prof Gaetano FIORE	▼
Italy	Prof Stefano MANCINI	▼
Luxembourg	Prof Adolfo DEL CAMPO	▼
Malta	Prof André XUEREB	▼
Netherlands	Dr Antonio FERREIRO	▼
Netherlands	Prof Renate LOLL	▼
Norway	Prof Leon LOVERIDGE	

Poland	Dr Jaroslaw MISZCZAK [^]
Poland	Dr Adamantia ZAMPELI
Portugal	Prof Paulo MONIZ
Portugal	Dr Nikola PAUNKOVIĆ Instituto de Telecomunicações Av. Rovisco Pais, Instituto Superior Técnico, Torre Norte Portugal 1049-001 Lisbon +351218417140 npaunkovic@gmail.com Participating actions CA23115 CA23130
Romania	Dr Maria Anastasia JIVULESCU
Romania	Prof Nicolina POP
Serbia	Dr Aleksandra GOČANIN
Serbia	Dr Marko VOJINOVIC
Slovakia	Dr Natália SALOMÉ MÓLLER
Slovakia	Dr Mario ZIMAN
Slovenia	Dr Samed BAJRIC
Slovenia	Prof Rainer KALTENBAEK
Spain	Prof Dmitri SOKOLOVSKI
Spain	Dr Adrian DEL RIO VEGA
Sweden	Dr Guilherme FRANZMANN
Sweden	Dr Magdalena ZYCH



Switzerland	Dr Viktoria KABEL	▼
Switzerland	Prof André STEFANOV	
Türkiye	Prof Ozgur YILDIRIM	
Türkiye	Prof Kadri ÖZDEMİR	
United Kingdom	Prof Kasia REJZNER	
United Kingdom	Prof Mairi SAKELLARIADOU	



Action documents

Memorandum of Understanding



COST Association
Avenue du Boulevard – Bolwerklaan 21
1210 Brussels | Belgium

BE0829.090.573
RPM/RPR Bruxelles/Brussel

+32 2 533 38 00

© 2025 COST Association | Legal

News

Events

Videos

Publications

Vacancies

Contact Us

Stay connected

CA23130 - Bridging high and low energies in search of quantum gravity (BridgeQG)

 Downloads

[Home](#) > [Browse Actions](#) >

Bridging high and low energies in search of quantum gravity (BridgeQG)

Description

Management Committee

Main Contacts and Leadership

Working Groups and Membership

Action Details

 MoU - 043/24

 CSO Approval date - 17/05/2024

 Start date - 18/09/2024

 End date - 17/09/2028

How can I participate?

- Read the Action Description [MoU](#)
- Inform the Main Proposer/Chair of your interest ([email](#))
- [Apply](#) to join your Working Groups of interest
- Please note, Management Committee nominations are carried out through the [COST National Coordinators](#)

Management Committee

Country

MC Member



Austria	Dr Lin-Qing CHEN	✓
Austria	Dr Thomas GALLEY	✓
Bosnia and Herzegovina	Prof Suad KUNOSIC	✓
Bosnia and Herzegovina	Prof Vedad PASIC	✓
Bulgaria	Prof Vladimir DOBREV	✓
Bulgaria	Dr Denitsa STAICOVA	✓
Croatia	Dr Tomislav TERZIĆ	✓
Czech Republic	Dr Petr KOTLAŘÍK	✓
Czech Republic	Mr Federico URBAN	✓
Denmark	Prof Troels HARMARK	✓
Denmark	Prof Niels OBERS	✓
Estonia	Dr Manuel HOHMANN	✓
Finland	Dr Sergey TSYGANKOV	✓
France	Dr Julien BOLMONT	✓
Germany	Dr Alba DOMI	✓
Germany	Dr Christian PFEIFER	✓
Greece	Prof Nikolaos MAVROMATOS	✓
Greece	Prof Emmanuel SARIDAKIS	✓
Hungary	Prof Árpád László GERGELY	✓
Ireland	Dr Maria CHERNYAKOVA	✓
Ireland	Mr Kay LEHNERT	✓
Israel	Prof Eduardo GUENDELMAN	✓
Israel	Prof Yosef VERBIN	✓
Italy	Prof Giovanni AMELINO CAMELIA	✓
Italy	Dr Giacomo ROSATI	✓
Malta	Dr Cecilia LEVIGANDI	✓

Malta	PROT JACKSON LEVI SAID
Netherlands	Dr Sjors HEEFER
Netherlands	Prof Gary STEELE
Norway	Dr Anna PACHOL
Poland	Prof Jerzy KOWALSKI-GLIKMAN
Poland	Dr Tomasz TRZESNIEWSKI
Portugal	Prof Filipe JOAQUIM
Portugal	Dr Nikola PAUNKOVIĆ Instituto de Telecomunicações Av. Rovisco Pais, Instituto Superior Técnico, Torre Norte Portugal 1049-001 Lisbon +351218417140 npaunkovic@gmail.com Participating actions CA23115CA23130
Romania	Dr Eugeniu Mihnea POPESCU
Romania	Dr Nicoleta VOICU
Serbia	Prof Goran DJORDJEVIC
Serbia	Prof Nikola KONJIK
Slovakia	Dr Martin KRSSAK
Spain	Prof Ángel BALLESTEROS
Spain	Prof Jose Manuel CARMONA
Sweden	Prof Carlos PEREZ DE LOS HEROS
Sweden	Dr Magdalena ZYCH



Switzerland	Dr Flaminia GIACOMINI
Switzerland	Prof Philippe JETZER
Türkiye	Prof Sengul KURU
Türkiye	Prof Deniz SUNAR CERCI
United Kingdom	Prof Adrian KENT
United Kingdom	Prof Mairi SAKELLARIADOU



Action documents

Memorandum of Understanding



COST Association
Avenue du Boulevard – Bolwerklaan 21
1210 Brussels | Belgium

BE0829.090.573
RPM/RPR Bruxelles/Brussel

+32 2 533 38 00

© 2025 COST Association | Legal

News

Events

Videos

Publications

Vacancies

Contact Us

Stay connected



entropy

an Open Access Journal by MDPI

IMPACT
FACTOR
2.419

Information Geometry of Classical and Quantum States and Applications

Guest Editor

Dr. Nikola Paunković

Deadline

31 December 2020

mdpi.com/si/35228

Special Issue

Invitation to submit

Search for Articles:

Title / Keyword

Author / Affiliation / Email

Entropy ▼

All Article Types ▼

Search

Advanced

Journals / Entropy / Special Issues / Information Geometry of Classical and Quantum States and Applications

IMPACT
FACTOR
2.0Indexed in:
PubMedCITESCORE
5.2

entropy

Submit to *Entropy*Review for *Entropy*

Propose a Special Issue

Journal Menu

- [Entropy Home](#)
- [Aims & Scope](#)
- [Editorial Board](#)
- [Reviewer Board](#)
- [Topical Advisory Panel](#)
- [Photography Exhibition](#)
- [Instructions for Authors](#)
- **[Special Issues](#)**
- [Topics](#)
- [Sections & Collections](#)
- [Article Processing Charge](#)
- [Indexing & Archiving](#)
- [Editor's Choice Articles](#)
- [Most Cited & Viewed](#)
- [Journal Statistics](#)

Information Geometry of Classical and Quantum States and Applications

- [Special Issue Editors](#)
- [Special Issue Information](#)
- [Keywords](#)
- [Benefits of Publishing in a Special Issue](#)
- [Published Papers](#)

A special issue of *Entropy* (ISSN 1099-4300). This special issue belongs to the section "[Quantum Information](#)".

Deadline for manuscript submissions: **closed (25 June 2021)** | Viewed by 411

Share This Special Issue



Special Issue Editor



Special Issue Editor



Dr. Nikola Paunković

Guest Editor

[E-Mail](#) [Website](#)

1. Instituto de Telecomunicações, 1049-001 Lisboa, Portugal

2. Departamento de Matemática, Instituto Superior Técnico, Universidade de Lisboa, Av. Rovisco Pais, 1049-001 Lisboa, Portugal

Interests: information geometry of Hilbert spaces and many-body physics; topological phases of matter and phase transitions; quantum cryptography; quantum mechanics and gravity; entanglement and indistinguishability; classical, quantum and total correlations

Special Issue Information

Dear Colleagues,

Information geometry has a long history of applications in both classical and quantum physics, as well as in statistics, computer science, and other disciplines. Since the pioneering work of Fisher and others from the beginning of the 20th century, distance-like quantities measuring distinguishability between probability distributions, or their information content, have been used to tackle problems in statistics and information science. Various geometric and topological phases (Pancharatnam, Longuet-Higgins, Berry, Aharonov-Bohm, etc.) were in the second half of the last century shown useful in optics, chemistry, and atomic and molecular, as well as in condensed matter physics.

Recently, information geometry of quantum states has drawn considerable attention in various fields. Fidelity susceptibility and the related quantities have shown to be useful figures of merit when probing phase transitions of novel exotic (say, topological) matter, which do not fall within the standard symmetry-breaking paradigm. In high-energy physics, various information metrics were used in AdS/CFT and other holographic approaches, in the “space from Hilbert space” paradigm, as well as in lattice gauge theories. In the context of machine learning, information-based volumes of classical and quantum states were used in estimating the complexity of describing probability distributions and density matrices. At the end of this short, but by no means exhaustive, list of applications, distance measures between the processes were introduced to study channel capacity and communication complexity.

This novel rapid progress shows that in spite of their longevity, information geometry applications are offering research opportunities and open many new questions to be answered. Due to technological advances, the increased computational power of today’s devices allows tackling previously intractable numerical studies and developing new methods. Moreover, novel quantum technologies offer experimental ways of performing quantum state estimation and metrology. Therefore, theoretical, as well as computational and experimental studies are all welcome in this Special Issue.

Dr. Nikola Paunković

Guest Editor

Manuscript Submission Information

Submit to *Entropy*

Review for *Entropy*

Propose a Special Issue

Journal Browser

volume

issue

Go

> Forthcoming issue

> Current issue

Vol. 27 (2025)	Vol. 13 (2011)
Vol. 26 (2024)	Vol. 12 (2010)
Vol. 25 (2023)	Vol. 11 (2009)
Vol. 24 (2022)	Vol. 10 (2008)
Vol. 23 (2021)	Vol. 9 (2007)
Vol. 22 (2020)	Vol. 8 (2006)
Vol. 21 (2019)	Vol. 7 (2005)
Vol. 20 (2018)	Vol. 6 (2004)
Vol. 19 (2017)	Vol. 5 (2003)
Vol. 18 (2016)	Vol. 4 (2002)
Vol. 17 (2015)	Vol. 3 (2001)
Vol. 16 (2014)	Vol. 2 (2000)
Vol. 15 (2013)	Vol. 1 (1999)
Vol. 14 (2012)	



Back to Top

Submit to *Entropy*

Review for *Entropy*

Propose a Special Issue

Manuscript Submission Information

Manuscripts should be submitted online at www.mdpi.com by **registering** and **logging in to this website**. Once you are registered, **click here to go to the submission form**. Manuscripts can be submitted until the deadline. All submissions that pass pre-check are peer-reviewed. Accepted papers will be published continuously in the journal (as soon as accepted) and will be listed together on the special issue website. Research articles, review articles as well as short communications are invited. For planned papers, a title and short abstract (about 100 words) can be sent to the Editorial Office for announcement on this website.

Submitted manuscripts should not have been published previously, nor be under consideration for publication elsewhere (except conference proceedings papers). All manuscripts are thoroughly refereed through a single-blind peer-review process. A guide for authors and other relevant information for submission of manuscripts is available on the **Instructions for Authors** page. *Entropy* is an international peer-reviewed open access monthly journal published by MDPI.

Please visit the **Instructions for Authors** page before submitting a manuscript. The **Article Processing Charge (APC)** for publication in this **open access** journal is 2600 CHF (Swiss Francs). Submitted papers should be well formatted and use good English. Authors may use MDPI's **English editing service** prior to publication or during author revisions.

Keywords

- Distinguishability, fidelity, geometric phases, and Fisher information
- Entanglement and correlations
- Equilibrium and dynamical phase transitions
- Topological phases of matter
- Entropy and area laws
- AdS/CFT correspondence
- Tensor networks
- Quantum estimation and metrology
- Machine learning





applied sciences

an Open Access Journal by MDPI

IMPACT
FACTOR
2.679

CITESCORE
3.7

Recent Development and Application of Quantum Communication and Security Protocols

Guest Editors

Dr. Nikola Paunković, Dr. André Souto

Deadline

31 July 2022

mdpi.com/si/62298

Special Issue

Invitation to submit

Search for Articles:

Title / Keyword

Author / Affiliation / Email

Applied Sciences ▼

All Article Types ▼

Search

Advanced

Journals / Applied Sciences / Special Issues / Recent Development and Application of Quantum Communication and Security Protocols

IMPACT
FACTOR
2.5CITESCORE
5.5*applied sciences*Submit to *Applied Sciences*Review for *Applied Sciences*

Propose a Special Issue

Journal Menu

- [Applied Sciences Home](#)
- [Aims & Scope](#)
- [Editorial Board](#)
- [Reviewer Board](#)
- [Topical Advisory Panel](#)
- [Instructions for Authors](#)
- **[Special Issues](#)**
- [Topics](#)
- [Sections & Collections](#)
- [Article Processing Charge](#)
- [Indexing & Archiving](#)
- [Editor's Choice Articles](#)
- [Most Cited & Viewed](#)
- [Journal Statistics](#)
- [Journal History](#)

Recent Development and Application of Quantum Communication and Security Protocols

- [Print Special Issue Flyer](#)
- [Special Issue Editors](#)
- [Special Issue Information](#)
- [Keywords](#)
- [Benefits of Publishing in a Special Issue](#)
- [Published Papers](#)

A special issue of *Applied Sciences* (ISSN 2076-3417). This special issue belongs to the section "Electrical, Electronics and Communications Engineering".

Deadline for manuscript submissions:
closed (31 July 2022) | Viewed by
11846



Share This Special Issue



Special Issue Editors



Dr. Nikola Paunković

[E-Mail](#) [Website](#)

Guest Editor

1. Instituto de Telecomunicações, Av. Rovisco Pais 1, 1049-001 Lisboa, Portugal

2. Departamento de Matemática, Instituto Superior Técnico, Universidade de Lisboa, Av. Rovisco Pais 1, 1049-001 Lisboa, Portugal

Interests: information geometry of Hilbert spaces and many-body physics; topological phases of matter and phase transitions; quantum cryptography; quantum mechanics and gravity; entanglement and indistinguishability; classical, quantum, and total correlations

Special Issues, Collections and Topics in MDPI journals



Dr. André Souto

[E-Mail](#) [Website](#)

Guest Editor

LASIGE, Departamento de Informática, Faculdade de Ciências da Universidade de Lisboa, Campo Grande, 016, 1749-016 Lisboa, Portugal

Interests: quantum computation; computational complexity; cryptography; kolmogorov complexity

Special Issues, Collections and Topics in MDPI journals

Special Issue Information

Dear Colleagues,

Since the famous BB84 quantum key distribution protocol that overcomes the classical counterparts of general key-agreement protocols was established, quantum communication schemes have become one of the central topics of research triggered by the second quantum revolution.

At present, quantum communication is one of the most prominent areas of emerging quantum technologies, with new applications, such as the quantum internet, which will become a reality in the near future. To leverage this new reality, the development of new applications of quantum communication is growing. In particular, issues of security and privacy arise as crucial requirements in a vast number of different applications. While the question of secure communication, addressed by various key distribution schemes, holds the most prominent position within quantum cryptography, many other tasks have recently been attracting the attention of the community. Quantum cryptography beyond key distribution, addressing privacy requirements, ranges from secure

Submit to *Applied Sciences*

Review for *Applied Sciences*

Propose a Special Issue

issue

Go

> Forthcoming issue

> Current issue

Vol. 15 (2025)

Vol. 7 (2017)

Vol. 14 (2024)

Vol. 6 (2016)

Vol. 13 (2023)

Vol. 5 (2015)

Vol. 12 (2022)

Vol. 4 (2014)

Vol. 11 (2021)

Vol. 3 (2013)

Vol. 10 (2020)

Vol. 2 (2012)

Vol. 9 (2019)

Vol. 1 (2011)

Vol. 8 (2018)

Submit to *Applied Sciences*

Review for *Applied Sciences*

Propose a Special Issue

attention of the community. Quantum cryptography beyond key distribution, addressing privacy requirements, ranges from secure multiparty computations (private data mining, e-voting, etc.), through authentication, blind computation, contract signing protocols, secret sharing, etc. The range of new applications that are more efficient regarding information transmission and with fewer costs of types of resources needed is so vast that any list has the risk of being incomplete.

Therefore, theoretical as well as computational and experimental studies and new developments and applications of quantum communications are all welcome in this Special Issue.

Dr. Nikola Paunković

Dr. André Souto

Guest Editors

Manuscript Submission Information

Manuscripts should be submitted online at www.mdpi.com by **registering** and **logging in to this website**. Once you are registered, **click here to go to the submission form**. Manuscripts can be submitted until the deadline. All submissions that pass pre-check are peer-reviewed. Accepted papers will be published continuously in the journal (as soon as accepted) and will be listed together on the special issue website. Research articles, review articles as well as short communications are invited. For planned papers, a title and short abstract (about 100 words) can be sent to the Editorial Office for announcement on this website.

Submitted manuscripts should not have been published previously, nor be under consideration for publication elsewhere (except conference proceedings papers). All manuscripts are thoroughly refereed through a single-blind peer-review process. A guide for authors and other relevant information for submission of manuscripts is available on the **Instructions for Authors** page. *Applied Sciences* is an international peer-reviewed open access semimonthly journal published by MDPI.

Please visit the **Instructions for Authors** page before submitting a manuscript. The **Article Processing Charge (APC)** for publication in this **open access** journal is 2400 CHF (Swiss Francs). Submitted papers should be well formatted and use good English. Authors may use MDPI's **English editing service** prior to publication or during author revisions.

Keywords

- quantum communication protocols
- applications for secure quantum communications
- key distribution/arrangement schemes
- secure multi-party computation
- authentication schemes
- blind computation
- contract signing
- semi-quantum communication applications



Special Issue

Quantum Information and Condensed Matter Physics

Message from the Guest Editors

Recent years have witnessed the emergence of novel materials and different, exotic systems and phases, whose description and analysis often go beyond the standard methods and require novel approaches and quantities to study. Traditional concepts, such as spontaneous symmetry breaking and strong correlations, have been extended or replaced by concepts from topology or highly entangled states. In this respect, quantum information theory offers a different perspective and provides a number of sought-after quantities to tackle these new physics. The emergent "second quantum revolution" and the new field of quantum information, which has been rapidly expanding in the past 2–3 decades, have provided an important application within the field of condensed matter problems. For instance, characterizing the entanglement of a given phase provides complementary information on the physical details of a given system, and by using the fidelity, quantum transitions between different phases can be detected and analyzed, in a way that is to some extent independent of the detailed knowledge of the system properties, such as order parameters.

Guest Editors

Dr. Pedro D. Sacramento

Departamento de Física and CeFEMA, Instituto Superior Técnico, Av. Rovisco Pais, 1049-001 Lisboa, Portugal

Dr. Nikola Paunkovic

SQIG – Instituto de Telecomunicações, Instituto Superior Técnico, Universidade Técnica de Lisboa, Av. Rovisco Pais, 1049-001 Lisboa, Portugal

Deadline for manuscript submissions

closed (31 January 2023)



Symmetry

an Open Access Journal
by MDPI

Impact Factor 2.2
CiteScore 5.3



mdpi.com/si/40264

Symmetry
Editorial Office
MDPI, Grosspeteranlage 5
4052 Basel, Switzerland
Tel: +41 61 683 77 34
symmetry@mdpi.com

[mdpi.com/journal/
symmetry](https://mdpi.com/journal/symmetry)



Search for Articles:

[Advanced](#)[Journals](#) / [Symmetry](#) / [Special Issues](#) / [Quantum Information and Condensed Matter Physics](#)IMPACT
FACTOR
2.2CITESCORE
5.3[Submit to Symmetry](#)[Review for Symmetry](#)[Propose a Special Issue](#)

Journal Menu

- [Symmetry Home](#)
- [Aims & Scope](#)
- [Editorial Board](#)
- [Reviewer Board](#)
- [Topical Advisory Panel](#)
- [Instructions for Authors](#)
- [Special Issues](#)**
- [Topics](#)
- [Sections & Collections](#)
- [Article Processing Charge](#)
- [Indexing & Archiving](#)
- [Editor's Choice Articles](#)
- [Most Cited & Viewed](#)
- [Journal Statistics](#)
- [Journal History](#)

Quantum Information and Condensed Matter Physics

- [Print Special Issue Flyer](#)
- [Special Issue Editors](#)
- [Special Issue Information](#)
- [Keywords](#)
- [Benefits of Publishing in a Special Issue](#)
- [Published Papers](#)

A special issue of *Symmetry* (ISSN 2073-8994). This special issue belongs to the section "**Physics**".

Deadline for manuscript submissions: **closed (31 January 2023)** | Viewed by 18191

Share This Special Issue



Special Issue Editors

Submit to *Symmetry*

Review for *Symmetry*

Propose a Special Issue

volume

issue

Go

> Forthcoming issue

> Current issue

Vol. 17 (2025)

Vol. 16 (2024)

Vol. 15 (2023)

Vol. 14 (2022)

Vol. 13 (2021)

Vol. 12 (2020)

Vol. 11 (2019)

Vol. 10 (2018)

Vol. 9 (2017)

Vol. 8 (2016)

Vol. 7 (2015)

Vol. 6 (2014)

Vol. 5 (2013)

Vol. 4 (2012)

Vol. 3 (2011)

Vol. 2 (2010)

Vol. 1 (2009)

Special Issue Editors



Dr. Pedro D. Sacramento [E-Mail](#) [Website](#)

Guest Editor

Departamento de Fisica and CeFEMA, Instituto Superior Tecnico, Av. Rovisco Pais, 1049-001 Lisboa, Portugal

Interests: Topological phases of matter; Quantum information and condensed matter physics; Non-equilibrium dynamics; Strongly correlated systems; Fractionalization and confinement



Dr. Nikola Paunkovic [E-Mail](#) [Website](#)

Guest Editor

SQIG – Instituto de Telecomunicações, Instituto Superior Técnico, Universidade Técnica de Lisboa, Av. Rovisco Pais, 1049-001 Lisboa, Portugal

Interests: macroscopic distinguishability; phase transitions and the emergence of classicality from quantum physics; entanglement and indistinguishability; entanglement in many-body systems; quantum walks; quantum communication protocols; the concept of indistinguishability in quantum mechanics

Special Issues, Collections and Topics in MDPI journals

Special Issue Information

Dear Colleagues,

Recent years have witnessed the emergence of novel materials and different, exotic systems and phases, whose description and analysis often go beyond the standard methods and require novel approaches and quantities to study. Traditional concepts, such as spontaneous symmetry breaking and strong correlations, have been extended or replaced by concepts from topology or highly entangled states. In this respect, quantum information theory offers a different perspective and provides a number of sought-after quantities to tackle these new physics. The emergent "second quantum revolution" and the new field of quantum information, which has been rapidly expanding in the past 2–3 decades, have provided an important application within the field of condensed matter problems. For instance, characterizing the entanglement of a given phase provides complementary information on the physical details of a given system, and by using the fidelity, quantum transitions between different phases can be detected and analyzed, in a way that is to some extent independent of the detailed knowledge of the system properties, such as order parameters.

This Special Issue of *Symmetry* will focus on the interplay between quantum information and condensed matter, considering both established aspects and new trends in topics such as entanglement, fidelity and fidelity susceptibility, the geometrical aspects of quantum information, topological phase transitions (both symmetry-protected topological phases and phases with long-range topological order), Loschmidt echo and its generalizations to finite temperatures and mixed states, interacting systems, tensor networks, and gauge theories and gauge symmetries. Quenched systems and the associated dynamical phase transitions (these include the behavior of various quantities in time, such as the suggested entanglement, etc.) will also be considered. You are therefore invited to submit either a short review or your original work on any of these subjects.



Submit to *Symmetry*

Review for *Symmetry*

Propose a Special Issue

therefore invited to submit either a short review or your original work on any of these subjects.

Dr. Pedro D. Sacramento

Dr. Nikola Paunkovic

Guest Editors

Manuscript Submission Information

Manuscripts should be submitted online at www.mdpi.com by **registering** and **logging in to this website**. Once you are registered, **click here to go to the submission form**. Manuscripts can be submitted until the deadline. All submissions that pass pre-check are peer-reviewed. Accepted papers will be published continuously in the journal (as soon as accepted) and will be listed together on the special issue website. Research articles, review articles as well as short communications are invited. For planned papers, a title and short abstract (about 100 words) can be sent to the Editorial Office for announcement on this website.

Submitted manuscripts should not have been published previously, nor be under consideration for publication elsewhere (except conference proceedings papers). All manuscripts are thoroughly refereed through a single-blind peer-review process. A guide for authors and other relevant information for submission of manuscripts is available on the **Instructions for Authors** page.

Symmetry is an international peer-reviewed open access monthly journal published by MDPI.

Please visit the **Instructions for Authors** page before submitting a manuscript. The **Article Processing Charge (APC)** for publication in this **open access** journal is 2400 CHF (Swiss Francs). Submitted papers should be well formatted and use good English. Authors may use MDPI's **English editing service** prior to publication or during author revisions.

Keywords

- Symmetry
- Entanglement and entanglement growth
- Fidelity
- Topological phases and transitions
- Geometry, topology, and quantum information





universität
wien

Fakultät für Physik

Institut für Experimentalphysik
Ao. Univ.-Prof. Dr. Caslav Brukner
Boltzmannngasse 5, A-1090 Wien

caslav.brukner@univie.ac.at

Tel.: +43 1 4277 29573

Fax: +43 1 4277 9512

To Whom it May Concern

Vienna, Thursday, 16 February
2006

Concerning: Letter of Invitation for Dr. Nikola
Paunkovic

Dear Madam/Sirs,

This is to confirm that we invite Dr. Nikola Paunkovic to multiple visit our group "Quantum Experiments and Foundation of Physics", at the Institute of Experimental Physics, University of Vienna and work on the joint research projects. We will provide him with the usual infrastructure, namely his own desk and internet and library access. The invitation is valid for the period of six months from March 2006 to September 2006.

Sincerely yours,

Caslav Brukner

Universität Wien
Fakultät für Physik
Institut für Experimentalphysik
Boltzmannngasse 5
A-1090 Wien



universität
wien

Fakultät für Physik

Institut für Experimentalphysik
Ao. Univ.-Prof. Dr. Caslav Brukner
Boltzmannngasse 5, A-1090 Wien

caslav.brukner@univie.ac.at

Tel.: +43 1 4277 29573

Fax: +43 1 4277 9512

To Whom it May Concern

Vienna, Tuesday, 17 July 2007

Concerning: Letter of Invitation for Dr. Nikola
Paunkovic

Dear Madam/Sirs,

This is to confirm that we invite Dr. Nikola Paunkovic to multiple visit our group "Quantum Experiments and Foundation of Physics", at the Institute of Experimental Physics, University of Vienna and work on the joint research projects. We will provide him with the usual infrastructure, namely his own desk and internet and library access. The invitation is valid for the period of six months from August 2007 to February 2008.

Sincerely yours,

Caslav Brukner
University of Vienna
Faculty of Physics
Quantum Optics, Quantum Nanophysics,
Quantum Information
Boltzmannngasse 5
A-1090 Wien
Austria



universität
wien

Fakultät für Physik

Institut für Experimentalphysik
Ao. Univ.-Prof. Dr. Caslav Brukner
Boltzmanngasse 5, A-1090 Wien

caslav.brukner@univie.ac.at

Tel.: +43 1 4277 29573

Fax: +43 1 4277 9512

To
Whom It May Concern

Concerning: Visit Confirmation

Wednesday, 29 October 2008

Dear Madam / Sir,

This is to confirm that Dr. Nikola Paunkovic visited the group "Quantum Optics, Quantum Nanophysics, Quantum Information" at the Faculty of Physics, University of Vienna from October 24th to October 29th 2008. Dr. Paunkovic gave a talk entitled "Macroscopic Distinguishability between Quantum States Defining Different Phases of Matter". With the scientists in Vienna he started collaboration on general macroscopic state distinguishability and the emergence of classical like behaviour.

With best regards,

Caslav Brukner



**Institut für Quantenoptik und
Quanteninformation**

Österreichische Akademie der Wissenschaften

Boltzmannngasse 3
1090 Wien, Austria, Europe
Tel +43 1 4277 29553
iqoqi-vienna@oeaw.ac.at
www.iqoqi-vienna.at

Direktor
Univ.-Prof. Dr. Caslav Brukner
Administrativer Direktor: Alexander Gutschner
Kontaktperson: Sonja Redl

Wien, am 13.12.2017

Dear Colleagues,

This is to confirm that **Dr. Nikola Paunkovic** Instituto de Telecomunicações, Lisbon, visited from November 02 to November 13, 2017 Institute for Quantum Optics and Quantum Information (IQOVI) of the University of Vienna. As a part of the visit, Dr. Paunkovic gave a talk entitled "Quantum contract signing" on Friday, November 10, 2017.

Detailed information on the talk can be found at <https://www.iqoqi-vienna.at/news/events/detail/article/invitation-to-a-talk-nikola-paunkovic-friday-nov-10th-2017-1430h-at-the-iqoqi-seminar-room/>

With best wishes



Marcus Huber

Group leader at the IQOVI Vienna



Institute for Quantum Optics and Quantum Information
Austrian Academy of Sciences
Boltzmannngasse 3
1090 Vienna, Austria
T +43 1 4277 29582
iqoqi-vienna@oeaw.ac.at

Kontakt: marcus.huber@oeaw.ac.at
<http://www.iqoqi-vienna.at/research/huber-group/>
Institut für Quantenoptik und Quanteninformation
Boltzmannngasse 3
1090 Wien



Nikola Paunkovic <npaunkovic@gmail.com>

FW: Request for peer review of a Sêr Cymru II COFUND Fellowship proposal

Lucy.Thomas@wales.gsi.gov.uk <Lucy.Thomas@wales.gsi.gov.uk>

Tue, Nov 1, 2016 at 4:47 PM

To: npaunkov@math.ist.utl.pt

Cc: SERCYMRUII@wales.gsi.gov.uk

Dear **Dr Nikola Paunkovic**,**Request for peer review of a Sêr Cymru II COFUND Fellowship proposal**

I write on behalf of the Welsh Government's Sêr Cymru II Programme (<http://businesswales.gov.wales/expertisewales/support-and-funding-researchers>) to ask if you would be willing to review a research proposal for a Sêr Cymru II **COFUND Fellowship** in [REDACTED] please.

Your recognised expertise and excellent track record will be of great value for our selection process and we should be grateful if you were able to agree.

Background - Sêr Cymru II Programme

Sêr Cymru II is a 7-year funding programme (worth in the region of £60 million) which aims to build research capacity in Wales by attracting and supporting world-class researchers at different stages of their careers.

- Applications have been invited for Research Chairs and fellowships in:
- Life Sciences and Health,
- Advanced Engineering and Materials,
- Low Carbon, Energy and Environment,
- ICT,
- and related areas of Applied Social Science.

A candidate for a Sêr Cymru II **COFUND Fellowship** will be an outstanding researcher in a university, research institute or industry and recognised as having great potential in their field.

The proposal for peer review

The application for peer review relates to a proposed **COFUND Fellowship** and the title of the research is [REDACTED]

Peer review assessment

If you are willing to accept this request, we will ask you to provide an assessment of the application against a template peer review assessment form that is attached for your consideration.

Timescale

To assist our planning and management of this process, I should be grateful if you could let me know if you are willing to accept this request to undertake the peer review as soon as possible please.

If you choose to accept, we will send you the full proposal and associated documents. Unfortunately, we are working to a tight timescale on this and we will require you to return your peer review assessment by **2nd December**. (Please let me know if you require more time).

I hope you will be able to accept our request and I look forward to hearing from you.

Yours sincerely

Lucy.

Lucy Thomas
Llywodraeth Cymru / Welsh Government
Parc Cathays / Cathays Park
Caerdydd / Cardiff
CF10 3NQ

029 2082 1668

Lucy.thomas@cymru.gsi.gov.uk / Lucy.thomas@wales.gsi.gov.uk

On leaving the Government Secure Intranet this email was certified virus free. Communications via the GSi may be automatically logged, monitored and/or recorded for legal purposes.
Wrth adael Mewnrwyd Ddiogel y Llywodraeth nid oedd unrhyw feirws yn gysylltiedig â'r neges hon. Mae'n ddigon posibl y bydd unrhyw ohebiaeth drwy'r GSi yn cael ei logio, ei monitro a/neu ei chofnodi yn awtomatig am resymau cyfreithiol.

2 attachments



Ser Cymru II referee template COFUND.docx

79K



Terms and Conditions for Peer Reviewers for Sêr Cymru II version 1.docx

104K



Nikola Paunkovic <npaunkovic@gmail.com>

FW: Request for peer review of a Sêr Cymru II COFUND Fellowship proposal

Lucy.Thomas@wales.gsi.gov.uk <Lucy.Thomas@wales.gsi.gov.uk>

Mon, Dec 12, 2016 at 5:41 PM

To: npaunkovic@gmail.com

Good afternoon

Thank you very much for your review. Your time and effort is much appreciated.

Regards

Lucy.

Lucy Thomas

Llywodraeth Cymru / Welsh Government
Parc Cathays / Cathays Park
Caerdydd / Cardiff

CF10 3NQ

03000 251 668

Lucy.thomas@cymru.gsi.gov.uk / Lucy.thomas@wales.gsi.gov.uk

From: Nikola Paunkovic [mailto:npaunkovic@gmail.com]

Sent: 01 December 2016 00:51

To: Thomas, Lucy (EST - Science)

Cc: Nikola Paunkovic; SERCYMRUII

[Quoted text hidden]

[Quoted text hidden]

[Quoted text hidden]



Nikola Paunkovic <npaunkovic@gmail.com>

NCN: OPUS Invitation to review grant proposal for the National Science Center, Poland

National Science Centre, Poland <osf_administracja@opi.org.pl>

Fri, Mar 24, 2017 at 2:10 PM

Reply-To: ewelina.szymanska-skolimowska@ncn.gov.pl

To: npaunkov@math.ist.utl.pt

Nikola Paunković

Dear Prospective Reviewer,

We would like to invite you to review a research proposal submitted to the executive government agency of National Science Centre (Narodowe Centrum Nauki - NCN; <http://www.ncn.gov.pl>).

Proposal's data:

We would greatly appreciate your reply within the next 3 days about your intention to review the proposal. Should you choose to accept our invitation, please complete the evaluation form no later than **18th April, 2017** using the OSF electronic submission system (<https://osf.opi.org.pl>).

If you cannot evaluate this proposal we would be grateful for suggesting an alternate qualified reviewer.

We offer remuneration of PLN 400,00 gross (equivalent of c.a. EUR 100 gross) for a completed review of the proposal.

For detailed instructions regarding the use of the system please see [Guidelines for the Written Review](#).

Please do not hesitate to contact us if you require any further information regarding the mission statement of the Centre or the reviewing process.

Kind regards,
dr inż. Ewelina Szymańska-Skolimowska
Discipline Coordinator
National Science Centre
ewelina.szymanska-skolimowska@ncn.gov.pl

--

Utworzono / Created: 2017-03-24, 14:10:28

Regulations

My Account

New Reviewer Invitations (0)

by invitation date

by registration no.

Final reports of international programs

Under Review (0)

by invitation date

by registration no.

Completed Reviews (1)

by date of completion

by registration no.

Date of Completion

contains

Search

Main page

Knowledge base

Helpdesk

Technical support:
Working days:
8:15 am – 4:15 pm CET/CEST
(22) 351-70-89

LIST OF PROPOSALS – COMPLETED REVIEWS

Number of all items 1

Number of items per page: 100 ▾ Sort order: Presented in ascending order ▾ Go to application No.:

1

No.	Reg. No		Date of Completion	Title
1.		View Proposal	2017-04-18	



Nikola Paunkovic <npaunkovic@gmail.com>

Review_request PAUNKOVI'C [REDACTED]

prxquantum@aps.org <prxquantum@aps.org>

Fri, Jan 22, 2021 at 3:51 PM

Reply-To: prxquantum@aps.org

To: npaunkovic@gmail.com

[REDACTED]

Dear Dr. Paunkovic,

We would appreciate your review of this manuscript, which has been submitted to PRX Quantum. The journal is dedicated to the quantum information science and technology community, covering research with an emphasis on lasting and profound impact.

Please read the abstract below and quickly let us know whether we can count on you.

() I will be sending a report within ____ day(s).

() I am unable to review it. Alternative referee suggestions:

Thank you for your help.

Yours sincerely,

Stojan Rebic, Ph.D.

Co-Managing Editor

PRX Quantum

Email: prxquantum@aps.org

<https://journals.aps.org/prxquantum/>

NEWS FROM THE PHYSICAL REVIEW JOURNALS

Eight Physical Review journals introduce Letters, retire Rapid Communications

<http://go.aps.org/3pWrlUS>

Promoting Inclusive and Respectful Communications

<http://go.aps.org/2IU1psq>

APS paying all APC fees for fully open access PRX Quantum in 2021

<http://go.aps.org/2WjdH0H>

We ask that you download the manuscript and return your report via:

[REDACTED]

ABSTRACT:

[REDACTED]

[REDACTED]

FORMS AND MEMOS:

Please see the following:

<https://journals.aps.org/prxquantum/referees/guidelines-for-referees>
Guidelines to referees PRX Quantum

Alternatively, you may send your completed Referee Response Form by email to prxquantum@aps.org. If you use email, either reply to this message or give as the subject "Report PAUNKOVI'C [REDACTED]". Please refrain from using gender-specific pronouns to refer to the author(s) (see attached Guidelines for Referees memo).

PRX Quantum - REFEREE RESPONSE FORM

Insert X in the parentheses in the response form as appropriate.

Referee: Dr. Paunkovi'C,

Manuscript Number: [REDACTED]

Author: [REDACTED]

Title: [REDACTED]

PRX Quantum is highly selective, publishing research with an emphasis on lasting and profound impact.

Submitted manuscripts should meet at least one of the following criteria:

- Significantly advance quantum information science and technology, or push the field in a new direction.
- Establish a substantial connection between different area(s) within quantum information, or between the field and other scientific disciplines.
- Introduce new engineering capabilities, computational concepts, techniques, materials, or methodologies of exceptional importance to the topical area(s) of the journal.
- Address a timely topic of high interest and impact across the multidisciplinary quantum information community.

With this in mind, please assess:

I) Level of innovation:

Negligible ☐ Low ☐ Average ☐ High ☐

Level of significance:

Negligible ☐ Low ☐ Average ☐ High ☐

II) Technically correct and well executed?

Yes ☐ Maybe ☐ No ☐



Nikola Paunkovic <npaunkovic@gmail.com>

Thank you for your report on [REDACTED]

prxquantum@aps.org <prxquantum@aps.org>
To: npaunkovic@gmail.com

Sat, Apr 3, 2021 at 9:20 PM

Here is a copy of your report which you recently submitted via our web server:

Please do not worry if the formatting looks awry; fixed width fonts are required.

Referee: 621338 Dr. N. Paunković
Current Email: npaunkovic@gmail.com
MsCode: [REDACTED]
Date: 03Apr2021

Level of innovation: [REDACTED]
Level of significance: [REDACTED]
Technically correct and well executed? [REDACTED]
Well supported and substantiated? [REDACTED]
Overall scientific quality: [REDACTED]
Quality of presentation: [REDACTED]

Recommendation:

[REDACTED]

begin_report

[REDACTED]



Nikola Paunkovic <npaunkovic@gmail.com>

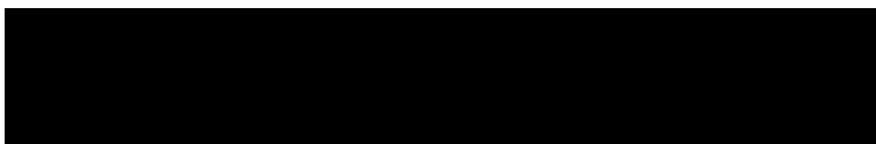
Review_request PAUNKOVI'C [REDACTED]

prl@aps.org <prl@aps.org>

Wed, Jan 18, 2023 at 7:39 PM

Reply-To: prl@aps.org

To: npaunkovic@gmail.com



Dear Dr. Paunkovic,

We would appreciate your review of this manuscript, which has been submitted to Physical Review Letters.

Please read the abstract below and let us know promptly whether or not you will be able to review the manuscript. Suggestions for alternative referees would be welcome.

Comments from the editor:

A previous referee was unable to review this. Our criteria require a clear justification for publication in PRL, as opposed to a specialized journal. Please address the Physical Review Letters criteria of impact, interest, and innovation in your report.

Supplemental Material associated with this manuscript is available via our referee server.

Thank you for your help.

Yours sincerely,

Dr. Abhishek Agarwal
Associate Editor
Physical Review Letters
Email: prl@aps.org
<https://journals.aps.org/prl/>
Follow us on Twitter @PhysRevLett

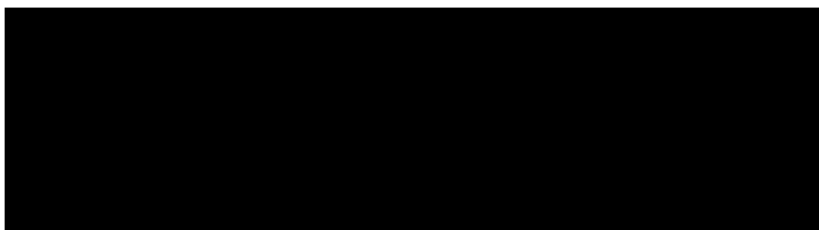
NEWS FROM THE PHYSICAL REVIEW JOURNALS

PRX Energy is now open for submissions
<https://go.aps.org/3lNdlqK>

We ask that you download the manuscript and return your report via:



ABSTRACT:



FORMS AND MEMOS:

Please see the following:

<https://journals.aps.org/prl/referees/guidelines-for-referees>

Guidelines to referees for Physical Review Letters

Alternatively, you may send your completed Referee Response Form by email to prl@aps.org. If you use email, either reply to this message or give as the subject "Report PAUNKOVI'C [REDACTED]".

Physical Review Letters - REFEREE RESPONSE FORM

Insert X in the parentheses in the response form as appropriate.

Referee: Dr. Paunkovi'C,

Manuscript Number: [REDACTED]

Author: [REDACTED]
[REDACTED]

Title: [REDACTED]
[REDACTED]

PRL aims to publish innovative work of significant impact and interest. Your report and recommendation should address the basic question about any possible Letter: Why should this paper be published in PRL, rather than in the Physical Review, which also publishes papers that significantly advance physics?

I. Based on the above, please judge the manuscript regarding its:

1) Impact on the specific field:

very low () () () () () very high

2) Impact on physics research:

very narrow () () () () () very broad

3) Degree of innovation:

very low () () () () () very high

4) Validity:

not valid () () () () () valid

5) Readability for a nonspecialist:



Nikola Paunkovic <npaunkovic@gmail.com>

Thank you for your report on [REDACTED]

prl@aps.org <prl@aps.org>
To: npaunkovic@gmail.com

Thu, Mar 2, 2023 at 5:46 PM

Here is a copy of your report which you recently submitted via our web server:

Please do not worry if the formatting looks awry; fixed width fonts are required.

Referee: 621338 Dr. N. Paunković
Current Email: npaunkovic@gmail.com
MsCode: [REDACTED]
Date: 02Mar2023

	-2	-1	0	1	2
Impact on field:	very low	[REDACTED]			very high
Impact on physics:	very narrow	[REDACTED]			very broad
Innovation:	very low	[REDACTED]			very high
Validity:	not valid	[REDACTED]			valid
Accessibility:	not acc.	[REDACTED]			very acc.

Recommendation:

[REDACTED]

Would you be willing to review the paper again? [REDACTED]

Comments for the Editors:

begin_report

[REDACTED]



Nikola Paunkovic <npaunkovic@gmail.com>

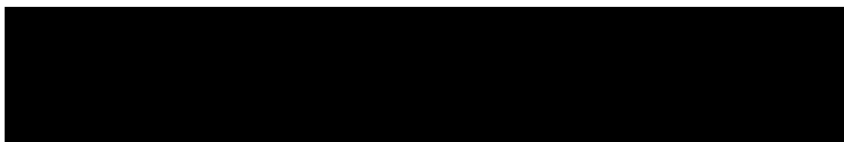
Review_request PAUNKOVI'C [REDACTED]

pra@aps.org <pra@aps.org>

Fri, May 6, 2022 at 9:32 PM

Reply-To: pra@aps.org

To: npaunkovic@gmail.com



Dear Dr. Paunković,

We would appreciate your review of this manuscript, which has been submitted to Physical Review A.

Please read the abstract below and let us know promptly whether or not you will be able to review the manuscript. Suggestions for alternative referees would be welcome.

Thank you for your help.

Yours sincerely,

Dr. Erin Knutson
Associate Editor
Physical Review A
Email: pra@aps.org
<https://journals.aps.org/pr/>
Follow us on Twitter @PhysRevA

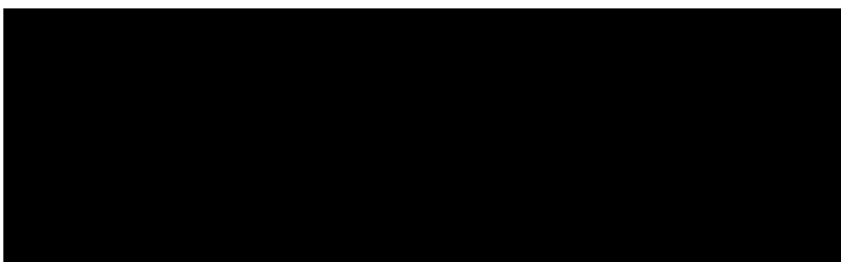
NEWS FROM THE PHYSICAL REVIEW JOURNALS

PRX Energy is now open for submissions

<https://go.aps.org/3lNdlqK>

We ask that you download the manuscript and return your report via:

<https://referees.aps.org/r/> [REDACTED]

ABSTRACT:**FORMS AND MEMOS:**

Please see the following:

<https://journals.aps.org/pr/referees/guidelines-for-referees>

Guidelines to referees for Physical Review

Alternatively, you may send your completed Referee Response Form by email to pra@aps.org. If you use email, either reply to this message or give as the subject "Report PAUNKOVI'C [REDACTED]".

Physical Review - REFEREE RESPONSE FORM

Insert X in the parentheses in the response form as appropriate.

Referee: Dr. Paunkovi'c,

Manuscript Number: [REDACTED]

Author: [REDACTED]

Title: [REDACTED]

1. Please summarize your assessment of the paper:

YES MAYBE NO

Does the paper contain enough significant new physics
to warrant publication in the Physical Review? () () ()
Is the paper scientifically sound and not misleading? () () ()
Is the paper well organized and clearly written? () () ()
Are the subject matter and style of presentation
appropriate for the Physical Review? () () ()
Is the length appropriate? () () ()

2. Please evaluate quality of Research and Presentation:

() Excellent ()
() Good ()
() Average ()
() Marginal ()
() Poor ()

3. Recommendation:

- () Publish without change (please give reasons in report).
() Publish after authors have considered the optional revisions mentioned
in the report.
() Publish after authors have made the revisions mentioned in the report.
(I do not need to see the manuscript again.)
() Revisions are necessary. Return to me on resubmittal.
() Revisions are necessary. On resubmittal, send to:

(Use as much space as needed to list
names of alternative reviewers.)

- () Manuscript is more appropriate for another
() journal (specify):
or () section (specify):
() Do not publish; see report.
() Other; see report.

begin_report (use as much space as is needed). Please refrain from using
gender-specific pronouns to refer to the author(s) (see Guidelines for
Referees memo):

end_report



Nikola Paunkovic <npaunkovic@gmail.com>

Thank you for your report on [REDACTED]

pra@aps.org <pra@aps.org>
To: npaunkovic@gmail.com

Thu, Jul 7, 2022 at 10:04 PM

Here is a copy of your report which you recently submitted via our web server:

Please do not worry if the formatting looks awry; fixed width fonts are required.

Referee: 621338 **Dr. N. Paunković**
Current Email: npaunkovic@gmail.com
MsCode: [REDACTED]
Date: 07Jul2022

Enough significant new physics? [REDACTED]
Sound and not misleading? [REDACTED]
Well organized, clear? [REDACTED]
Subject matter appropriate? [REDACTED]
Length appropriate? [REDACTED]

Quality of research: [REDACTED]
Quality of presentation: [REDACTED]

Recommendation:

[REDACTED]

begin_report

[REDACTED]

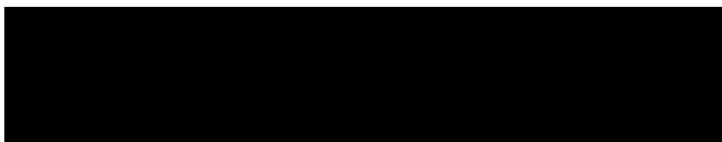


Nikola Paunkovic <npaunkovic@gmail.com>

Review_request PAUNKOVIC [REDACTED]

prb@aps.org <prb@aps.org>
Reply-To: prb@aps.org
To: nikola.paunkovic@qubit.org

Wed, Aug 20, 2008 at 5:03 AM



Dr. N. Paunkovic
SQIG - Instituto de TelecomunicaAAes
IST
P-1049-001 Lisbon, Portugal

Electronic URL-Download Referral from Physical Review B

Dear **Dr. Paunkovic,**

We would appreciate your review of this manuscript, which has been submitted to Physical Review B. This message is the COMPLETE REFERRAL. No hardcopy will be sent unless requested.

Comments from the editor specific to this manuscript:

We apologize for overburdening you, but we would particularly value your opinion.

Physical Review editors wish to maintain and improve the quality of the papers we publish. Is this paper important to the field? Does it significantly advance physics? Please consider these acceptance criteria in your report.

Thank you for your assistance.

We ask that you download the manuscript in PDF or PostScript format from:



Alternatively, you may access our referee server at <http://referees.aps.org/>

Your Referee ID is: 621338

(A link on the site enables you to generate a new password, which is not included here for security reasons, if you do not know your current one.)

We prefer that you return your report by web-upload through the referee server. You may instead send your report by email to prb@ridge.aps.org, or by postal mail or fax. If you use email, either reply to this message or give as the subject **Report PAUNKOVIC [REDACTED]**.

Please include a completed Referee Response Form with your report. In preparing your report, please consider the questions in the Suggestions for Referees. All forms, contact information, etc. are available at the referee web server.

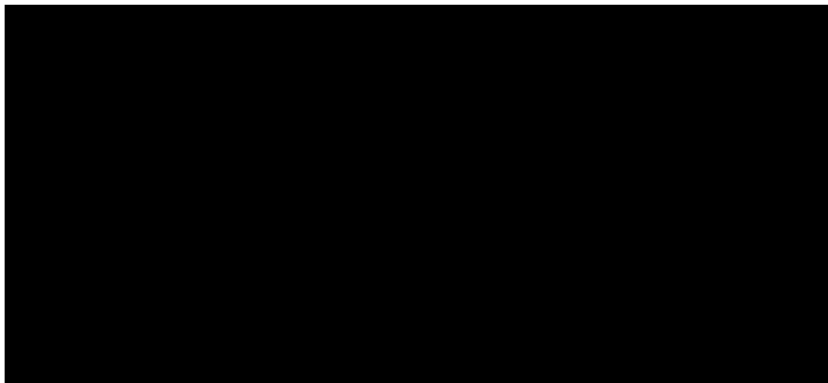
Thank you for your help.

Yours sincerely,

Ashot Melikyan
Assistant Editor
Physical Review B
Email: prb@ridge.aps.org
Fax: 631-591-4141
<http://prb.aps.org/>

PRL Celebrates 50 Years: <http://prl.aps.org/50years/>

ABSTRACT:



=====

FORMS:

=====

Please see the following forms:

<http://forms.aps.org/referee/referral-pr.pdf>
(Copy included)
<http://forms.aps.org/referee/suggestionforrefs-pr.pdf>
Physical Review Suggestions for Referees
<http://forms.aps.org/referee/rwstndrds-prb.pdf>
Review Standards - Notice to Referees - PRB

FORM: REFERRAL-PR-----

refresp-pr
revised 07/05

Physical Review - REFEREE RESPONSE FORM - Electronic mail version

Insert X in the parentheses in the response form as appropriate.

The preferred method for sending referee reports is via our referee web server (<http://referees.aps.org/>). If you do not have a password, you can request one by clicking a button available at the site. Your Referee ID is the six-digit number at the bottom of the first page of this referral, following your name. The referee web server allows you to upload your report and to respond to the questions on the Response

Form by clicking boxes.

Alternatively, you may send your report by email, fax, or conventional mail. If you use email, give as the subject "Report" followed by your last name in upper case, the manuscript code number, and the last name of the first author, for example, "Report BROWN BA1234 Smith"; and include in the message the responses to applicable questions on the Response Form (a template is available at <http://forms.aps.org/referee/refresp-pr.asc>). If you do not receive an acknowledgment within one working day, please repeat the message or send the report via another mode. (For technical reasons, we cannot send automatic acknowledgments if the subject line contains "Re:", "re:", etc., so please avoid such subject lines.)

If you use conventional mail or fax, please include the Response Form. The manuscript should not be returned (except perhaps for pages you have marked for the benefit of the author). Do not automatically follow an email or fax report with a backup by conventional mail.

Referee: Dr. Paunkovic, 621338

Manuscript Number: [REDACTED]

Author: [REDACTED]

Title: [REDACTED]

1. Please summarize your assessment of the paper:

YES MAYBE NO

Does the paper contain enough significant new physics
to warrant publication in the Physical Review? ☐ ☐ ☐
Is the paper scientifically sound and not misleading? ☐ ☐ ☐
Is the paper well organized and clearly written? ☐ ☐ ☐
Are the subject matter and style of presentation
appropriate for the Physical Review? ☐ ☐ ☐
Is the length appropriate? ☐ ☐ ☐

2. Please evaluate quality of Research and Presentation:

☐ Excellent ☐
☐ Good ☐
☐ Average ☐
☐ Marginal ☐
☐ Poor ☐

3. Recommendation:

- ☐ Publish without change (please give reasons in report).
☐ Publish after authors have considered the optional revisions mentioned in the report.
☐ Publish after authors have made the revisions mentioned in the report. (I do not need to see the manuscript again.)
☐ Revisions are necessary. Return to me on resubmittal.
☐ Revisions are necessary. On resubmittal, send to:

(Use as much space as needed to list
names of alternative reviewers.)

- ☐ Manuscript is more appropriate for another
☐ journal (specify):
or ☐ section (specify):
☐ Do not publish; see report.
☐ Other; see report.



Nikola Paunkovic <npaunkovic@gmail.com>

Thanks [REDACTED]**prb@aps.org** <prb@aps.org>

Thu, Apr 30, 2009 at 8:37 PM

Reply-To: prb@aps.org

To: nikola.paunkovic@qubit.org

[REDACTED]

Dr. N. Paunkovic
SQIG - Instituto de TelecomunicaAAes
IST
P-1049-001 Lisbon, Portugal

Dear Dr. Paunkovic,

Thank you very much for reviewing this paper. It was [REDACTED]
[REDACTED]

Your comments and advice for this work were appreciated. We enclose pertinent correspondence for your information and look forward to your continuing efforts as a referee on behalf of the Physical Review.

Yours sincerely,

Susan Farrant
Senior Assistant Editor
Physical Review B
Email: prb@ridge.aps.org
Fax: 631-591-4141
<http://prb.aps.org/>

Physics - spotlighting exceptional research: <http://physics.aps.org/>
PRB Editors' Suggestions: <http://prb.aps.org/#suggestions>

Second Report of the First Referee -- [REDACTED]

[REDACTED]



Nikola Paunkovic <npaunkovic@gmail.com>

Review_request PAUNKOVI'C [REDACTED]

pre@aps.org <pre@aps.org>

Tue, Dec 14, 2021 at 3:08 PM

Reply-To: pre@aps.org

To: npaunkovic@gmail.com

[REDACTED]

Dear Dr. Paunković,

We would appreciate your review of this manuscript, which has been submitted to Physical Review E. We append below the abstract of the manuscript. We realize that you may not be able to respond quickly, or at all, due to the current COVID-19 crisis. However, if you can, we would be grateful for your reply within 3 days, advising of your ability to return a report within 21 days. If you need extra time to prepare a report, or we can do something else to help you with your review, please let us know. If you cannot review, advice on suitable referees would be welcome.

To accept to review, visit:

[REDACTED]

To decline to review, visit:

[REDACTED]

If you need more information or would like to send us a report now, please log into our referee server at:

[REDACTED]

Comments from the editor:

Physical Review editors would like your help in maintaining high standards for our journal. Is this paper important to the field?
Does it significantly advance physics?

Thank you for your help.

Yours sincerely,

Juan-Jose Lieten-Santos

Associate Editor

Physical Review E

Email: pre@aps.org

<https://journals.aps.org/pre/>

Follow us on Twitter @PhysRevE

NEWS FROM THE PHYSICAL REVIEW JOURNALS

PRX Energy is now open for submissions

<https://go.aps.org/3lNdlqK>

ABSTRACT:

[REDACTED]

FORMS AND MEMOS:

Please see the following:

<https://journals.aps.org/pre/referees/guidelines-for-referees>

Guidelines to referees for Physical Review

Alternatively, you may send your completed Referee Response Form by email to pre@aps.org. If you use email, either reply to this message or give as the subject "Report PAUNKOVI'C".

Physical Review - REFEREE RESPONSE FORM

Insert X in the parentheses in the response form as appropriate.

Referee: Dr. Paunković,

Manuscript Number:

Author:

Title:

1. Please summarize your assessment of the paper:

YES MAYBE NO

Does the paper contain enough significant new physics to warrant publication in the Physical Review? () () ()

Is the paper scientifically sound and not misleading? () () ()

Is the paper well organized and clearly written? () () ()

Are the subject matter and style of presentation appropriate for the Physical Review? () () ()

Is the length appropriate? () () ()

2. Please evaluate quality of Research and Presentation:

() Excellent ()

() Good ()

() Average ()

() Marginal ()

() Poor ()

3. Recommendation:

() Publish without change (please give reasons in report).

() Publish after authors have considered the optional revisions mentioned in the report.

() Publish after authors have made the revisions mentioned in the report. (I do not need to see the manuscript again.)

() Revisions are necessary. Return to me on resubmittal.

() Revisions are necessary. On resubmittal, send to:

(Use as much space as needed to list names of alternative reviewers.)

() Manuscript is more appropriate for another

() journal (specify):

or () section (specify):

() Do not publish; see report.



Nikola Paunkovic <npaunkovic@gmail.com>

Thank you for your report on [REDACTED]

pre@aps.org <pre@aps.org>
To: npaunkovic@gmail.com

Mon, Mar 21, 2022 at 9:07 PM

Here is a copy of your report which you recently submitted via our web server:

Please do not worry if the formatting looks awry; fixed width fonts are required.

Referee: 621338 Dr. N. Paunković
Current Email: npaunkovic@gmail.com
MsCode: [REDACTED]
Date: 21Mar2022

Enough significant new physics? [REDACTED]
Sound and not misleading? [REDACTED]
Well organized, clear? [REDACTED]
Subject matter appropriate? [REDACTED]
Length appropriate? [REDACTED]

Quality of research: [REDACTED]
Quality of presentation: [REDACTED]

Recommendation:

[REDACTED]

begin_report

[REDACTED]

end_report

Comments for the Editors:

<UnidCorrFileAtt=YES>



Nikola Paunkovic <npaunkovic@gmail.com>

npj Quantum Information Invitation to Review for [REDACTED]

npjqi@nature.com <npjqi@nature.com>

Tue, May 9, 2023 at 8:51 AM

Reply-To: npjqi@nature.com

To: npaunkovic@gmail.com

Dear Dr. Paunkovic,

I am writing to invite you to review a manuscript for *npj Quantum Information*. The manuscript is entitled [REDACTED] and comes from [REDACTED] and colleagues; the abstract and author list are appended below. We would hope to receive your comments within 14 days from now, though if you require a few extra days then do let us know.

Part of the Nature Partner Journals series, *npj Quantum Information* is a Nature Research journal published by Springer Nature in partnership with University of New South Wales. The journal is open access and is dedicated to publishing the finest research on quantum information, including quantum computing, quantum communications and quantum information theory (full aims and scope can be seen at the journal website: <https://www.nature.com/npjqi/about/aims>).

To view the manuscript information, and to accept or decline this invitation, please use the link below (please click on the link or cut and paste the entire link into a new browser window. If the link is split between two or more lines, you will need to copy and paste each line of the link separately into a new browser window, making sure that no characters have been omitted).

[REDACTED]

If you accept this invitation you will be given online access to the manuscript files, instructions for referees, and the form to upload your report. We also hope that you would be willing to assess any revised versions of this paper.

If you are unable to review on this occasion, we would appreciate any suggestions for alternative reviewers with a similar expertise to yours - perhaps someone from your own research group? We strive to achieve a [diverse demographic representation](#) among our reviewers and we would welcome suggestions from under-represented groups in relation to gender, geographical origin and career stage.

Your prompt response to this request would be greatly appreciated, as is any time that you are able to spare us.

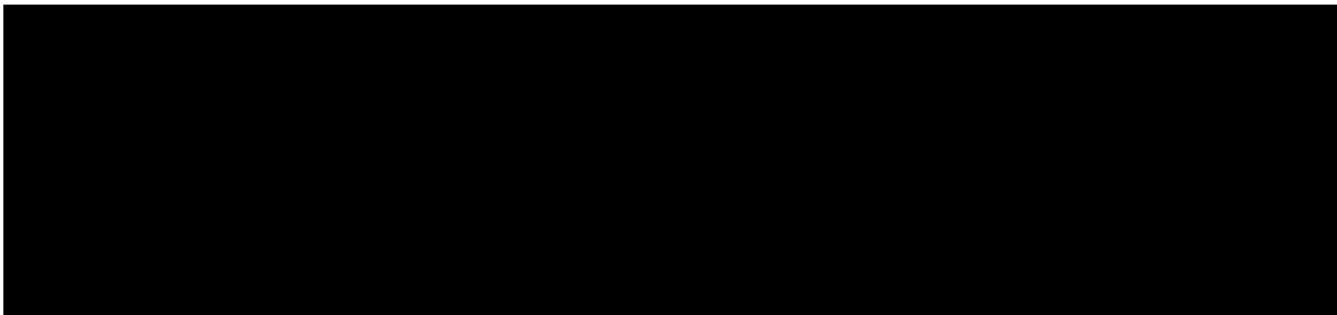
Yours sincerely,

Sarah Croke
Associate Editor
npj Quantum Information

Please note that your contact details are being held on our editorial databases which are used only for the management of the peer review process, and we might contact you in relation to Nature Research journals other than this one when your expertise is appropriate. If you would prefer us not to contact you in the future please let us know by emailing npjqi@nature.com.

Author list

Manuscript abstract



This email has been sent through the Springer Nature Tracking System NY-610A-NPG&MTS

Confidentiality Statement:

This e-mail is confidential and subject to copyright. Any unauthorised use or disclosure of its contents is prohibited. If you have received this email in error please notify our Manuscript Tracking System Helpdesk team at [Platform Support Helpdesk](#).

Details of the confidentiality and pre-publicity policy may be found here <http://www.nature.com/authors/policies/confidentiality.html>

[Privacy Policy](#) | [Update Profile](#)



Nikola Paunkovic <npaunkovic@gmail.com>

Thank you for submitting your review for [REDACTED] for the npj Quantum Information

npjqi@nature.com <npjqi@nature.com>

Fri, Jul 28, 2023 at 3:46 PM

Reply-To: npjqi@nature.com

To: npaunkovic@gmail.com

28th Jul 23

Dear Dr. Paunkovic:

Thank you for your review of [REDACTED]
[REDACTED] which we have safely
received. A copy of this review is attached for your reference.

Yours sincerely,

Manuscript Administration
npj Quantum Information

Priority of Publication: [REDACTED]

Recommendation: [REDACTED]

Comments to the Section Editor:

Comments to the Author:

Please see the attached.

Opt in to ORCID? (required): Yes

This email has been sent through the Springer Nature Tracking System NY-610A-NPG&MTS

Confidentiality Statement:

This e-mail is confidential and subject to copyright. Any unauthorised use or disclosure of its contents is prohibited. If you have received this email in error please notify our Manuscript Tracking System Helpdesk team at [Platform Support Helpdesk](#).

Details of the confidentiality and pre-publicity policy may be found here <http://www.nature.com/authors/policies/confidentiality.html>

[Privacy Policy](#) | [Update Profile](#)



Nikola Paunkovic <npaunkovic@gmail.com>

Quantum would like you to review: [REDACTED]
[REDACTED]

Dan Browne <notifications@email.scholasticahq.com>
Reply-To: conversations-[REDACTED]@email.scholasticahq.com
To: npaunkov@math.tecnico.ulisboa.pt

Thu, Apr 15, 2021 at 10:53 AM

You've been invited to review a manuscript by *Quantum*.
To accept or decline, click the link below or copy into your browser:

[REDACTED]

Dear Nikola,

I hope this email finds you well. I was wondering if you would be interested in reviewing the manuscript [REDACTED]
[REDACTED] for **Quantum**?

It is important that you please **let me know within a week** whether you are able to review this paper by choosing the option below. Thank you!

Here is some information about the journal:

[Quantum](#) is an **open-access** peer-reviewed journal for quantum science and related fields. **Quantum** is **non-profit** and **community-run**: it is an effort by researchers and for researchers to make science more open and publishing more transparent and efficient.

Acceptance threshold:

Quantum is **selective**. Correct research that incrementally improves a limited technique is below threshold. For original research, **either a significant technical or conceptual contribution**, or a nice combination of both is necessary for acceptance in Quantum. If you

have any questions about these criteria and their implementation, please contact me (simply reply to this email). The manuscript must be relevant for the community of the respective field. On the other hand, the expected number of citations is not an editorial criterion.

Review form:

To ensure a fair and transparent evaluation of submissions, Quantum asks referees **specific questions** concerning the technical and conceptual contributions of manuscripts, as well the quality of presentation. Nevertheless, if you would rather submit a **free-form review**, simply reply to this email and attach a file with your report. Please be aware that if you submit your report in this way, I will have to **manually associate the report with this referral** and mark it as completed. This can take a while and in the meantime you will **continue to receive automatic reminders**.

You can **preview the report form**, guidelines for referees and **acceptance criteria** [here](#).

If you believe that the manuscript does not warrant an in-depth review, or suspect you may have a conflict of interest, your feedback is still very valuable to us. For such communication, as well as any **comments or questions**, please simply **reply to this email**.

You may co-review the manuscript together with a suitable colleague. In that case, please let me know who else contributed to the review.

Yours sincerely,
Dan

Dan Browne
Editor at Quantum

By accepting to review a work for **Quantum**, you accept the [Editorial Policies](#) as well as the [Terms and Conditions](#) of **Quantum**.

Note: reviews are **single-blind**. Your reports are confidential, and your identity will only be shared with the Editorial Board (and admins from or working for the Executive Board, for troubleshooting purposes).

Either way, your identity will not be shared with anyone who has a conflict of interest.

Manuscript Details

Title

[REDACTED]

Authors

[REDACTED]

Deadline

May 15, 2021 - 5:00 pm CEST

Abstract

[REDACTED]

You've been invited to review a manuscript by *Quantum*.

To accept or decline, click the button below or copy this link into your browser:



Accept/decline invitation



Any questions?

This journal uses the Scholastica submission management platform to manage its review process! Our guide, *Reviewing Articles is Easy: A Helpful Guide for Reviewers*, provides a look at how reviewers use Scholastica to accept/decline reviewer invitations, submit reviews to journals, and more.

[Get the guide](#)



Nikola Paunkovic <npaunkovic@gmail.com>

Review successfully submitted

Quantum <notifications@email.scholasticahq.com>
Reply-To: Scholastica <noreply@email.scholasticahq.com>
To: Nikola Paunković <npaunkov@math.tecnico.ulisboa.pt>

Sat, Jul 17, 2021 at 6:47 PM

**Scholastica**

Your modern academic journal management platform

Hello Nikola Paunković,

Congrats!
**Your review has
been successfully
submitted**



Your review for [REDACTED]
[REDACTED] has been **successfully submitted** to *Quantum*.
The editors have been notified.

You can go back and read your review at anytime by logging into your Scholastica account and clicking "My Reviews".

[Read your review](#)

If you have any questions you can contact *Quantum* directly at
info@quantum-journal.org

PhD Thesis

Quantum oblivious transfer

João Paulo do Amaral de Jesus Rodrigues — 2017

Key information

Authors:

João Paulo do Amaral de Jesus Rodrigues ([João Paulo do Amaral de Jesus Rodrigues](#))

Supervisors:

Paulo Alexandre Carreira Mateus ([Paulo Alexandre Carreira Mateus](#)); [Nikola Paunkovic](#) ([Nikola Paunkovic](#))

Published in

04/07/2017

Abstract

A computação distribuída tem vindo a ganhar cada vez mais terreno devido à facilidade de comunicação entre dispositivos que tem vindo a aumentar, e ao avanço na capacidade de processamento de grandes quantidades de dados. A Computação Distribuída Segura (em inglês, Secure multiparty Computation, SMC) emerge num contexto onde se quer processar dados de múltiplas entidades, mas em que a privacidade destes dados têm de ser mantidas. A SMC possibilita a mineração de dados privados, votação electrónica, leilões electrónicos, entre outras funcionalidades seguras. Actualmente, todas estas funcionalidades são feitas recorrendo a uma entidade de confiança (trusted third party, TTP, em inglês) que idealmente permite a privacidade dos dados de cada entidade. Mas a informação terá de ser acedida pela TTP. O SMC permite cumprir a função do TTP sem essa partilha de dados. Um resultado bem estabelecido é que o SMC pode ser realizado recorrendo ao protocolo de transferência oblívia entre dois participantes (vide, por exemplo, [58]). No entanto, a segurança destes



computadores quânticos, ainda que só em teoria, constituem uma ameaça a estes problemas. Por outro lado, a segurança perfeita de protocolos de distribuição de chaves pode ser atingida recorrendo a tecnologias quânticas. A segurança baseia-se nas leis da física e actualmente existem várias propostas de distribuição de chaves a serem estudadas. Comercialmente já existem soluções baseadas no protocolo BB84 proposto por Bennett e Brassard, o primeiro protocolo demonstrado ser, teoricamente, incondicionalmente seguro. Esta tese é dedicada ao estudo de propriedades quânticas para a implementação de protocolos de transferência oblívia. Apresentaremos um protocolo de transferência oblívia de uma mensagem baseados em rotações em qubits, um de transferência oblívia de um bit com passeio aleatório quântico discreto e dois protocolos de transferência oblívia de mensagens recorrendo a estados quânticos coerentes, cujas seguranças se baseiam nas leis da física.

Distributed computation has been growing throughout recent years due to the ease of communication between different devices and the growth of computational power. On the other hand, there has always been the need for separate entities to share critical information with some designated party in order to calculate the market price for goods, voting, auctions, and so on. Nowadays, all these functionalities are carried out entrusting critical data to a trusted third party (TTP). By the nature of those data, any leakage could be harmful for some of the entities. Secure Multiparty Computation (SMC) emerges in this context where multiple entities wish to jointly process their data without entrusting critical data to a TTP. A well established result is that SMC can be implemented using oblivious transfer protocols (see, for example, [58]). As a drawback, the security of these protocols, as well as of almost all key exchange and asymmetric encryption schemes, relies on computational hardness of some mathematical problem. Quantum computers, for now only on the theoretical level, are a serious threat to all those cryptographic systems aforementioned. Quantum systems are a threat to classical cryptographic systems, but they are also a solution when it comes to key exchange protocols. Bennett and Brassard proposed the first quantum key exchange protocol which was proven unconditionally secure at the theoretical level. Ever since then, more proposals began to appear and some were proven to be unconditionally secure. Security of these protocols is based on the laws of physics. This thesis is dedicated to the proposal and the study of oblivious transfer protocols based on quantum mechanics. We will present a bit string oblivious transfer protocol based on single-qubits rotations, a bit oblivious transfer with discrete-time quantum random walks and two bit-string oblivious transfer protocols based on coherent quantum states and discuss their security under practical assumptions.

Publication details



**João Paulo do Amaral de Jesus
Rodrigues**
ist152086

Supervisors of this institution:



**Paulo Alexandre Carreira
Mateus**
ist13783



Nikola Paunkovic
ist32694

RENATES TID

101552980

Degree Name

Doutoramento em Segurança de Informação

Fields of Science and Technology (FOS)

computer-and-information-sciences - **Computer and information sciences**

Keywords

OBLIVIOUS TRANSFER

PERFECT SECRECY

QUANTUM WALKS

COHERENT STATES

TRANSFERÊNCIA OBLÍVIA

SEGURANÇA PERFEITA

PASSEIO ALEATÓRIO QUÂNTICO

ESTADOS COERENTES

Publication language (ISO code)

eng - English

Rights type:

Open access

Instituto Superior Técnico

Financing entity

Instituto de Telecomunicações

Financing entity

Fundação para a Ciência e a Tecnologia

Download files

[Thesis - Quantum Oblivious Tran...](#) (7.98 MB)

AVAILABLE

Cite publication

Powered by FenixEdu™

[User manual](#)

CO-FINANCED BY:

[Support materials](#)

[Support](#)

[Open Access Policy](#)



[FAQ](#)

2022-2025 © Instituto Superior Técnico



TÉCNICO
LISBOA

UNIVERSIDADE DE LISBOA
INSTITUTO SUPERIOR TÉCNICO

Quantum Oblivious Transfer

João Paulo do Amaral de Jesus Rodrigues

Supervisor: Doctor Paulo Alexandre Carreira Mateus

Co-Supervisor: Doctor Nikola Paunković

**Thesis approved in public session to obtain the PhD Degree in
Information Security**

Jury final classification: Pass with Distinction

Jury

Chairperson: Chairman of the IST Scientific Board

Members of the Committee:

Doctor Vítor João Rocha Vieira, Invited Full Professor, Instituto Superior Técnico, Universidade de Lisboa

Doctor Armando Humberto Moreira Nolasco Pinto, Associate Professor, Universidade de Aveiro

Doctor Paulo Alexandre Carreira Mateus, Assistant Professor (with Habilitation), Instituto Superior Técnico, Universidade de Lisboa

Doctor João Filipe Quintas dos Santos Rasga, Assistant Professor, Instituto Superior Técnico, Universidade de Lisboa

Doctor Jeroen Antonius Maria van de Graaf, Adjunct Professor, Universidade Federal de Minas Gerais, Brasil

Doctor Nikola Paunković, Researcher, Instituto de Telecomunicações, Lisboa

Funding Institutions:

**Instituto de Telecomunicações
Fundação para a Ciência e a Tecnologia**

2017

PhD Thesis

Quantum walks in cryptography and finite-temperature topological phase transitions

Chrysoula Vlachou — 2018

Key information

Authors:

Chrysoula Vlachou ([Chrysoula Vlachou](#))

Supervisors:

Paulo Alexandre Carreira Mateus ([Paulo Alexandre Carreira Mateus](#)); [Nikola Paunković \(Nikola Paunkovic\)](#)

Published in

09/07/2018

Abstract

Quantum cryptography is an active area of research, since it was shown that the security of some of the classical cryptosystems currently used can be compromised by adversaries with access to quantum computers. In the first part of this thesis, we propose new secure quantum cryptosystems based on quantum walks, which have been proved very useful in several quantum computation tasks. In particular, we design a secure quantum public-key cryptosystem, as an alternative to the classical counterparts, whose security can be jeopardised by quantum adversaries. Moreover, we propose three new quantum key distribution protocols and analyse their security and robustness properties.

The design of long-term stable quantum memories is currently one of the biggest technological challenges towards the construction of operational and scalable quantum



behaviour of systems exhibiting topological order, as they possess some unique properties which could be used to construct quantum memories. By means of the fidelity between two quantum states and the Uhlmann parallel transport condition in the space of the purifications of density matrices, we investigate the existence of topological phase transitions at finite temperatures. We also probe the robustness of the edge states on the boundary between two different symmetry-protected topological phases with respect to the temperature. This analysis shows that there exist no thermal phase transitions and the topological features, present at zero temperature, are gradually smeared out as the temperature increases. Our study of the Majorana modes (edge states of topological superconductors) at low but finite temperatures, suggests that they could be used to achieve realistic quantum memories.

We also performed the same analysis for the effective Hamiltonians resulting from quantum walk protocols that have been shown to simulate symmetry-protected topological phases. The results that we obtained are consistent with the previous, indicating the absence of thermally-driven phase transitions. Moreover, in this case, our analysis revealed the existence of finite-temperature parameter-driven phase transitions.

Finally, we investigated the existence of finite-temperature phase transitions in topological systems out of equilibrium. So far, there exist two different approaches to infer the possibility of phase transitions at finite temperatures for such systems, which were giving opposite predictions. We analytically derived the relevant quantities and showed the origin of such different behaviours. Moreover, we argued which is the most suitable approach that better captures the many-body nature of topological systems and can be used in realistic implementations.

Publication details

Authors in the IST community:



Chrysoula Vlachou
ist423035

Supervisors of this institution:



**Paulo Alexandre Carreira
Mateus**
ist13783



Nikola Paunkovic
ist32694

101598440

Degree Name

Doutoramento em Física

Fields of Science and Technology (FOS)

physical-sciences - Physical sciences

Publication language (ISO code)

eng - English

Rights type:

Embargo lifted

Date available:

06/11/2019

Institution name

Instituto Superior Técnico

Download files

[Vlachou_thesis_final.pdf](#) (8.28 MB)

AVAILABLE

Cite publication

UNIVERSIDADE DE LISBOA
INSTITUTO SUPERIOR TÉCNICO

Quantum walks in cryptography and
finite-temperature topological phase transitions

Chrysoula Vlachou

Supervisor: Doctor Paulo Alexandre Carreira Mateus

Co-Supervisor: Doctor Nikola Paunković

Thesis approved in public session to obtain the PhD Degree in
Physics

Jury final classification: Pass with Distinction

Jury

Chairperson: Doctor José Luís Rodrigues Júlio Martins, Instituto Superior Técnico da Universidade de Lisboa

Members of the Committee:

Doctor Armando Humberto Moreira Nolasco Pinto, Universidade de Aveiro

Doctor Pedro Domingos Santos do Sacramento, Instituto Superior Técnico da Universidade de Lisboa

Doctor Miguel António da Nova Araújo, Escola de Ciências e Tecnologia da Universidade de Évora

Doctor Nikola Paunković, Instituto de Telecomunicações, Lisboa

Funding Institution: Fundação para a Ciência e a Tecnologia (FCT)

2018

PhD Thesis

Tracking topological phase transitions using information geometric quantities

Syed Tahir Amin — 2020

Key information

Authors:

Syed Tahir Amin ([Syed Tahir Amin](#))

Supervisors:

Vítor João Rocha Vieira ([Vítor João Rocha Vieira](#)); [Nikola Paunkovic \(Nikola Paunkovic\)](#)

Published in

02/28/2020

Abstract

This thesis is devoted to the study of topological phase transitions in 2D topological insulators and various kinds of topological superconductors of free fermions using information geometric quantities: fidelity, fidelity susceptibility, and a quantity closely related to the Uhlmann phase. By using Boltzmann Gibbs states, we also incorporate finite temperature effects on the fate of topological phase transitions. Fidelity basically measures how similar or different two states are. Our first non-trivial results include the detection of topological phase transitions in 2D topological insulators and topological superconductors with short-range hopping and pairing amplitudes. The systems under study are translationally invariant. The Hamiltonians of topological insulators and topological superconductors depend on some parameters, such as hopping amplitudes or chemical potential, which drive the systems across different topological phases. The parameter points



Uhlmann quantity is constructed in such a way that it only captures the sudden variations in the eigenstates of the density operators. We find that both quantities capture the critical points of topological phase transitions. The drop in the fidelity from one in the parameter manifold signals phase transitions. The departure of the Uhlmann quantity from zero across critical points also signals topological phase transitions. Both the drop of the fidelity and the peak of the Uhlmann quantity at critical points gradually smear out as we increase the temperature of the systems under study. To investigate the temperature effects, we analytically proved the absence of topological phase transitions by studying the fidelity susceptibility in great detail for the models considered. We find that the two limits of the fidelity susceptibility, zero-temperature limit and thermodynamic limit, do not commute. The fidelity susceptibility which is obtained by first taking the zero-temperature limit and then the thermodynamic limit always diverges at critical points and thus signals topological phase transitions. Whereas, the fidelity susceptibility which is obtained by first applying the thermodynamic limit and then the zero-temperature limit gets one additional term which cures the divergence and thus is perfectly normal. We also studied edge states of the topological insulator. Our analysis of the edge states with respect to temperature strengthens the argument of the gradually smearing out of the topological behavior of the system. We also calculated the critical exponents. After studying the topological phase transitions across critical points, we start working on topological phase transitions across the critical lines in parameter manifolds. First, we consider the Kitaev chain with long-range pairing and then a 2D topological superconductor with both long-range pairing and hopping amplitudes. Using our recent theory of information geometric quantities we find the following features: the drop in the fidelity and peaking up of the Uhlmann quantity is maximum when we cross the critical line perpendicularly; when moving along the critical lines we find that the states in the parameter space stay approximately the same and therefore the drop in the fidelity, the divergence in the fidelity susceptibility and the peak of the Uhlmann quantity disappear. We also find that in the long-range Kitaev model, the critical exponents across the critical lines are not the same. Along with the Kitaev model with long-range hopping amplitudes, we also study the Kitaev model with long-range pairing amplitudes and the Haldane model to see the behavior of our information geometric quantities along the critical lines in parameter manifold.

Esta tese é dedicada ao estudo de transições de fase topológicas em isoladores topológicos 2D e vários tipos de supercondutores topológicos de férmions livres usando quantidades geométricas da teoria da informação: fidelidade, susceptibilidade da fidelidade e uma quantidade intimamente relacionada com a fase de Uhlmann. Usando os estados de Boltzmann-Gibbs, estudamos também os efeitos da temperatura finita sobre o que acontece as transições de fase topológicas. Os nossos primeiros resultados não triviais incluem a detecção de transições de fase topológicas em isoladores topológicos 2D e supercondutores topológicos com amplitudes de salto e emparelhamento de longo alcance em estudo de



conduzem os sistemas através de diferentes fases topológicas. Esses parâmetros geralmente controlam transições de fase topológicas no espaço de parâmetros. Os pontos em que as transições de fase ocorrem são conhecidos como pontos críticos. A fidelidade captura a mudança drástica nos valores próprios e nos estados próprios dos operadores de densidade. Por outro lado, a quantidade de Uhlmann é construída de tal maneira que captura apenas as variações repentinas nos estados próprios dos operadores de densidade. Nós descobrimos que ambas as quantidades capturam os pontos críticos das transições de fase topológicas. A queda na fidelidade de um no espaço de parâmetros sinaliza transições de fase. O desvio da quantidade de Uhlmann de zero entre pontos críticos também sinaliza transição de fase topológicas. Tanto a queda da fidelidade como o pico da quantidade de Uhlmann em pontos críticos diminuem gradualmente à medida que aumentamos a temperatura do sistema. Para investigar os efeitos da temperatura, comprovamos analiticamente a ausência de transições de fase topológicas, estudando a susceptibilidade da fidelidade em grande detalhe para os modelos considerados. Descobrimos que os dois limites da susceptibilidade da fidelidade, limite de temperatura zero e limite termodinâmico, não coincidem. A susceptibilidade da fidelidade, obtida tomando primeiro o limite de temperatura zero e depois o limite termodinâmico, diverge sempre em pontos críticos e, portanto, sinaliza transições topológicas de fase. Ao passo que a susceptibilidade da fidelidade, obtida pela aplicação primeiro do limite termodinâmico e depois do limite de temperatura zero, obtém um termo adicional que cura a divergência e é, portanto, perfeitamente normal. Também estudamos estados de borda do isolador topológico. A nossa análise dos estados das bordas em relação à temperatura reforça o argumento da eliminação gradual do comportamento topológico do sistema. Calculamos também os expoentes críticos. Depois de estudar as transições de fase topológicas nos pontos críticos, começamos a trabalhar nas transições de fase topológicas nas linhas críticas no espaço de parâmetros. Primeiro, consideramos a de Kitaev com emparelhamento de longo alcance e, em seguida, um supercondutor topológico 2D com amplitudes de emparelhamento e salto de longo alcance. Usando a nossa teoria recente das quantidades geométricas da teoria da informação, encontramos os seguintes resultados: A queda na fidelidade e o pico da quantidade de Uhlmann são máximos quando cruzamos a linha crítica perpendicularmente; ao longo das linhas críticas os estados no espaço dos parâmetros permanecem aproximadamente os mesmos, portanto, a queda na fidelidade, a divergência da susceptibilidade da fidelidade e o pico da quantidade de Uhlmann desaparecem. Também descobrimos que no modelo de Kitaev de longo alcance, os expoentes críticos nas linhas críticas não são os mesmos. Juntamente com o modelo de Kitaev com amplitudes de salto de longo alcance, também estudamos o modelo de Kitaev com amplitudes de emparelhamento de longo alcance e o modelo de Haldane para ver o comportamento das nossas quantidades geométricas da teoria da informação ao longo das linhas críticas no espaço de parâmetros.

**Authors in the IST community:****Syed Tahir Amin**

ist426602

Supervisors of this institution:**Vítor João Rocha Vieira**

ist10953

**Nikola Paunkovic**

ist32694

RENATES TID

101495927

Degree Name

Doutoramento em Física

Fields of Science and Technology (FOS)

physical-sciences - Physical sciences

Keywords

TOPOLOGICAL PHASES TRANSITIONS

FIDELITY

FIDELITY SUSCEPTIBILITY

UHLMANN PHASE

FASES TOPOLDGICAS

TRANSIÇÕES DE FASES TOPOLDGICAS

FIDELIDADE

SUSCETIBILIDADE DA FIDELIDADE

FASE DE UHLMAN

Publication language (ISO code)

eng - English

Embargo lifted

Date available:

12/05/2020

Institution name

Instituto Superior Técnico

Download files

[Thesis.pdf](#) (16.59 MB)

AVAILABLE

Cite publication

Powered by FenixEdu™

[User manual](#)

CO-FINANCED BY:

[Support materials](#)

[Support](#)

[Open Access Policy](#)



[FAQ](#)

2022-2025 © Instituto Superior Técnico

UNIVERSIDADE DE LISBOA
INSTITUTO SUPERIOR TÉCNICO

**Tracking topological phase transitions using information
geometric quantities**

Syed Tahir Amin

Supervisor: Doctor Vítor João Rocha Vieira

Co-Supervisor: Doctor Nikola Paunković

**Thesis approved in public session to obtain the PhD Degree in
Physics**

Jury final classification: Pass with Distinction

Jury

**Chairperson: Doctor José Luís Rodrigues Jólíio Martins, Instituto Superior Técnico,
Universidade de Lisboa**

Members of the Committee:

**Doctor Vítor João Rocha Vieira, Instituto Superior Técnico, Universidade de
Lisboa**

**Doctor Miguel António da Nova Araújo, Escola de Ciências e Tecnologia, da
Universidade de Évora**

**Doctor Eduardo Filipe Vieira de Castro, Faculdade de Ciências, da Universidade
do Porto**

**Doctor Pedro José Gonçalves Ribeiro, Instituto Superior Técnico, Universidade
de Lisboa**

Funding Institutions

FCT - Fundação para a Ciência e Tecnologia

2020

PhD Thesis

Practical quantum privacy protocols

Preeti Yadav — 2020

Key information

Authors:

Preeti Yadav ([Preeti Yadav](#))

Supervisors:

Paulo Alexandre Carreira Mateus ([Paulo Alexandre Carreira Mateus](#)); [Nikola Paunković](#) ([Nikola Paunkovic](#)); André Nuno Carvalho Souto ([André Nuno Carvalho Souto](#))

Published in

11/06/2020

Abstract

Quantum technology has undoubtedly changed the course of information processing. Its most prominent application, quantum key distribution, enables two users to share perfectly secure keys, by requiring them to be capable of performing quantum operations. A natural question arises towards reducing users' technological requirements. In the first part of this thesis, we demonstrate a novel semi-quantum key distribution scheme with classical users. The quantum operations are delegated to an untrusted third party providing the users access to a superimposed single photon, and the key exchange is achieved via interaction-free measurements on the shared state. Unlike key distribution, where mutually trusting users work together against a common eavesdropper, there are some schemes where users do not trust each other. In the scenario of distrustful cryptography, we dedicate the second part of this thesis to commitmentbased protocols. Secure multiparty computation between distrusting users can be implemented using a commitment scheme as a primitive. Its



exchanging qubits and performing hash-functions based commitments, to achieve high-speed secure oblivious transfer, paving path for the expansion of applications based on secure multiparty computation. The no-go theorems on the impossibility of secure bit commitment motivated several proposals for bit commitment protocols secure under certain assumptions, like a trusted party, computational hardness, or noisy memories. We investigate the minimal assumptions required to obtain a universally composable bit commitment protocol by proposing a scheme with a trusted third party broadcasting quantum and classical resources to the users. It is known to be impossible to achieve fair contract signing without a trusted third party (Trent). We present a fair and optimistic contract signing protocol using entanglement, where after initialising the contract, Trent is only contacted in case of communication disruption, to verify clients' honesty and deliver signed certificates. A single client can obtain the signed contract alone, without needing the other client's presence. When first contacting Trent, clients need not have agreed upon a definitive contract and moreover, never reveal the actual contract to Trent. Finally, the protocol is abuse-free as it does not require exchanging large number of signed authenticated messages during the actual contract signing process, hence, the clients cannot misuse those signed messages.

A tecnologia quântica mudou inquestionavelmente o rumo do processamento de informações. A sua aplicação mais proeminente, a distribuição quântica de chaves, permite que duas partilhem chaves perfeitamente seguras, exigindo apenas que as partes sejam capazes de executar operações quânticas. A questão natural surge se indagar da possibilidade de se reduzir os requisitos tecnológicos dos intervenientes. Na primeira parte desta tese, apresentamos um novo esquema de distribuição de chaves semi-quântico em que as partes são clássicas. As operações quânticas são delegadas a terceiros em que não confiam, distribuindo pelos utilizadores um único fóton em sobreposição, e a troca de chaves é conseguida por meio de medições sem interação no estado partilhado. Ao contrário do processo de distribuição de chaves, no qual os dois participantes confiam um no outro e trabalham em conjunto contra intrusos, existem esquemas criptográficos em que os participantes não confiam um no outro. Num cenário, dedicamos a segunda parte desta tese a protocolos baseados em esquemas de compromisso. A computação multi-participante segura entre partes que não confiam mutuamente um no outro, pode ser implementada usando esquemas de compromisso de bits como primitiva. A sua implementação está condicionada pela segurança e eficiência da implementação de protocolos de transferência oblívios clássicos. Apresentamos um esquema híbrido para partilha de chaves oblívios de força eficiente e segura através da troca de qubits e utilizando esquemas de compromisso baseados em funções de hash, para criar transferências oblívios segura e de alta velocidade, abrindo caminho para a expansão de aplicações baseadas em computação multi-participante segura. Os teoremas que afirmam a impossibilidade de um esquema de compromisso de bits seguros motivaram várias propostas de protocolos de compromisso de bit seguros sob certas



necessárias para obter um protocolo de compromisso de bits ser universalmente componível, propondo um esquema com uma terceira entidade quântica confiável parte que transmita recursos quânticos e clássicos para os utilizadores. Sabe-se que é impossível desenvolver um esquema de assinaturas de contrato justa sem a intervenção de uma terceira parte em que os utilizadores não confiam (Trent). Apresentamos um protocolo para assinatura de contrato que é optimista e justo usando o entrelaçamento, em que após a inicialização do contrato, Trent é contactado apenas em caso de interrupção da comunicação, para verificar a honestidade dos clientes e entregar certificados assinados. Um único cliente pode obter o contrato assinado por si só, sem precisar da presença do outro cliente. Além disso, ao entrar em contato com Trent pela primeira vez, os clientes não precisam de ter acordado os termos do contrato definitivo e, nunca revelam o conteúdo do contrato a Trent. Por último, o protocolo é livre de abuso, pois não requer a troca de um grande número de mensagens autenticadas assinadas durante o processo efectivo de assinatura do contrato, portanto, os clientes não podem usar indevidamente essas mensagens assinadas.

Publication details

Authors in the IST community:



Preeti Yadav
ist426119

Supervisors of this institution:



Paulo Alexandre Carreira Mateus
ist13783



Nikola Paunkovic
ist32694



André Nuno Carvalho Souto
ist90766

RENATES TID

101494530

Degree Name



Fields of Science and Technology (FOS)

computer-and-information-sciences - **Computer and information sciences**

Keywords

CRIOGRAFIA QUÂNTICA

COMUNICAÇÃO QUÂNTICA

DISTRIBUIÇÃO DE CHAVES

COMPROMISSO DE BITS

TRANSFERÊNCIA OBLÍVIA

QUANTUM CRYPTOGRAPHY

QUANTUM COMMUNICATION

KEY DISTRIBUTION

BIT COMMITMENT

OBLIVIOUS TRANSFER

Publication language (ISO code)

eng - English

Rights type:

Embargo lifted

Date available:

09/14/2021

Institution name

Instituto Superior Técnico

Financing entity

Fundação para a Ciência e a Tecnologia

Download files

[Preeti_thesis.pdf](#) (7.04 MB)

AVAILABLE

UNIVERSIDADE DE LISBOA
INSTITUTO SUPERIOR TÉCNICO

Practical quantum privacy protocols

Preeti Yadav

Supervisor: Doctor Paulo Alexandre Carreira Mateus

Co-Supervisors: Doctor Nikola Paunković

Doctor André Nuno Carvalho Souto

Thesis approved in public session to obtain the PhD Degree in
Information Security

Jury final classification: Pass with Distinction

Jury

Chairperson: Doctor Rui Jorge Morais Tomaz Valadas, Instituto Superior Técnico, Universidade de Lisboa.

Members of the Committee:

Doctor Paulo Alexandre Carreira Mateus, Instituto Superior Técnico, Universidade de Lisboa.

Doctor Ernesto Fagundes Galvão, International Iberian Nanotechnology Laboratory, Braga.

Doctor Vladimir Bozin, Faculty of Mathematics, University of Belgrade, Serbia.

Doctor João Filipe Quintas dos Santos Rasga, Instituto Superior Técnico, Universidade de Lisboa.

Doctor Andreas Miroslaus Wichert, Instituto Superior Técnico, Universidade de Lisboa.

Funding Institution: Fundação para a Ciência e a Tecnologia (FCT)

PhD Thesis

Asymmetric quantum cryptography and multipartite correlations

Mariano José Lemus Hernández — 2022

Key information

Authors:

Mariano José Lemus Hernández ([Mariano José Lemus Hernández](#))

Supervisors:

Paulo Alexandre Carreira Mateus ([Paulo Alexandre Carreira Mateus](#)); [Nikola Paunković](#) ([Nikola Paunković](#))

Published in

03/16/2022

Abstract

Esta tese trata da análise de esquemas criptográficos multipartidos seguras, e do estudo da principal fonte de protocolos de processamento de informação, as correlações totais, clássicas e quânticas multipartidas, e as suas complexidades. Motivados pela utilidade da computação multipartida segura como uma ferramenta de protecção de privacidade, e identificando o seu custo de transferência oblívia como o seu maior desafio de implementação, propomos uma realização prática de transferência oblívia quântica. A nossa solução procura resolver as limitações na segurança e eficiência que os esquemas clássicos de transferência oblívia sofrem. São apresentados resultados preliminares de performance no contexto de uma experiência realizada envolvendo uma fonte de fótons entrelaçados em que a codificação é feita através da polarização. Os resultados de impossibilidade em atingir



dentro de certas hipóteses. Tais abordagens incluem parceiro de confiança, hardness computacional, e memórias com ruído e de armazenamento limitado. É apresentado um protocolo universalmente componível de compromisso de bits, em que é assumida a hipótese minimal de que é feita partilha segura, sem interações, de recursos clássicos e quânticos por um parceiro alheio aos participantes. Com base em trabalhos anteriores para uma hierarquia de correlação para distribuições de probabilidade, formalizamos uma teoria de estruturas de correlação para sistemas quânticos. Exploramos algumas das suas propriedades matemáticas, complexidade computacional, uso para compressão de informações de estados quânticos e alguns aspetos da categorização de correlações pela forma como são distribuídas, bem como pela sua natureza (clássica/quântica). Além disso, apresentamos uma aplicação prática para o framework de estruturas de correlação para a classificação cega de conjuntos de dados de série temporal. Apresentamos um método baseado no corte seletivo de correlações que não estão diretamente conectadas à variável de classe até que um critério de otimalidade seja satisfeito. O algoritmo foi capaz de adivinhar com sucesso a classe de dados de teste de fontes reais usando apenas alguns passos de tempo iniciais. A sua versatilidade para aplicação em outros problemas é destacada.

The subject of this thesis is the analysis of secure asymmetric cryptographic schemes, and the study of the main resource for information processing protocols, the total, classical and quantum multipartite correlations. Motivated by the usefulness of secure multiparty computation as a privacy-protecting data analysis tool, we propose a practical quantum realization of randomized oblivious transfer. Our solution is aimed at targeting the limitations of security and efficiency faced by the classical schemes for oblivious transfer. A detailed security proof is presented for the protocol. We also provide preliminary results of performance from an experimental setup based on an entangled photons source and polarization encoding. The impossibility results for achieving unconditionally secure bit commitment have driven the research for secure solutions under several different assumptions. We propose a criteria for ranking the complexity of such assumptions, together with new functionality, called the asymmetric quantum beamer, which is minimal under a listed criteria. Using this new assumption we develop a universally composable bit commitment protocol with linear complexity in its security parameter. Based on previous work for a correlation hierarchy for probability distributions, we formalize a framework of correlation structures for quantum systems. We explore some of its mathematical properties, computational complexity, use for information compression of quantum states, and some aspects of categorization of correlations by the way they are distributed as well as by their nature (classical/quantum). Additionally, we present a practical application for the correlation structures framework for early classification of time series data sets. The proposed method is based on selectively cutting correlations that are not directly connected to the class variable until a criterion of optimality is satisfied. The algorithm was able to successfully guess the class of test data from real world sources using only a few initial time



Authors in the IST community:



Mariano José Lemus Hernández

ist427022

Supervisors of this institution:



Paulo Alexandre Carreira

Mateus

ist13783



Nikola Paunkovic

ist32694

RENATES TID

101503970

Degree Name

Doutoramento em Física

Fields of Science and Technology (FOS)

physical-sciences - Physical sciences

Keywords

QUANTUM CRYPTOGRAPHY

OBLIVIOUS TRANSFER

BIT COMMITMENT

QUANTUM MULTIPARTITE CORRELATIONS

QUANTUM KOLMOGOROV COMPLEXITY

CRIOGRAFIA QUÂNTICA

TRANSFERÊNCIA OBLÍVIA

COMPROMISSO DE BITS

CORRELAÇÕES QUÂNTICAS MULTI-PARTIDAS

COMPLEXIDADE DE KOLMOGOROV QUÂNTICA



eng - English

Rights type:

Open access

Institution name

Instituto Superior Técnico

Financing entity

Download files
Decreto-Lei nº 113/2017 da Ciência e a Tecnologia

[Mariano Lemus Thesis PhD.pdf](#) (2.38 MB)

AVAILABLE

Cite publication

Powered by FenixEdu™

User manual

CO-FINANCED BY:

Support materials

Support

Open Access Policy



FAQ

2022-2025 © Instituto Superior Técnico

UNIVERSIDADE DE LISBOA
INSTITUTO SUPERIOR TÉCNICO

**Asymmetric Quantum Cryptography and
Multipartite Correlations**

Mariano José Lemus Hernández

Supervisor: Doctor Paulo Alexandre Carreira Mateus

Co-Supervisor: Doctor Nikola Paunković

Thesis approved in public session to obtain the PhD Degree in
Physics

Jury final classification: Pass with Distinction

Jury

Chairperson: Doctor José Luís Rodrigues Júlio Martins, Instituto Superior Técnico, Universidade de Lisboa.

Members of the Committee:

Doctor Vítor João Rocha Vieira, Instituto Superior Técnico, Universidade de Lisboa.

Doctor Paulo Alexandre Carreira Mateus, Instituto Superior Técnico, Universidade de Lisboa.

Doctor Ämin Baumeler, Institute for Quantum Optics and Quantum Information
Vienna, Austrian Academy of Sciences, Austria.

Doctor Walter O. Krawec, University of Connecticut, USA.

Funding Institution: Fundação para a Ciência e a Tecnologia (FCT)

PhD Thesis

Nonlocality and contextuality: concepts and applications in quantum information

Ricardo André Faleiro Miguel — 2022

Key information

Authors:

Ricardo André Faleiro Miguel ([Ricardo André Faleiro Miguel](#))

Supervisors:

Paulo Alexandre Carreira Mateus ([Paulo Alexandre Carreira Mateus](#)); [Nikola Paunkovic \(Nikola Paunkovic\)](#)

Published in

03/04/2022

Abstract

Nas áreas da informação quântica e fundamentos da mecânica quântica, perceber o conceito de não-classicalidade é de extrema importância. O termo caracteriza, de grosso modo, qualquer fenómeno quântico que não só aparenta estar em confronto com uma certa noção de intuição clássica, mas que está provadamente em contradição com as previsões empíricas dessas mesmas teorias. Os exemplos típicos são a não-localidade e a contextualidade, que foram originalmente caracterizados através de uma abordagem baseada em resultados de impossibilidade conhecidos como os resultados no-go. A não-localidade e a contextualidade, se bem que conceitos cruciais a considerar nas questões da estranheza e das dificuldades conceptuais da mecânica quântica, também se apresentam como recursos de informação úteis, cujo potencial pode ser aproveitado para efeitos de



particular na não-localidade e na contextualidade, estudando-as através da perspectiva de jogos cooperativos, que oferece uma interpretação intuitiva dos resultados no-go como protocolos interactivos entre vários agentes que tentam computar uma determinada função, contrangidos por um conjunto de restrições operacionais. Neste quadro, a não-classicalidade inerente ao jogo manifesta-se como um recurso que potencia a chamada vantagem quântica-sobre-clássica. Este termo descreve sucintamente que jogadores com acesso ao leque completo das estratégias fornecidas pela receita quântica operacional irão ter uma melhor prestação no jogo que jogadores restritos às teorias clássicas alternativas. Finalmente, algumas aplicações na informação quântica são discutidas, nomeadamente em criptografia quântica, em que diversos tipos de fenómenos não-clássicos se apresentam como tendo uma importância crucial para garantir segurança em vários protocolos.

In quantum foundations and quantum information, understanding the notion of non-classicality is of extreme importance. This term broadly characterizes quantum phenomena which not only appear to be at odds with certain instances of classical intuition, but are provably in contradiction with empirical predictions of classical theories. The archetypal examples of nonclassical phenomena, produced by operational quantum mechanics, are nonlocality and contextuality, which have traditionally been characterized within a framework of impossibility results, known as no-go results. Nonlocality and contextuality, while being at the core of the weirdness and conceptual issues of quantum theory, also provide useful information theoretical resources that can be harnessed for information processing purposes, for instance, in quantum computation and quantum cryptography. In this thesis, we detail various types of non-classical phenomena, in particular nonlocality and contextuality, by studying them within the framework of cooperation multiplayer games. This framework provides an intuitive way to interpret such no-go results as interactive protocols where agents try to jointly compute a desired function under a set of operational restrictions. Therein, the non-classical behavior particular to the setup emerges as a resource for appropriately constructed games, powering the so called quantum-over-classical advantage — a term which succinctly describes that players exploiting the full range of operational quantum strategies perform better at the game than the players restricted to the alternative classical theories. Finally, we will discuss some applications in quantum information, namely, within quantum cryptography, where different types of non-classical behaviour are of crucial importance in order to guarantee security of various protocols.

Publication details

Authors in the IST community:



SCHOLAR

Ricardo André Faleiro Miguel

ist188512

**Supervisors of this institution:**

**Paulo Alexandre Carreira
Mateus**
ist13783



Nikola Paunkovic
ist32694

RENATES TID

101697481

Degree Name

Doutoramento em Física

Fields of Science and Technology (FOS)

physical-sciences - Physical sciences

Keywords

NON-CLASSICALITY

NONLOCALITY

CONTEXTUALITY

COOPERATION GAMES

QUANTUM-OVER-CLASSICAL ADVANTAGE

NÃO-CLASSICALIDADE

NÃO-LOCALIDADE

CONTEXTUALIDADE; JOGOS COOPERATIVOS

VANTAGEM QUÂNTICA-SOBRE-CLÁSSICA

Publication language (ISO code)

eng - English

Rights type:

Open access

Institution name



Financing entity

Fundação para a Ciência e a Tecnologia

Download files

[R.Faleiro - PhD Thesis.pdf](#) (1.15 MB)

AVAILABLE

Cite publication

Powered by FenixEdu™

[User manual](#)

CO-FINANCED BY:

[Support materials](#)

[Support](#)

[Open Access Policy](#)



[FAQ](#)

2022-2025 © Instituto Superior Técnico



**UNIVERSIDADE DE LISBOA
INSTITUTO SUPERIOR TÉCNICO**

Nonlocality and Contextuality:
Concepts and Applications in Quantum Information

Ricardo André Faleiro Miguel

Supervisor: Doctor Paulo Alexandre Carreira Mateus

Co-Supervisor: Doctor Nikola Paunković

Thesis approved in public session to obtain the PhD Degree in
Physics

Jury final classification: Pass with Distinction

Jury

Chairperson: Doctor José Luis Rodrigues Júlio Martins, Instituto
Superior Técnico, Universidade de Lisboa;

Members of the Committee:

Doctor Ernesto Fagundes Galvão, International Iberian Nanotechnology
Laboratory (INL), Braga;

Doctor Borivoje Dakić, Faculty of Physics, University of Vienna, Austria;

Doctor Pedro José Gonçalves Ribeiro, Instituto Superior Técnico,
Universidade de Lisboa;

Doctor Hugo Fernando Santos Terças, Instituto Superior Técnico,
Universidade de Lisboa;

Doctor Nikola Paunković, Instituto de Telecomunicações, IT-Lisboa;

Doctor Chrysoula Vlachou, Instituto de Telecomunicações, IT-Lisboa;

Funding Institution - Fundação para a Ciência e Tecnologia