Slovenská národná výskumná platforma kvantových technológií

AKČNÝ PLÁN PLATFORMY

Mário Ziman, Miroslav Grajcar, Tomáš Samuely, Martin Gmitra

2018

Cieľom Slovenskej národnej výskumnej platformy v kvantových technológiách (**platformy QUTE**) je vytvoriť podmienky pre zvýšenie konkurencieschopnosti a excelentnosti Slovenska vo výskume a inováciách v oblasti kvantových technológií, ktoré budú hrať kľúčovú úlohu v budúcich priemyselných a bezpečnostných aplikáciách. Akčný plán vypracováva detaily ako iniciovať a podporovať ich rozvoj na Slovensku, a v súčinnosti výskumných tímov platformy dosiahnuť dlhodobú udržateľnosť výskumu a vývoja v tejto oblasti.

Kľúčovými aktivitami Platformy QUTE sú:

- vytvorenie vzdelávacieho študijného programu a založenie medzinárodného **vzdelávacieho centra eduQUTE**, ktoré má ambíciu stať sa medzinárodným školiacim strediskom európskeho významu
- vytvorenie virtuálneho **inštitútu kvantových technológií iQUTE**, ktorý bude združovať jednotlivé výskumné tímy pracujúce na výskumných zámeroch kvantovej iniciatívy
- v spolupráci so zahraničnými partnermi vybudovanie **kvantovej komunikačnej siete QUAPITAL** spájajúcej stredoeurópske hlavné mestá

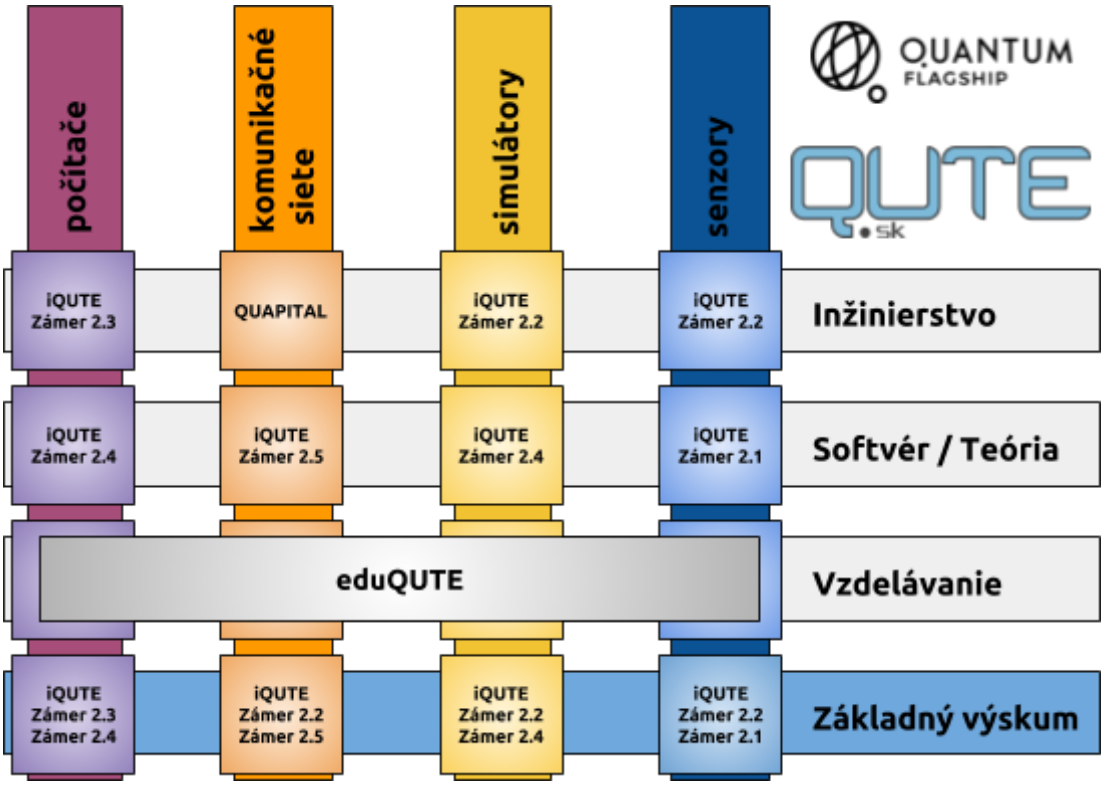
Iba **excelentný** výskum má schopnosť konkurovať v medzinárodných projektových výzvach. Akčný plán pomôže zapojiť jednotlivé výskumné tímy do excelentných medzinárodných konzorcií, ktoré následne prinesú nové možnosti a v neposlednom rade aj finančné zdroje pre ďalší výskum. Okrem zapájania sa do medzinárodných projektových programov platforma QUTE zintenzívni už existujúcu komunikáciu aj s relevantnými priemyselnými partnermi ako sú IBM, Dell, Slovak Telekom, Eset, a iné.

Akčný plán pre Slovensko **je ideovo v súlade s európskou iniciatívou** Quantum Technologies Flagship (QT Flagship, http://qt.eu/), ktorá má štyri strategické technologické ciele: **kvantový počítač, kvantová komunikačná sieť, kvantové senzory a metrológia a kvantový simulátor**, všetky vychádzajúce zo základného výskumu. Dôležitou súčasťou stratégie sú aktivity vytvárajúce nástroje pre dosiahnutie strategických cieľov. Zameriavajú sa na rozvoj **kvantového inžinierstva** (materiálov a kontroly)**, kvantového softvéru** (teórie), a **systému vzdelávania** novej generácie kvantových fyzikov a inžinierov schopných prenášať výsledky výskumu do priemyselnej praxe.

V ďalších častiach tento akčný plán popisuje konkrétne aktivity a výskumné zámery platformy QUTE, odhadovaný rozpočet, ktorý umožní tieto ciele naplniť v nasledujúcich piatich rokoch, štruktúru platformy QUTE a jednotlivé výskumné tímy.

Platforma QUTE združuje sedem inštitúcií:

- Fyzikálny ústav SAV (FÚ SAV),
- Elektrotechnický ústav SAV (ELÚ SAV),
- Matematický ústav SAV (MÚ SAV),
- Ústav experimentálnej fyziky SAV (ÚEF SAV),
- Fakulta matematiky, fyziky a informatiky UK (FMFI UK),
- Prírodovedecká fakulta UPJŠ (PF UPJŠ),
- Fakulta elektrotechniky a informatiky STU (FEI STU).



Jednotlivé zámery (popísané v ďalšej časti) vychádzajú z celoeurópskej stratégie kvantového flagshipu (viď obrázok) a prispievajú k dosiahnutiu jeho cieľov. Dosiahnutie cieľov tohto akčného plánu spočíva na dvoch pilieroch: zabezpečení personálneho obsadenia a posilnení experimentálneho vybavenia na už existujúcich pracoviskách. Predpokladané náklady pre platformu QUTE na obdobie 5 rokov sú vo výške 8,725 milióna EUR. Vďaka tejto podpore bude možné uskutočniť aktivity akčného plánu a etablovať slovenský výskum a školu v medzinárodnom kontexte. Najdôležitejším dlhodobým výsledkom bude príprava konkurencieschopných ľudských zdrojov, ktoré majú potenciál budovať moderný a inovatívny priemysel.

Finančná podpora nám umožní

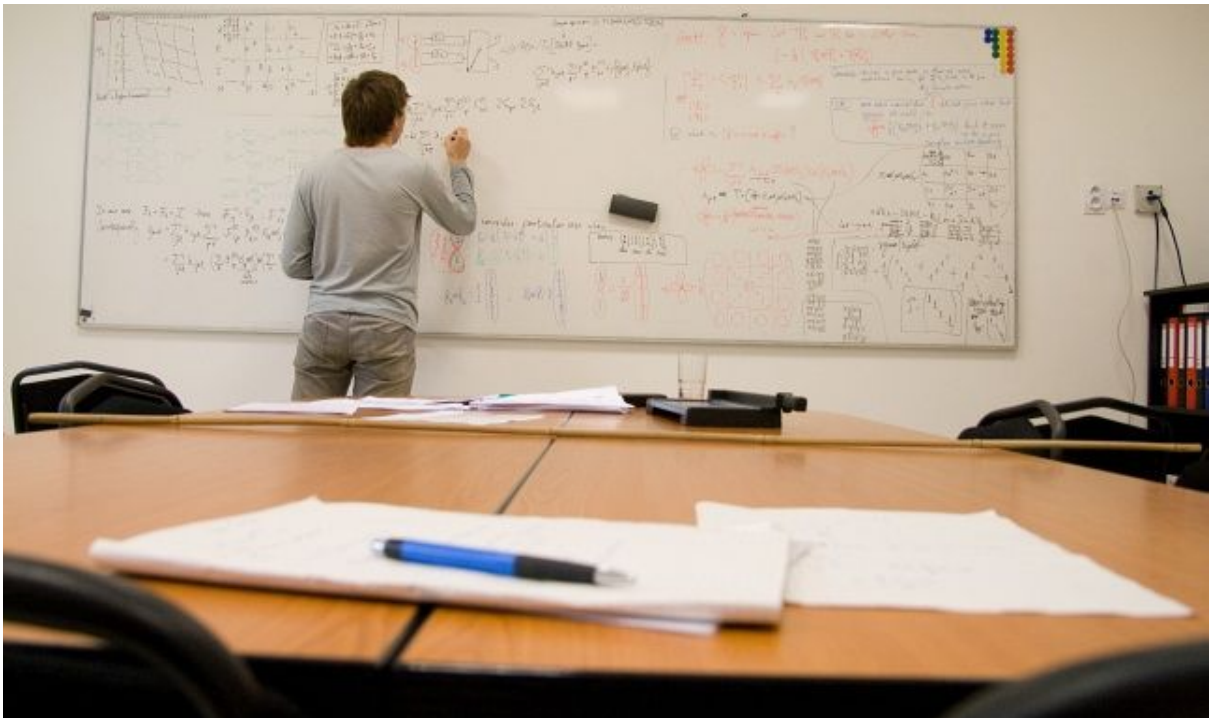
- vytvoriť medzinárodne etablované vzdelávacie centrum v oblasti kvantových technológií
- udržať na Slovensku kvalitných študentov a mladých vedeckých pracovníkov
- pritiahnuť na Slovensko nových kvalitných vedeckých pracovníkov
- významne prispieť k vývoju kvantových inovácií a technológií
- zvýšiť úspešnosť v medzinárodných projektových výzvach a strategických konzorciách
- vytvoriť vedecko-výskumné zázemie a infraštruktúru pre vznikajúci kvantový priemysel

PLÁNOVANÉ AKTIVITY

1. AKTIVITA eduQUTE: ŠKOLA KVANTOVÝCH TECHNOLÓGIÍ

Cieľ: Vytvorenie národného vzdelávacieho centra eduQUTE

Slovensko v posledných rokoch čelí “úniku mozgov”, ktorý zasahuje všetky stupne vysokoškolského štúdia. Jedným z dôvodov je aj zmenšujúca sa atraktivita slovenského výskumného priestoru, najmä jeho finančná nestabilita, malá flexibilita a neexistencia dodatočných zdrojov financovania, a nízka mzdová konkurencieschopnosť (aj v porovnaní so štátmi V4). V podpore prichádzajúcej revolúcie v oblasti kvantových informačných technológií vidíme možnosť vytvorenia pilotného programu podpory vedy a výskumu, ktorý má vďaka existujúcej expertíze potenciál tento nepriaznivý vývoj zvrátiť. Chceme vytvoriť moderný edukačný a výskumný program so stabilizovaným finančným modelom, ktorý bude atraktívny pre kvalitných uchádzačov aj v medzinárodnom meradle.



Zámer 1.1 Vytvorenie systému vzdelávania v oblasti kvantových technológií (od bakalárskeho po postdoktorandský stupeň)

(koordinátor: Gabriel Semanišin)

Partneri: FMFI UK, FEI STU, UPJŠ, FÚ SAV, ÚEF SAV, MÚ SAV, ELÚ SAV,
Zodpovední riešitelia: Miroslav Grajcar, Pavol Zajac, Gabriel Semanišin

Popis zámeru:
Kvantové technológie sú prienikom inžinierskych, fyzikálnych, matematických a informatických odborov. Vytvorenie takéhoto vzdelávacieho programu preto ide výrazne nad rámec fakúlt ba dokonca nad rámec možností jednotlivých vysokých škôl. Národná platforma QUTE zabezpečí spoluprácu Slovenskej technickej univerzity, Univerzity Komenského, Univerzity P.J. Šafárika ako aj relevantných ústavov SAV na vypracovaní medziodborového štúdia kvantových technológií. Vytvoríme systém udeľovania štipendií s cieľom motivovať študentov, aby si vybrali študijný odbor kvantových technológií.

Ciele:
C 1.1.1 Vytvorenie programu magisterského/inžinierskeho/doktorandského štúdia
Plánujeme, že v septembri 2021 budú v pripravenom programe prví študenti. Propagácia výskumného a študijného smeru na vytipovaných stredných a vysokých školách začne v priebehu roka 2019.

C 1.1.2 Vytvorenie systému štipendií
Vďaka podpore formou odborových motivačných štipendií predpokladáme zvýšenie atraktivity študijného programu kvantových technológií, čo by malo zabezpečiť kvalitných študentov na druhom a treťom stupni štúdia v tejto oblasti. Kým nebude schválený nový program, tak o toto štipendium sa budú môcť uchádzať študenti z výskumných tímov z platformy. Plánujeme 300 eur/mesačne pre druhý stupeň a plus 400 eur/mesačne (600 eur/mesačne) k základnému doktorandskému štipendiu (po dizertačnej skúške).

Zámer 1.2 Vytvorenie doktorandskej školy a Flagship tréningového centra

(koordinátor: Vladimír Bužek)

Partneri: FMFI UK, FEI STU, UPJŠ, FÚ SAV, ÚEF SAV, MÚ SAV, ELÚ SAV,
Zodpovední riešitelia: Vladimír Bužek, Mário Ziman, Miroslav Grajcar, Tomáš Samuely, Martin Gmitra

Popis zámeru:
Doktorandi partnerov platformy budú tvoriť doktorandskú školu, v rámci ktorej sa bude uskutočňovať vzdelávanie formou letných škôl, ktoré budú otvorené pre zahraničných účastníkov, a na ktorých budú prednášať prevažne zahraniční lektori. Súčasťou bude aj plná finančná podpora štvormesačnej stáže (pre domácich doktorandov) na zahraničnom pracovisku. V rámci edu-QUTE sa touto aktivitou pokúsime o vytvorenie európskeho vzdelávacieho centra v oblasti kvantových technológií, ktoré by zabezpečovalo teoretické vzdelávanie pre celý Quantum Flagship a bolo by spolufinancované z európskych zdrojov. Už dnes existujú podmienky pre to, aby takéto vzdelávacie centrum vzniklo na báze Centra pre výskum kvantovej informácie, vedeckého pracoviska FÚ SAV, ktoré má skúsenosti s organizáciou vedeckých podujatí, vrátane letných a zimných škôl. Cieľom vzniku takéhoto centra je kvalitatívny posun v úrovni vzdelávania slovenských študentov. Prednášky popredných európskych odborníkov v danej oblasti budú neoceniteľné pre študentov platformy a zároveň zviditeľnia slovenskú vedu a samotné Slovensko.

Ciele:
C 1.2.1 Spoločné magisterské/inžinierske a doktorandské kurzy
Vyučovanie formou krátkodobých intenzívnych kurzov všeobecnejších predmetov o kvantových technológiách optimalizuje výdavky na vzdelávanie. Združením študentov z viacerých inštitúcií sa dosiahne kritické množstvo nevyhnutné pre zmysluplnosť kurzu. Kurzy budú spočiatku organizované prezenčne, ale plánujeme postupný prechod na online kurzy.

C 1.2.2 Letné školy eduQUTE
Letné doktorandské školy budú zamerané na špecifické kurzy z aktuálnych oblastí kvantových technológií v rozsahu 6-10 h/kurz v počte 4-6 kurzov na letnú školu. Kurzy budú viesť prevažne zahraniční lektori. Školy budú otvorené aj zahraničným účastníkom. Trvanie škôl sa predpokladá 10-14 dní a súčasťou budú aj cvičenia a diskusie s prednášajúcim. Účastníci budú mať aktívnu prezentáciu vo forme posteru.

C 1.2.3 Zapojenie do edukačných aktivít Flagshipu QT
Vytvorené národné školiace stredisko na FÚ SAV sa aktívne zapojí do kvantového flagshipu s ambíciou stať sa vzdelávacím centrom pre Flagship, prinajmenšom pre krajiny strednej Európy. V rámci kreditového systému budú kurzy aj absolvované letné školy akceptované ako súčasť doktorandského programu v kvantových technológiách v celej Európe.

Zámer 1.3 Vytvorenie podpory postdoktorandov fellowQUTE

(koordinátor: Miroslav Grajcar)

Partneri: FMFI UK, FEI STU, UPJŠ, FÚ SAV, UEF SAV, MÚ SAV, EIÚ SAV,
Zodpovední riešitelia: Miroslav Grajcar, Mário Ziman, Tomáš Samuely, Martin Gmitra

Popis zámeru:
Na Slovensku prakticky neexistuje spôsob podpory postdoktorandských miest, napriek tomu, že práve postdoktorandi sú hlavnou výskumnou silou. Našim cieľom je vytvoriť systém, ktorý by umožnil otvorenie medzinárodne kompetetívnych postdoktorandských pozícií. Jednotlivé partnerské organizácie sa budú o tieto miesta uchádzať v otvorenej súťaži. Postdoktorandské pozície budú maximálne trojročné. Predpokladáme postupné vytvorenie minimálne 12 takýchto pozícií (bežiacich súčasne), ktoré budú pokrývať výskumné zámery iQUTE.

Ciele:

C 1.3.1 Kvalitní postdoktorandi fellowQUTE
Základné výberové kritériá, spôsob a formu výziev a tvorbu výberových komisií bude definovať výkonná rada platformy QUTE. Jej návrh bude schvaľovať Správna rada platformy QUTE.

C 1.3.2 QUTE workshops
Na týchto workshopoch sa okrem podporených postdoktorandov stretnú všetky skupiny platformy. Organizovať sa budú jedenkrát za rok. Na stretnutí budú prezentované dosiahnuté výsledky jednotlivých postdoktorandov a skupín a zhodnotí sa plnenie zámerov platformy. Okrem výskumu budú diskutované aj organizačné otázky a úlohy platformy. Tieto workshopy budú mať prevažne interný charakter, ale budú na nich pozvaní relevantní zahraniční špecialisti s cieľom obohatiť Platformu QUTE o novú expertízu a potenciálne nové výskumné úlohy.

C 1.3.3 Školenia postdoktorandov v soft-skills
V rámci workshopu QUTE bude zorganizované satelitné jednodňové školenie postdoktorandov a doktorandov v písaní projektov, v autorskom a patentovom práve, v zlepšení prezentačných schopností a spôsobu komunikácie výsledkov výskumu pre verejnosť, atď.

2. AKTIVITA iQUTE: INŠTITÚT KVANTOVÝCH TECHNOLÓGIÍ

Cieľ: Založenie virtuálneho inštitútu a udržateľnosť excelentného výskumu

Inštitút iQUTE pokrýva výskumné ciele platformy QUTE. Ide o virtuálnu štruktúru, ktorá organizačne sídli na FÚ SAV, a okrem **výskumných aktivít** vykonáva aj **expertnú a popularizačnú činnosť**. Je zložená z výskumných tímov jednotlivých inštitúcií platformy QUTE. Vedúci tímov tvoria Radu iQUTE, na čele ktorej stojí koordinátor QUTE.

Teoretický výskum iQUTE je zameraný na základný výskum kvalitatívne nových kvantovo-informatických štruktúr, certifikáciu a optimalizáciu kvantových technológií, vývoj efektívnych algoritmov na simulácie kvantových systémov, analýzu výpočtovej zložitosti fyzikálnych systémov, návrhy bezpečných komunikačných protokolov. Kľúčové strategické ciele platformy QUTE sú zamerané na teoretické modelovanie a experimentálny vývoj kvantového hardvéru v supravodičových a polovodičových systémoch, na realizáciu kvantovej pamäte a kvantového “repeatera” a ďalších technológií, pre globálnu kvantovú sieť (quantum internet). V oblasti kvantových počítačov a simulátorov budú výskumné tímy iQUTE skúmať niekoľko možností implementácie kvantových bitov - elementárnych prvkov kvantových technológií.

Zoznam výskumných tímov:

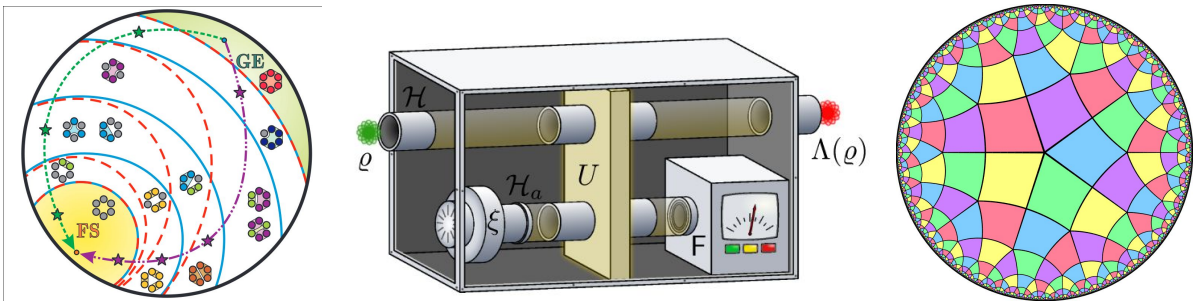
- G1 Skupina kvantových informačných štruktúr a sietí (M. Ziman)
- G2 Skupina kvantových simulácií a algoritmických metód (A. Gendiar)
- G3 Laboratórium kvantových meraní (M. Grajcar)
- G4 Laboratórium kvantového magnetizmu (E. Čižmár)
- G5 Laboratórium fyziky nízkych teplôt (P. Skyba)
- G6 Laboratórium topologicky-chránených kvantových bitov (T. Samuely)
- G7 Laboratórium post-kvantovej kryptografie (P. Zajac)
- G8 Skupina kvantového počítania a algoritmov (M. Gmitra)

Zámer 2.1 Kvantové informačné štruktúry a metrológia

(koordinátor: Anna Jenčová)

Partneri: FÚ SAV, MÚ SAV
Zodpovední riešitelia: Mário Ziman, Anna Jenčová, Michal Sedlák, Vladimír Bužek, Daniel Reitzner, Peter Rapčan

Popis zámeru:
Výskum v oblasti kvantovo-informatických štruktúr definuje základný teoretický rámec pre kvantové technológie, t.j. vytvára koncepty a metódy, ktoré nám umožňujú kvantové technológie vôbec definovať, určiť základné teoretické ako aj praktické ohraničenia ich funkcionality, a nakoniec aj certifikovať ich implementácie.



Fyzika kvantových systémov nás núti prehodnotiť mnohé z našich predstáv o fungovaní sveta. Nielenže štandardné fyzikálne veličiny nemôžu mať ľubovoľné hodnoty (sú kvantované), ale ani o nich nevieme hovoriť s určitosťou. Túto náhodnosť je treba prijať ako súčasť kvantového sveta. Kvantová teória informácie hľadá pridanú hodnotu práve v tejto kvantovej náhodnosti a snaží sa pomocou nej vylepšiť existujúce technológie.

Analýzou kvantových modelov je možné identifikovať a kvantifikovať tie ich kvantové vlastnosti, o ktorých hodnotách vieme hovoriť s určitosťou, avšak otázkou je ako tieto veličiny získavať (efektívne) z experimentálnych dát. Tieto kvantové veličiny úzko súvisia práve s rozvojom kvantových technológií, pretože kvantifikujú tie prejavy kvantového sveta, ktoré nám umožňujú posunúť hranice komunikačných a výpočtových technológií. Hovoríme, že tieto veličiny vytvárajú tzv. kvantovo-informatické štruktúry.

Našim konkrétnym zámerom bude preskúmať kvantovo-technologický potenciál kvantových štruktúr vyššieho rádu, v ktorých je informácia zakódovaná do transformácií kvantových systémov, s ktorými vieme experimentálne priamo pracovať. Tieto štruktúry nám umožňujú vytvárať hypotetické interferencie medzi kauzálnymi poradiami, o ktorých sa podarilo ukázať, že zvyšuje efektivitu výpočtov oproti kvantovému počítaniu (prvého rádu). Ich zrealizovaná experimentálna demonštrácia je ešte stále predmetom diskusie, ale ukazujú sa ďalšie kvalitatívne nové vlastnosti takéhoto spracovania informácie.

Overenie a porovnanie kvality funkcionality kvantových zariadení je dôležitou súčasťou kvantových technológií. Súčasná kvantová metrológia sa prevažne venuje vylepšeniu metrologických postupov a presností pri meraní klasických fyzikálnych parametrov systémov, t.j. fyzikálnych jednotiek. Našim cieľom bude identifikovať a štandardizovať univerzálne postupy pre efektívnu charakterizáciu kvantových vlastností systémov, resp. odmerať kvantovo-informačné jednotky ako napríklad nelokálnosť, nekompatibilitu, nemarkovovskosť, a iné. Inými slovami vytvoriť kvantové metrologické štandardy, špeciálne pre kvantové procesy a samotné merania. Dôležitou úlohou je certifikácia meracích prístrojov, ktorá je netriviálna v tom, že overenie správnej funkcionality meracieho prístroja vyžaduje úplnú znalosť meraného objektu (etalón). Avšak takúto znalosť

vieme z definície získať, až keď systém zmeriame certifikovanými meracími prístrojmi. Dôležitou otázkou (s dopadom na bezpečnostné aspekty kvantových technológií) je do akej miery môžeme, resp. musíme spraviť *ad hoc* predpoklady o vlastnostiach používaných prístrojov a systémov.

Hlavné výskumné ciele

C 2.1.1 Kvantové výpočty a komunikácia vyššieho rádu

V tomto výskumnom programe máme za cieľ analyzovať potenciálny prínos vyšších rádov pre kvantové výpočtové zrýchlenie. V prípade kvantovej bezpečnosti nás zaujíma, či sú kvantové protokoly odolné voči útokom pomocou vyšších štruktúr. Tento výskum otvára úplne novú oblasť spracovania informácie a má potenciál zrevidovať základy kvantových informačných technológií.

C 2.1.2 Metrologické štandardy pre kvantové procesy a merania

Vypracovanie štandardov predstavuje nástroj pre kvantový priemysel, ktorý bude schopný hodnotiť a certifikovať kvantové technológie. Ide o dlhodobý cieľ zahŕňajúci mnoho čiastkových výskumných úloh. Tieto sú zaujímavé ako z praktického aj z konceptuálneho pohľadu samotnej teórie, pretože dávajú abstraktným matematickým pojmom konkrétny význam.

C 2.1.3 Optimalizácia kvantových štruktúr a spracovania informácie

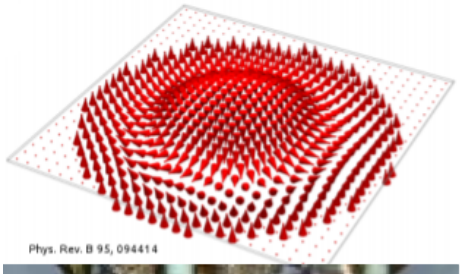
Systematický výskum existencie a optimálnych riešení pre jednotlivé úlohy kvantového spracovania informácie, ako napríklad protokoly pre optimálne klonovanie, programovateľné procesory a rozhodovacie protokoly, má priamy dopad na všetky kvantové technológie. Riešenie týchto modelových úloh je užitočné pre pochopenie možností, ktoré sú sa objavia pri riešení predošlých cieľov, a ich následné využitie v aplikáciách.

Zámer 2.2 Kvantové elektronické zariadenia pre kvantovú komunikáciu a počítanie

(koordinátor: Miroslav Grajcar)

Inštitúcie: FMFI UK, FÚ SAV, EIU SAV, UEF SAV

Zodpovední riešitelia: Miroslav Grajcar, Daniel Manca, Pavol Neilinger, Ján Greguš, Richard Hlubina, Peter Markoš, Peter Skyba, Peter Szabo, Peter Samuely, Vladimír Cambel



Popis zámeru:
Cieľom je konštrukcia špičkových elektronických zariadení s využitím kvantových technológii, na úrovni porovnateľnej s najvyspelejšmi európskymi výskumnými ústavmi. V súčasnosti už pracujeme na danej problematike v rámci APVV projektu QUTEMAD a snažíme sa zapojiť do projektov iniciatívy QT Flagship. V dokumente „Quantum Technologies Roadmap 2016“ sú supravodivé obvody priamo uvedené ako sľubná platforma pre kvantové zariadenia s optimálnymi vlastnosťami. Tieto zariadenia môžu pracovať až po tzv. kvantovú limitu. V projekte sa sústredíme na **realizáciu konkrétnych zariadení založených na supravodičoch**, alebo supravodivých obvodoch pracujúcich v blízkosti kvantovej limity. Jedným z hlavných cieľov projektu je realizácia funkčného parametrického zosilňovača signálu, ktorý by priniesol reálne zlepšenie v porovnaní so zosilňovačmi na báze HEMT - tranzistorov s vysokou elektrónovou mobilitou.

Súčasťou tohto zámeru je aj výskum v oblasti nových materiálov, keďže pokrok v kvantových technológiách je viazaný na pokrok v realizácii netradičných kvantových ako aj klasických materiálov. Jedným z príkladov takýchto sľubných materiálov sú topologické izolátory. Sú typické tým, že hoci vo vnútri sú nevodivé, na povrchu, respektíve na hranách sú vodivé. Tieto vodivé stavy sú pritom mimoriadne odolné (takmer nezničiteľné, hovorí sa tomu topologicky chránené), čo pre tieto materiály ponúka množstvo praktických aplikácií.

Našou ďalšou stratégiou je zamerať sa na oblasť kvantovej komunikácie. Budeme skúmať hybridné schémy spájajúce mikrovlnné a optické frekvencie. Cieľom je konštrukcia takzvaného kvantového opakovača “quantum repeater”, ako kľúčového prvku kvantovej komunikácie. Umožnil by bezpečný prenos údajov na veľké vzdialenosti cez už existujúce (a nezabezpečené) optické linky. Okrem opakovača takáto kvantová komunikačná infraštruktúra vyžaduje aj vysoko-účinné jednofotónové detektory. Medzi najúčinnejšie dnes patria detektory na báze neusporiadaných supravodičov WSi, NbN, MoC, MoRe s ktorými máme skúsenosti a sú predmetom nášho výskumu. Posledným komponentom na ktorý sa v tejto oblasti chceme zamerať sú takzvané N-V centrá v diamante. Tie by mohli byť použité na transformáciu kvantovej informácie zakódovanej v optickom fotóne do mikrovlnného fotónu, čo by umožňovalo použitie supravodivých kvantových bitov pri konštrukcii kvantových opakovačov.

Na Slovensku sú len dve laboratóriá, ktoré prevádzkujú zmiešavacie refrigerátory a majú skúsenosti s prácou pri ultra nízkych teplotách a teda sú spôsobilé pre kvantové merania, detekciu a simulácie na supravodivých kvantových systémoch. Obe sú súčasťou platformy QUTE. Laboratórium kvantových meraní (spoločné pracovisko FÚ SAV a FMFI UK) v Bratislave a Centrum fyziky nízkych teplôt (spoločné pracovisko ÚEF SAV a UPJŠ) v Košiciach budú spolupracovať na dosiahnutí stanovených výskumných cieľov. Pri konštrukcii mikrovlnných zosilňovačov pracujúcich vo vysokých frekvenciách sa takisto spoliehame na expertízu ELÚ SAV, ktorý má bohaté skúsenosti s vývojom prototypov HEMT tranzistorov využívajúcich nové materiály a technológie ich prípravy.

Hlavné výskumné ciele:

C2.2.1 Kvantovo-limitované zosilňovače pre kvantovú komunikáciu a počítanie

Cieľom je realizácia funkčného prototypu parametrického zosilňovača signálu dosahujúceho špičkové parametre: zosilnenie väčšie ako 10 dB, teplota šumu v blízkosti kvantovej alebo dokonca subkvantovej limity. Takýto parametrický zosilňovač je kľúčový pre účinné kvantové merania a otvára možnosť realizácie kvantovej spätnej väzby. Špičkové HEMT zosilňovače schladené pod 20 K majú zosilnenie >20 dB a teplotu šumu T_N~2 K v pásme 4-8 GHz. Zosilňovače pracujúce v kvantovej limite by mali byť schopné dosiahnuť teplotu šumu porovnateľnú s energiou kvantových fluktuácií $k_B T_N$~ω/2, teda menej ako 0.2 K. Ďalšie rádové zlepšenie sa dá dosiahnuť supravodivými mikrovlnnými parametrickými zosilňovačmi. Supravodivé obvody, ktorých výroba je vďaka elektrónovej litografii jednoduchá, sú atraktívnou bázou kvôli nízkym stratám, ktoré dovoľujú dosahovať kvantovú limitu šumu v GHz pásme. Špičkové parametre supravodivých parametrických zosilňovačov sú >10 dB a T_N~0.2K, čo postačuje na manipuláciu s kvantovými stavmi poľa mikrovlnových fotónov, ako aj na ich meranie. Ale spracovanie kvantovej informácie vyžaduje takú vysokú účinnosť, ktorú dokážu poskytnúť len zosilňovače pracujúce v tzv. subkvantovej limite s $k_B T_N << \omega/2$. Takéto mikrovlnné zosilňovače stále nie sú k dispozícii a ich dizajn a realizácia bude jedným z cieľov nášho projektu. Cesta, ako k nim dospieť, vedie buď cez zlepšenie štandardných materiálov používaných pri výrobe týchto zariadení, resp. v použití netradičných kvantových materiálov.

C2.2.2 Jednofotónové detektory v optickej a mikrovlnnej oblasti s účinnosťou nad 90%.

Budeme testovať rôzne systémy schopné detekovať jeden fotón ako sú kvantové bodky, supravodivé detektory na báze neusporiadaných supravodičov, supravodivé bolometre. V súčasnosti testujeme nový typ supravodivého detektora na báze neusporiadaných supravodičov.

C2.2.3 Prenos kvantovej informácie z optickej do mikrovlnnej oblasti a späť s cieľom konštrukcie kvantového opakovača.

Ide o najambicióznejší cieľ nakoľko takýto prenos s dostatočnou účinnosťou nebol doteraz realizovaný. V spolupráci s Leibnizovým inštitútom fotonických technológií (Jena, Nemecko) sa chceme pokúsiť o realizáciu takéhoto prenosu cez vysokofrekvenčnú oblasť v ktorej má zahraničný partner dlhoročné skúsenosti.

C2.2.4 Využitie skyrmiónov na uchovanie klasickej a kvantovej informácie.

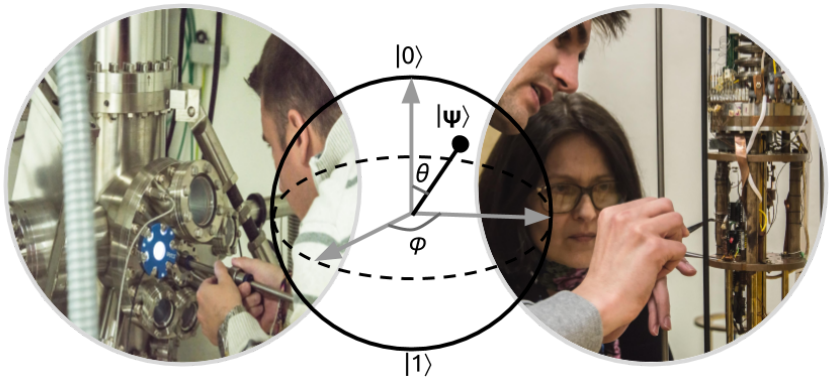
Veľmi progresívnym sa javí využitie skyrmiónov ako pamäťovej bunky schopnej uchovať kvantovú informáciu. ELÚ SAV pracuje na problematike skyrmiónov pre klasické počítače a v rámci tejto úlohy sa pokúsime ukázať, že je možné uchovať aj kvantovú informáciu pomocou skyrmiónu.

Zámer 2.3 Implementácie kvantových bitov

(koordinátor: Tomáš Samuely)

Inštitúcie: UPJŠ, FÚ SAV, EIU SAV, UEF SAV

Zodpovední riešitelia: Martin Gmitra, Jozef Strečka, Ondrej Hutník, Tomáš Samuely, Vladimír Komanický, Pavol Szabo, Peter Samuely, Jozef Kačmarčík, Zuzana Vargaeštoková, Erik Čižmár, Martin Orendáč, Alžbeta Orendáčová, Alexander Feher, Róbert Tarasenko, Vladimír Tkáč, Karol Flachbart, Slavomír Gabáni, Gabriel Pristáš, Peter Staňo



Popis zámeru:
O kvantovom počítači máme jasné teoretické predstavy. Nateraz nám však chýba vhodný kvantový hardvér pre **realizáciu kvantových bitov** (tiež *qubit*). Zložitosť jeho vývoja v reálnom prostredí si vyžaduje spoločné teoretické a experimentálne úsilie. Ukazuje sa, že najvhodnejšími kandidátmi na kvantové bity sú hybridné systémy na báze supravodičov alebo polovodičov. Kým supravodičové prototypy (pokrýva ich experimentálne aj zámer 2.2) sú v súčasnosti experimentálne lepšie zvládnuté, tie polovodičové majú blízko k už k existujúcemu počítačovému hardvéru.

Hlavná strategická výhoda polovodičových kvantových bitov je možnosť integrácie s kremíkovými čipmi a s existujúcim štandardným hardvérom. Už dlhšie je predmetom výskumu viacero ich variácií, no v poslednom období (2-3 roky) sa v tejto oblasti odohrali významné zmeny: viacerým výskumným skupinám sa podarilo zreprodukovať niekoľko kľúčových experimentov s prototypmi v kremíkových štruktúrach. To odštartovalo intenzívny vedecko-výskumný záujem o kremíkové kvantové bity na úrovni od vládnych agentúr až po súkromné IT spoločnosti (napr. Intel). Našim zámerom je podieľať sa na výskume teoretických modelov pre **“kvantové bodky” v kremíku** v spolupráci s experimentálnymi skupinami. Technologicky je možné kvantová bodku vyrobiť v špeciálnej polovodičovej nanoštruktúre a uväzniť v nej jeden elektrón, ktorý predstavuje kvantový bit.

Okrem spinových stavov individuálnych elektrónov možno využiť pre kvantové výpočty aj kolektívne spinové stupne voľnosti pochádzajúce z viazaných stavov systému viacerých elektrónov nízkorozmerných magnetických materiálov a nanoštruktúr. **Molekulárne nanomagnety**, ktoré z magnetického hľadiska predstavujú experimentálnu realizáciu malých elektrónových spinových klastrov, majú pre kvantové počítanie dve veľmi dôležité vlastnosti: (i) molekulárnym inžinierstvom je možné ich vlastnosti pripraviť na mieru, pričom zostávajú takmer nezmenené aj pri ich umiestnení na substrát (podložku); (ii) vzhľadom na silnejšiu interakciu medzi elektrónovými spinmi môže byť operačný čas kvantových hradiel (rádovo nanosekundy) podstatne kratší ako doba “života” takýchto kvantových bitov (rádovo mikrosekundy).

Výhodou vysokospinových molekúl a izolovaných iónov je, že ponúkajú možnosť umiestniť viacero kvantových bitov v jednej sade energetických hladín spinového systému a jednoducho adresovať multiqubitové kvantové logické operácie zmenou aplikovaného magnetického poľa, resp. frekvencie mikrovlnného pulzu. V Košiciach existuje silná tradícia experimentálneho výskumu takýchto spinových systémov. Navyše magnetické ióny je možné využiť v kvantových výpočtoch aj ako **kvantovú pamäť**, kedy molekulový magnet umiestnený v mikrorezonátore môže priamo vytvárať súčasť kvantovej zbernice pozostávajúcej so supravodivými mezoštruktúrami. Dôležitým parametrom, ktorý bude potrebné dosiahnuť, je silná väzba súboru spinov k mikrovlnnému rezonátoru potrebná na koherentný prenos kvantovej informácie. Pre úspešný prenos informácie nie je dôležitá len vhodná konštrukcia rezonátora, ale aj výber vhodného súboru spinov.

Jedným z najpálčivejších problémov, ktoré podstatne ovplyvňujú rozvoj kvantových počítačov, je, že fyzická realizácia kvantových bitov v akomkoľvek systéme podlieha kvantovým chybám – dekoherencii kvantových systémov, kvantovému šumu pri unitárnych operáciách, a podobne. Intuitívnym riešením tohto problému, podobne ako u klasických počítačov, je redundancia, teda použitie viacerých bitov na rovnaké operácie. Pre kvantové počítače však takýto spôsob korekcie chýb komplikujú viaceré principiálne prekážky, napr. technická náročnosť zvyšovania počtu previazaných kvantových bitov, alebo nemožnosť klonovania neznámeho kvantového stavu. Existuje však možnosť, ako sa kvantovým chybám úplne vyhnúť – zrealizovať tzv. **topologicky chránené kvantové bity.** Teoretické práce naznačujú, že takéto topologicky chránené bity sa dajú realizovať formou jednorozmerných spinovo polarizovaných nanoštruktúr vytvorených na povrchu niektorých špecifických supravodičov. V *Centre fyziky veľmi nízkych teplôt* v Košiciach sa už desaťročia venujeme špičkovému výskumu supravodivých materiálov, z ktorých niektoré majú vlastnosti vhodné práve na realizáciu týchto systémov. Našim cieľom bude takéto systémy pripraviť a študovať ich vlastnosti z pohľadu realizácie kvantových bitov.

Hlavné výskumné ciele:

C2.3.1 Implementácia kvantových bitov v kremíku

Vytvorená vedecká skupina v prvej fáze preskúma pomocou počítačových simulácií vychádzajúc z mikroskopických modelov vlastnosti kremíkových kvantových bodiek s cieľom identifikovať mechanizmy kvantového šumu v izotopicky čistom kremíku a v kremíku s dierovou vodivosťou. Na Slovensku síce neexistuje laboratórium experimentujúce s polovodičovými kvantovými čipmi, avšak kontakty riešiteľov umožňujú relevantný teoretický výskum v spolupráci s poprednými zahraničnými expertmi v tejto oblasti (napríklad v Japonsku a Nemecku).

C2.3.2 Previazané kvantové bity v molekulárnych nanomagnetoch

Preskúmame odolnosť kvantového previazania voči teplotným fluktuáciám vo vybraných nízkorozmerných kvantových spinových systémoch zahrňujúcich okrem iného aj molekulové nanomagnety. Spravíme komplexnú analýzu začínajúc teoretickým výpočtom z prvých princípov až po následné teoretické modelovanie dostupných, resp. novo nameraných experimentálnych údajov.

C2.3.3 Kvantová teleportácia a komunikácia pomocou spinových reťazcov

Z hľadiska kvantovej komunikácie a kvantového spracovania informácie je tiež dôležitá teleportácia kvantovo previazaných stavov, ktorú plánujeme preskúmať v systéme komunikačných kanálov tvorených dvoma kvantovými spinovými reťazcami. Spoľahlivosť štandardného teleportačného protokolu pozostávajúceho zo sústavy dvoch kvantových kanálov budeme charakterizovať pomocou prekryvu vstupného čistého kvantovo

previazaného stavu prvého spinového reťazca so zmiešaným kvantovým stavom získaným na výstupe druhého spinového reťazca.

C2.3.4 Materiály s topologicky-chránenými kvantovými bitmi

Špičková výbava našich laboratórií umožňuje prípravu a charakterizáciu spinovo polarizovaných nanoštruktúr. Cieľom je pripraviť a otestovať jeden takýto systém – supravodič s Isingovou spin-orbitálnou väzbou s feromagnetickým nanoreťazcom na povrchu, na ktorom chceme experimentálne demonštrovať existenciu topologicky chránených Majorana viazaných stavov pomocou spinovo polarizovanej skenovacej tunelovej mikroskopie.

C2.3.5 Kvantové bity uložené v magnetických iónoch

V prvej fáze identifikujeme spinový systém vhodný pre obvody s kvantovou pamäťou na báze magnetických iónov a následne navrhneme a zostrojíme mikrovlnný rezonátor vhodný pre takéto obvody. V poslednej fáze budeme hľadať kombináciu spinového systému a mikrorezonátora s optimálnou väzbou. Vlastnosti magnetického systému (masívnej vzorky, zriedenej vzorky alebo tenkej vrstvy), ktoré je potrebné poznať pre vytvorenie kvantového bitu alebo pamäťového objektu je možné určiť pomocou štandardnej elektrónovej paramagnetickej rezonancie. S cieľom prispieť k vývoju kvantovej elektroniky využijeme poznatky našich expertov v oblasti magnetickej rezonancie a výbornej technickej základne pre litografickú prípravu mezoskopických štruktúr pri dizajnovaní vlastných rezonátorov.

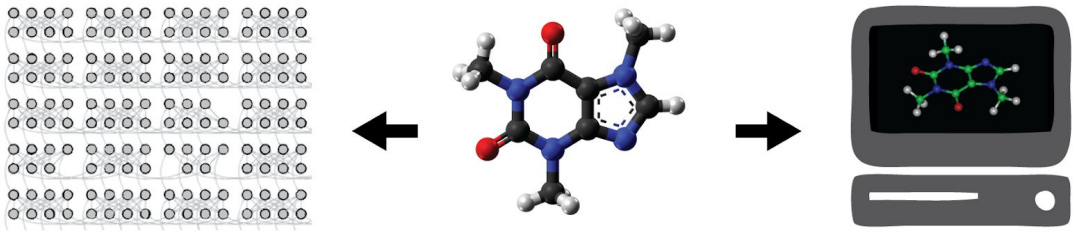
Zámer 2.4 Kvantové simulácie a výpočtová zložitosť

(koordinátor: Andrej Gendiar)

Partneri: FÚ SAV, ÚEF SAV, UPJŠ

Zodpovední riešitelia: Andrej Gendiar, Daniel Nagaj, Daniel Reitzner, Peter Rapčan, Roman Krčmár, Hana Čenčaríková, Gabriel Semanišin,

Popis zámeru:



kvantová simulácia
programovateľný systém supravodivých qubitov

zaujímavá molekula
reálny fyzikálny/chemický mnohočasticový systém

klasická simulácia
náročné numerické riešenie rovníc

Naším cieľom je vývoj špičkových simulačných metód pre veľké kvantovomechanické systémy a ich aplikácia vo fyzike tuhých látok a kvantovej chémii. Kvantové simulácie sú jedným z pilierov kvantového Flagshipu, a oblasťou, kde sa očakáva najväčšie uplatnenie stredne veľkých a mierne zašumených kvantových čipov vyvinutých v blízkej budúcnosti. Pomôžu nám virtuálne, rýchlo a relatívne lacno **simulovať a skúmať systémy náročné na výrobu alebo klasickú počítačovú simuláciu**. Výsledkom, ku ktorému nám dopomôžu tu vyvinuté metódy, by mohli byť nové supravodivé materiály pre elektrotechnické aplikácie, topologicky chránené kvantové pamäte, modelovanie jadrových reakcií, porozumenie štruktúre časopriestoru alebo nové liečivá vyvinuté vďaka porozumeniu trojrozmernej štruktúre a chemickej aktivite proteínov.

Úlohou fyziky je dospieť od prvotných princípov a rovníc k efektívnemu popisu celého systému. S rozvojom počítačovej techniky nastal obrovský pokrok aj v možnostiach numerických simulácií a mnohokrát vieme vysvetliť vlastnosti iba vďaka simuláciám. Zložitosť simulácie kvantových systémov však extrémne narastá s počtom častíc a práve fyzika takýchto mnohočasticových kvantových systémov (modelujúcich molekuly a materiály) nás typicky zaujíma.

Cieľom našich kvantových simulácií je analýza a veľmi presné riešenie úloh z kvantovej fyziky pre takéto mnohočasticové systémy. Simulácie prepájajú kvantovú teóriu s experimentálnymi meraniami a umožňujú nám skúmať reálne kvantové systémy pomocou numerických výpočtov, klasických či kvantových, podľa toho na akom hardvéri ich implementujeme. Experimentálne náročné merania tak môžeme vopred skúmať vďaka tomu, že sa simulovaný systém správa podľa rovníc kvantovej téorie. Týmto postupom vieme predpovedať aj celkom nové fyzikálne javy a navrhovať experimenty, ktoré v prípade úspešnej realizácie môžu byť neskôr aplikované až do priemyselnej výroby. Na druhej strane, neznáme javy alebo efekty, s ktorými sa experimentátori stretávajú, je potrebné zdôvodniť pomocou vhodnej teórie, ktorú ľahko overíme počítačovými simuláciami.

Našou expertízou a základným príspevkom je metóda tenzorových sietí. Stáli sme (skupina Dr. Gendiara na FÚ SAV) pri jej zrode a navrhli sme a publikovali niekoľko nových algoritmov pre popis mnohočasticových systémov s vysokou presnosťou. Táto metóda je založená na fragmentácii kvantových stavov do menších objektov - tenzorov. Tieto tenzory

sú vzájomne poprepájané a zvyčajne reprezentujú sieť interakcií medzi časticami. Vytvárajú tak matematickú štruktúru, pomocou ktorej reprezentujeme stav systému a dokážeme ho efektívne vyvíjať alebo optimalizovať. Naším cieľom je rozvoj tejto oblasti a návrh nových algoritmov pre štúdium vlastností kvantových fáz (topologické usporiadania), na analýzu hyperbolických geometrií priestoročasu (kvantová teória gravitácie), na fraktálne štruktúry a mnohorozmerné kvantové stavy častíc.

Keďže simulácie sú vo svojej podstate náročné, druhým cieľom tohto zámeru je **porozumenie výpočtovej zložitosti simulačných a optimalizačných úloh**, ktoré sa objavujú v priemyselných aplikáciách (návrhy rozloženia tranzistorov na čipe, rozoznávanie obrazov) ale aj vo fyzike tuhých látok (hľadanie stavov s najnižšou energiou, porozumenie koreláciám). Na túto zložitosť sa musíme pozrieť vo svetle kvantového počítania. Výsledkom bude nielen základný výskum na hranici teoretickej informatiky a kvantovej fyziky, ale aj praktické, efektívnejšie optimalizačné algoritmy, ktoré naplno využijú dostupné kvantové zdroje (previazanie, superpozície, tunelovanie).

Základnými nástrojmi na porozumenie zložitosti je mapovanie problémov medzi rôznymi oblasťami teoretickej informatiky a kvantovej fyziky. V tejto oblasti sme (skupina Dr. Nagaja na FÚ SAV) priniesli zásadné výsledky pre oblasť kvantovej zložitosti lokálnych Hamiltoniánov - prispeli k rozvoju optimalizačných adiabatických algoritmov, porozumeli možnostiam univerzálneho kvantového počítania pre mnohé modely interakcií, a objavili viaceré zaujímavé, jednoducho popísané fyzikálne systémy s prekvapivo komplikovanými vlastnosťami. Na ďalšie takéto objavy použijeme naše porozumenie mapovaniam potrebným pre simulácie jedného systému druhým, efektívnym interakciám, a rôznym metódam kódovania a opráv kvantovej informácie.

Súčasný rozvoj v oblasti umelej inteligencie a strojového učenia (tzv. machine learning) je determinovaný do značnej miery technologickými možnosťami. Je preto najvyšší čas využiť a aplikovať tieto možnosti aj do oblasti kvantových technológií. K tomu sa dá pristúpiť dvomi spôsobmi. Jedným z nich je použiť klasické nástroje machine learningu na optimalizáciu kvantovomechanických úloh, a tak prispieť k ich zefektívneniu. V druhom spôsobe sa chceme zaoberať možnosťou **kvantového strojového učenia**, t.j. takých sietí, ktoré by boli buď kvantové, alebo by vedeli narábať s kvantovými stavmi. Táto oblasť je horúcou témou súčasnosti s nie úplne jasným prínosom (high-risk-high-gain), ale s potenciálom vysvetliť kvantové mechanizmy radikálne odlišným spôsobom.

Dnes existuje veľa otvorených problémov súvisiacich s určením výpočtovej sily a ohraničení kvantových počítačov ako nového typu výpočtových nástrojov. Z hľadiska dlhoročnej tradície výskumu klasických automatov a formálnych jazykov (UPJŠ) je prirodzené rozšíriť a zúročiť získané poznatky v kontexte kvantových automatov. Štúdiom operátorových algebier v synergii s teoretickými fyzikmi sa chceme pokúsiť rozvinúť existujúce matematické modely kvantového počítania doteraz založené prevažne na konečnorozmerných Hilbertových priestoroch. Ako sa však ukazuje, kvantové toky sa dajú sémanticky označiť ako nekonečné tenzorové súčiny von Neumannových algebier, ktoré sú nutne nekonečnorozmerné, z čoho vyvstáva potreba hlbšieho štúdia ich štruktúr.

Hlavné výskumné ciele:

C 2.4.1 Od tenzorových sietí ku simuláciám kvantovej gravitácie

Vyvinieme algoritmy tenzorových sietí pre systémy interagujúcich častíc s multidimenzionálnymi stupňami voľnosti a variabilnou geometriou interakcií. Takýto diskrétny priestor môže mať zaujímavú geometriu zakriveného priestoru, napr. v blízkosti čiernej diery. Analýzou entropie previazania v zakrivenom priestore prispejeme do nepreskúmanej oblasti kvantovej gravitácie z pohľadu korešpondencie medzi tzv. Anti de-Sitterovým (hyperbolickým) priestorom a konformnou teóriou poľa.

C 2.4.2 Dominantnosť kvantových výpočtov

Cieľom je získať kvantový systém, ktorého výpočtové schopnosti vysoko prevyšujú možnosti klasických počítačov a simulácií. V tejto vysoko kompetitívnej oblasti v súčasnosti pracujú výskumné tímy s rozpočtom a ľudským potenciálom, ktorý ďaleko prevyšuje možnosti slovenskej platformy. Súťaží sa na dvoch frontoch: na technologickom a na konceptuálnom, ktorý nutne nevyžaduje až také obrovské investície. Ako navrhovatelia inovatívnych myšlienok sme zapojení v medzinárodných projektoch, v ktorých sú experimentálni partneri pripravení ich zrealizovať. Tento cieľ má aplikácie v oblasti kvantových technológií vo všeobecnosti, a takisto je dôležitý pre pochopenie výpočtovej zložitosti kvantových úloh a vývoj nových optimalizačných algoritmov.

C 2.4.3 Metódy strojového učenia v optimalizácii kvantového spracovania informácie

Rozvinieme techniky strojového učenia pre kvantové systémy a vyvinieme techniky na rýchle rozpoznávanie kvantových stavov, operácií a procesov, a ich následnú implementáciu a optimalizáciu. Tento cieľ má dve cesty, klasické strojové učenie a certifikáciu kvantových systémov, a na druhej strane čisto kvantové spracovanie informácie a súvisiacu výpočtovú zložitosť.

C 2.4.4 Kvantové kráčania na nemriežkových systémoch

Naším cieľom je využiť kvantové kráčania - šírenie excitácií v kvantových systémoch - na vývoj nových vyhľadávacích algoritmov. Môžu byť konceptuálne podobné klasickým Markovovským reťazcom, no využitie kvantových superpozícií umožní rádové urýchlenie počtu potrebných krokov. Špeciálne sa zameriame na kráčania na nemriežkových systémoch, podobných tým v cieli C 2.4.1.

C2.4.5 Matematické modely kvantových algoritmov

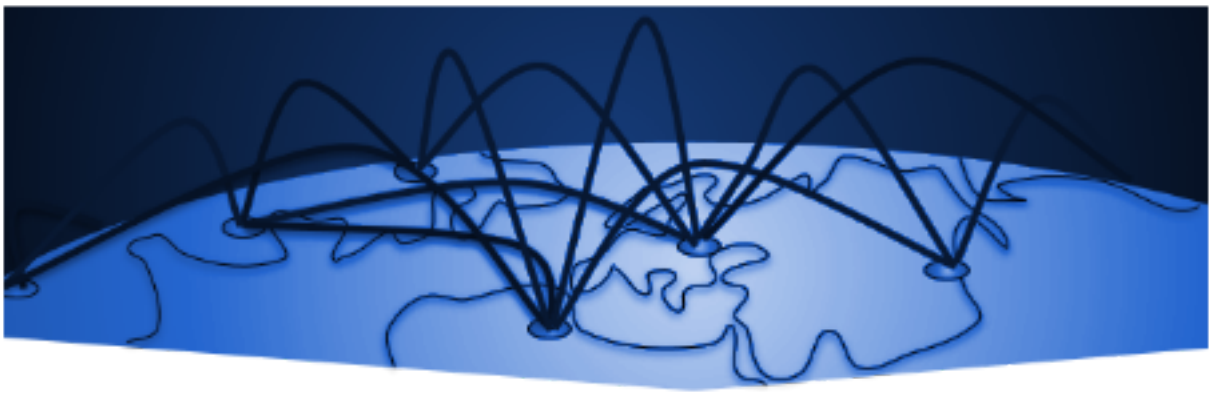
Cieľom je skombinovať poznatky z klasickej výpočtovej zložitosti, matematickej analýzy, algebry, kombinatorickej optimalizácie a návrhu algoritmov spolu s modelmi kvantového počítania za účelom vytvoriť nové kvantové algoritmy pre známe problémy s veľkou výpočtovou zložitosťou.

Zámer 2.5 Kvantové a postkvantové komunikačné siete

(koordinátor: Mário Ziman)

Inštitúcie: FEI STU, FÚ SAV, MÚ SAV

Zodpovední riešitelia: Pavol Zajac, Mário Ziman, Daniel Reitzner, Vladimír Bužek, Otokar Grošek, Karol Nemoga, Tomáš Fabšič



Popis zámeru:
Komunikačné protokoly môžu získať dodatočný stupeň ochrany za použitia princípov kvantovej mechaniky. Teoreticky je táto bezpečnosť dokonalá, avšak v nedokonalom svete je potreba brať do úvahy mnoho vplyvov. Kvantovo chránená komunikácia musí byť schopná tieto vplyvy identifikovať a odstrániť. V poslednom období sa vyvíjajú tzv. prístrojovo-nezávislé kryptografické schémy, ktoré vďaka kvantovej nelokálnosti (pseudo-telepatii) vedia eliminovať aj situácie, kedy dodané prístroje nie sú dôveryhodné, t.j. môžu obsahovať pre užívateľov neznáme trójske kone v podobe postranných komunikačných kanálov, ktorými tieto prístroje potenciálne komunikujú bez kontroly užívateľov. Niektoré z týchto prístupov sa zakladajú aj na našom doterajšom výskume o kvantovej nekompatibilite a nelokálnosti, ktoré sú nutnou podmienkou pre spoľahlivosť takýchto protokolov.

Z pohľadu bezpečnosti kvantových protokolov je kľúčovou fázou distribúcia kvantového kľúča, ktorý následne komunikáciu cez kvantovú komunikačnú sieť umožňuje, resp. ju do istej miery aj definuje. Otázkou je ako eliminovať vplyvy útočníkov, ale aj prípadného šumu, a umožniť tak distribúciu na ľubovoľné vzdialenosti. V prípade dvojužívateľských protokolov sú ideálnym riešením destilácia a kvantový zosilňovač. Naším primárnym cieľom je pozrieť sa na efektívnu (v zmysle komunikačnej zložitosti) distribúciu viacužívateľských kľúčov tolerujúcich aj existenciu šumu.

Alternatívou ku kvantovej kryptografii je tzv. post-kvantová kryptografia, ktorej cieľom je vyvinúť nové technologické štandardy a spôsoby klasického šifrovania, ktoré sú imúnne voči akémukoľvek kvantovému útoku. Tieto schémy sú známe už dlhšie, avšak výpočtová zložitosť šifrovania a dešifrovania bola pre počítače doby minulej príliš komplikovaná.

Hlavné výskumné ciele:

C2.5.1 Implementačne bezpečná prakticky prístrojovo-nezávislá kvantová komunikácia

Uskutočníme analýzu testov nelokálnosti (tzv. Bellových nerovností) pre viacrozmerné systémy. Následne, okrem zabezpečenia samotnej informácie, sa budeme venovať aj prístrojovo-nezávislým protokolom na zdieľanie tajomstva, anonymných kanálov, a kvantového anonymného hlasovania.

C2.5.2 Bezpečná distribúcia viacužívateľkých kvantových kľúčov

Súčasťou riešenia je mechanizmus vytvorenia stabilného previazaného stavu, ktorý sa dá transformovať do stavu umožňujúceho realizáciu požadovaného kvantového protokolu. Ohraničenia na možnosti certifikácie, resp. očistenia stavu, de facto limitujú možnosti samotných kvantových komunikačných technológií.

C2.5.3 Efektívna a bezpodmienečne bezpečná postkvantová kryptografia

Zameriame sa na vývoj a využitie algoritmov asymetrickej kryptografie, ktoré sú bezpečné voči útočníkovi s prístupom ku kvantovému počítaču, a efektívne na použitie v komunikačných protokoloch (post-kvantové algoritmy). Zaujímavá je aj otázka bezpečnej kombinácie štandardnej symetrickej a post-kvantovej asymetrickej kryptografie s kvantovou distribúciou kľúčov a používania kombinovaných protokolov.

3. AKTIVITA QUAPITAL

Cieľ: Vytvorenie veľkoškálovej kvantovej komunikačnej siete QUAPITAL.

Táto aktivita má za cieľ vybudovanie kvantovej kryptografickej siete medzi hlavnými mestami Európskej únie umožňujúcej bezpečnú komunikáciu medzi veľvyslanectvami a štátnymi inštitúciami jednotlivých krajín EÚ. Ide o medzinárodný infraštruktúrny zámer a v roku 2018 sa začalo formovať medzinárodné konzorcium európskych výskumných a priemyselných inštitúcií QUAPITAL (https://quapital.eu/). Samotné financovanie tejto časti projektu je mimoriadne nákladné, a preto už v prvej etape budeme hľadať iné (európske, aj súkromné) zdroje na jeho realizáciu.

Zámer 3.1 Vytvorenie kvantovej linky medzi Viedňou a Bratislavou

(koordinátor: Peter Rapčan)

Berúc do úvahy technologické know-how na Viedenskej univerzite (skupina profesora Ruperta Ursina), existujúcu spoluprácu medzi pracoviskami vo Viedni a v Bratislave (CVKI FÚ SAV) a geografickú blízkosť týchto dvoch miest je úplne prirodzené, aby prvá kvantová linka siete QUAPITAL vznikla práve tu.

Zámer 3.2 Vytvorenie kvantovej komunikačnej siete medzi hlavnými stredoeurópskymi mestami

(koordinátor: Vladimír Bužek)

Tento zámer je prirodzeným pokračovaním zámeru 3.1 a vytvorí unikátnu infraštruktúru, ktorá bude významným vedecko-výskumným prínosom.

ODHADOVANÝ ROZPOČET

Naplnenie aktivít a dosiahnutie zámerov platformy QUTE počíta s rozpočtom **8 725 000 eur** na 5 rokov. Z toho zhruba tretina na pokrytie experimentálnych potrieb (kapitálové a materiál) a zvyšok na personálne náklady (mzdové, cestovné a služby).

Celková suma je alokovaná pre jednotlivé aktivity nasledovne:

Aktivita eduQUTE

3 835 000 eur

- Mzdové náklady (2 304 000 eur) pokrývajú v každom roku riešenia jednu kompetentnú administratívnu silu, cca 8 postdoktorandov (3000 eur/mesačne) a štipendijnú podporu pre 16 doktorandov (plus 600 eur/mesačne) a 16 študentov druhého stupňa (300 eur/mesačne). Tieto náklady (spolu s nákladmi odvodenými) budú distribuované partnerom podľa ich úspešnosti pri rozdelení príslušných štipendií.
- Odvody (811 000 eur) súvisia so mzdovými nákladmi.
- Cestovné výdavky (80 000 eur) pokrývajú postdoktorandom ich konferencie a výskumné pobyty.
- Materiál pokrýva materiálové potreby postdoktorandov (80 000 eur) a administratívy (10 000 eur) na propagáciu kvantových technológií a prezentáciu výsledkov platformy.
- Náklady na organizovanie školy a workshopu (50 000 eur) pokrývajú primárne cestovné náklady pozvaných prednášajúcim a odmenu za ich prednáškové kurzy (120 eur/hodina)

Aktivita iQUTE

4 890 000 eur

Bežné prostriedky sú rozdelené medzi jednotlivých partnerov podľa očakávanej aktivity pri plnení plánovaných úloh a zámerov. Jeden osobomesiac je ohodnotený na 1600 eur. Nepriame náklady sú počítané ako cca 15 % z bežných. Kapitálové výdavky (v celkovej hodnote 3 000 000 eur) pokrývajú potrebné investície do plánovaných experimentov a budú distribuované podľa požiadaviek jednotlivým partnerom.

Bežné prostriedky:

- Centrum pre výskum kvantovej informácie, FÚ SAV (540 000 eur)
  Pokrýva 180 osobomesiacov riešiteľov na jednotlivých zámeroch akčného plánu, s tým súvisiace cestovné 30 000 eur a materiálové náklady 30 000 eur. Suma 18 000 eur je vyčlenená na hostí.
- FMFI UK (360 000 eur)
  Pokrýva 120 osobomesiacov riešiteľov na jednotlivých zámeroch akčného plánu, s tým súvisiace cestovné 20 000 eur a materiálové náklady 20 000 eur. Suma 12 000 eur je vyčlenená na hostí pri odhade 120 eur/deň pobytu.
- PF UPJŠ (360 000 eur)
  Pokrýva 120 osobomesiacov riešiteľov na jednotlivých zámeroch akčného plánu, s tým súvisiace cestovné 20 000 eur a materiálové náklady 20 000 eur. Suma 12 000 eur je vyčlenená na hostí pri odhade 120 eur/deň pobytu.
- FEI STU (180 000 eur)

Pokrýva 60 osobomesiacov riešiteľov na jednotlivých zámeroch akčného plánu, s tým súvisiace cestovné 10 000 eur a materiálové náklady 10 000 eur. Suma 6 000 eur je vyčlenená na hostí pri odhade 120 eur/deň pobytu.

- ÚEF SAV (180 000 eur)
  Pokrýva 60 osobomesiacov riešiteľov na jednotlivých zámeroch akčného plánu, s tým súvisiace cestovné 10 000 eur a materiálové náklady 10 000 eur. Suma 6 000 eur je vyčlenená na hostí pri odhade 120 eur/deň pobytu.
- MÚ SAV (180 000 eur)
  Pokrýva 60 osobomesiacov riešiteľov na jednotlivých zámeroch akčného plánu, s tým súvisiace cestovné 10 000 eur a materiálové náklady 10 000 eur. Suma 6 000 eur je vyčlenená na hostí pri odhade 120 eur/deň pobytu.
- ELÚ SAV (90 000 eur)
  Pokrýva 30 osobomesiacov riešiteľov na jednotlivých zámeroch akčného plánu, s tým súvisiace cestovné 5 000 eur a materiálové náklady 5 000 eur. Suma 3 000 eur je vyčlenená na hostí pri odhade 120 eur/deň pobytu.

Kapitálové výdavky (odhady výdavkov):

- 500 000 eur (FMFI UK) na 3D laserovú litografiu,
- 700 000 eur (UPJŠ) na upgrade EPR spektrometra Bruker ELEXSYS model E500 na model E580 FT/CW s héliovým kryostatom, dvojročná záruka s inštaláciou a dopravou,
- 500 000 eur (ELÚ SAV) na leptač a zariadenia PECVD na vytváranie izolácií vytvorených nanoštruktúr,
- 500 000 eur (ÚEF SAV) na refrigerátor a elektronické prístroje,
- 800 000 eur (FÚ SAV) na vybavenie laboratória kvantovej optiky

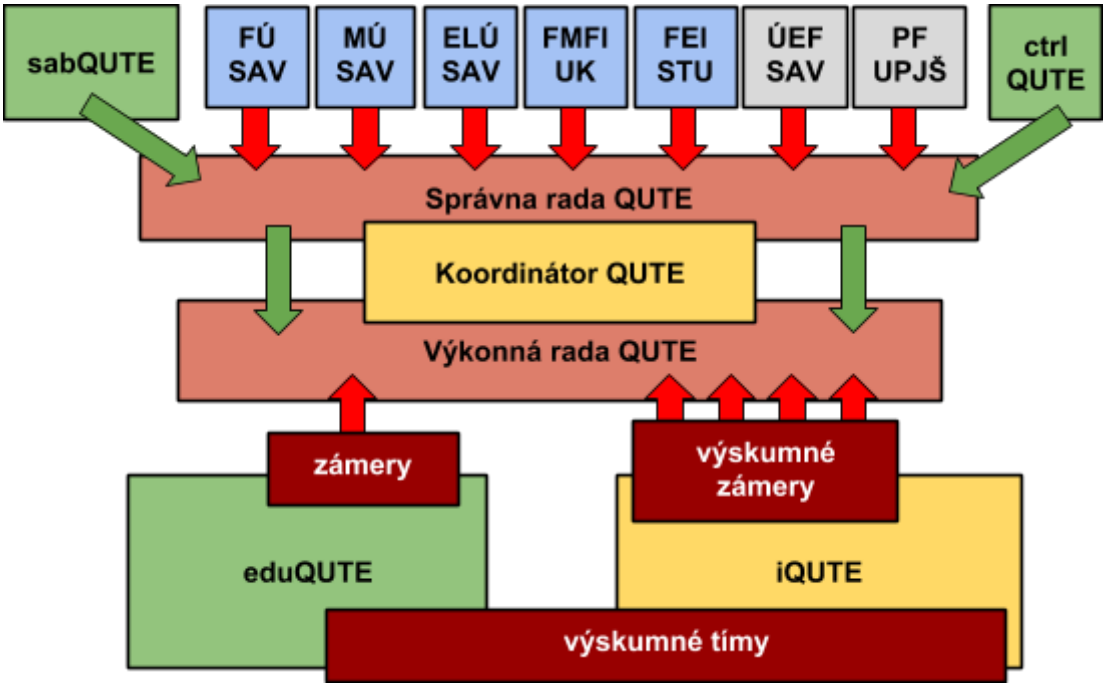
Aktivita QUAPITAL

0 eur

Finančné prostriedky na túto aplikačnú aktivitu plánujeme získať z iných zdrojov - verejných, aj súkromných.

POZNÁMKA: samotné financovanie Akčného plánu Platformy QUTE navrhujeme v dvoch platbách z dôvodu, čo najefektívnejšieho spôsobu využitia navrhovaných zdrojov. V prvej platbe vyplatiť 75% peňazí projektu na prvé tri roky riešenia projektových zámerov (kapitálové výdavky sa očakávajú práve v tomto období), a následne po zúčtovaní výsledkov, t.j. po výskumnej a finančnej správe. Po zvládnutí oponentúry výsledkov navrhujeme vyplatiť v ďalšej platbe zvyšok rozpočtu.

ORGANIZAČNÁ ŠTRUKTÚRA



Správna Rada národnej platformy QUTE (srQUTE) pozostáva zo zástupcov jednotlivých inštitúcií tvoriacich platformu. Zástupcov nominuje štatutár partnerskej organizácie na návrh riešiteľských tímov tejto organizácie, ktoré sú členmi platformy QUTE. srQUTE vymenúva koordinátora platformy QUTE, ktorý sa stáva jej členom a administratívne zabezpečuje jej fungovanie a komunikáciu s ostatnými štruktúrami platformy. Úlohou rady je prijímať strategické rozhodnutia ohľadne smerovania a fungovania platformy QUTE, rozhodovať o prijímaní/vylúčení nových výskumných tímov, ale aj partnerov, do platformy a hodnotiť ich aktivity. srQUTE pracuje v súčinnosti so všetkými zložkami platformy a tvorí prepojenie medzi sabQUTE a ctrlQUTE s vrQUTE.

Aktuálne zloženie srQUTE:

- Prof. RNDr. Vladimír Bužek, DrSc.
- RNDr. Vladimír Cambel, DrSc.
- Prof. RNDr. Alexander Feher, DrSc.
- Prof. RNDr. Miroslav Grajcar, DrSc.
- Doc. RNDr. Karol Nemoga, DrSc,
- Prof. RNDr. Peter Samuely, DrSc.
- Prof. Ing. Pavol Zajac, PhD
- Doc. Mgr. Mário Ziman, PhD

Výkonná Rada národnej platformy QUTE (vrQUTE) pozostáva z koordinátora QUTE, zástupcov iQUTE (koordinátorov jednotlivých zámerov) a jedného zástupcu z Rady eduQUTE. Na čele vrQUTE stojí koordinátor QUTE. Úlohou vrQUTE je koordinovať aktivity jednotlivých členov, zorganizovať a uskutočniť naplánované aktivity. Výkonná rada

- navrhuje jednotlivé výskumné a organizačné aktivity platformy,
- navrhuje procedurálne postupy pri rozdeľovaní finančných zdrojov iQUTE a eduQUTE,
- menuje výberové a organizačné komisie, vypracováva ročnú správu projektu.

Činnosť vrQUTE je monitorovaná srQUTE, ktorá jednotlivé návrhy vrQUTE schvaľuje.

Aktuálne zloženie vrQUTE:

- Mgr. Andrej Gendiar, PhD
- Prof. RNDr. Miroslav Grajcar, DrSc.
- Mgr. Anna Jenčová, DrSc.
- Mgr. Tomáš Samuely, PhD
- Doc. Mgr. Mário Ziman, PhD
- Prof. RNDr. Vladimír Bužek, DrSc.

Koordinátor QUTE je hlavným kontaktným bodom platformy. Jeho úlohou je aktívne koordinovať jednak výkonnú radu, kooperáciu so správnou radou a aktivity jednotlivých tímov platformy QUTE.

Koordinátor: doc. Mgr. Mário Ziman, PhD

Kontrolná rada národnej platformy QUTE (ctrlQUTE) bude pozostávať z troch členov, ktorých úlohou je kontrolovať výročné a finančné správy.

Medzinárodná vedecká poradná rada národnej platfomy QUTE (sabQUTE, Science Advisory Board) bude tvorená piatimi pozvanými odborníkmi zo zahraničia, ktorí sú volení srQUTE. Ich úlohou je monitorovať aktivity národnej platformy, kriticky a konštruktívne komentovať najmä vedecko-výskumné a organizačné aktivity.

iQUTE je virtuálny kvantový inštitút, ktorý združuje jednotlivé **výskumné tímy** a koordinuje ich výskumné a popularizačné aktivity. Zabezpečuje výmenu informácií medzi nimi a organizuje spoločné semináre a konferencie v oblasti kvantových technológií. Sídli na FÚ SAV a jeho činnosť administratívne zabezpečuje Centrum pre výskum kvantovej informácie. Aktivity iQUTE sú definované ako výskumné zámery, z ktorých každý má svojho koordinátora. Koordinátori sú súčasťou vrQUTE. Vedúci riešitelia jednotlivých výskumných tímov tvoria **Radu iQUTE**. Úlohou tejto rady je koordinovať výskumnú a popularizačnú činnosť, kontrolovať napĺňanie výskumných cieľov a definovať nové vedecké výzvy. Rada iQUTE informuje o výsledkov a návrhoch vrQUTE a sabQUTE.

eduQUTE je školiace stredisko platformy QUTE sídliace na FÚ SAV, ktoré administruje zdroje pre študentov, doktorandov a postdoktorandov, organizuje výberové konania, letné školy a národný workshop fellowQUTE. Aktivity eduQUTE sú definované ako zámery, z ktorých každý má svojho koordinátora. Koordinátori zámerov spolu s koordinátorom QUTE tvoria **Radu eduQUTE**. Rada eduQUTE informuje o výsledkov a návrhoch sabQUTE a vrQUTE.

VÝSKUMNÉ TÍMY iQUTE

G1 Skupina kvantových informačných štruktúr a sietí

Inštitúcie: FÚ SAV, MÚ SAV
Vedúci: Mário Ziman

Členovia: Anna Jenčová, Michal Sedlák, Vladimír Bužek, Daniel Reitzner, Anatolij Dvurečenskij

Expertíza: Analýza a optimalizácia matematických štruktúr a vlastností kvantovej informácie (napr. klonovanie, programovanie, odhadovanie, rozlišovanie) a identifikácia a verifikácia kvantovo-informatických zdrojov (napr. previazanie, nekompatibilita, nelokálnosť). Návrh viacužívateľských protokolov pre zdieľanie kvantového tajomstva a anonymného hlasovania. Výpočet kvantových kapacít pre komunikačné kanály a štruktúra kanálov s pamäťou.

Najvýznamnejšie výsledky:

- M. Hillery, V. Bužek, and A. Berthiaume: Quantum secret sharing, Phys. Rev. A 59, 1829 (1999), 1700+ citácií
- V. Bužek and M. Hillery: Quantum copying: Beyond the noncloning theorem, Phys. Rev. A 54, 1844 (1996), 700+ citácií
- F. DeMartini, V. Bužek, F. Sciarrino, and C. Sias: Experimental realization of the universal NOT gate, Nature 419, 815 (2002), 130+ citácií
- V.Scarani, M.Ziman, P.Štelmachovič, N.Gisin, V.Bužek: Thermalizing Quantum Machines: Dissipation and Entanglement, Phys. Rev. Lett. 88 , 97905-1 (2002), 90+ citácií
- M. Hillery, M. Ziman, V. Bužek, M. Bielikova: Towards quantum-based privacy and voting, Physics Letters A 349, Issues 1-4 , pp 75-81 (2006), 50+ citácií
- A. Jenčová, D. Petz, Sufficiency in quantum statistical inference, Commun. Math. Phys. 263, 259-276 (2006), 50+ citácií
- M. Ziman: Process POVM: A mathematical framework for the description of process tomography experiments, Phys. Rev. A 77, 062112 (2008), 30+ citácií

Mgr. Mário Ziman, PhD (41) bol doktorandom na Fyzikálnom ústave SAV, absolvoval postdoktorandský pobyt v Česku (FI MU, Brno), na Slovensku (FÚ SAV) a vo Švajčiarsku (ETH Zurich). Venuje sa matematickému formalizmu kvantovej teórie, fundamentálnym otázkam kvantovo-informatických štruktúr, kvantovej kryptografii a kvantovej metrológii. Je autorom knihy “The Mathematical Language of Quantum Theory” (Cambridge University Press), spoluautorom 71 článkov, ktoré získali spolu 850+ WOK citácií, jeho h-index je 18.

G2 Skupina kvantových simulácií a algoritmických metód

Inštitúcie: FÚ SAV
Vedúci: Andrej Gendiar

Riešitelia: Daniel Nagaj, Daniel Reitzner, Roman Krčmár, Peter Rapčan, Peter Staňo

Expertíza tímu: Vývoj kvantových vyhľadávacích algoritmov založených na kvantovom kráčaní. Kvantová teória zložitosti a výpočtová zložitosť simulácií fyzikálnych systémov na klasických a kvantových počítačoch. Vývoj a analýza kvantových optimalizácií. Algoritmy tenzorových sietí pre mnohočasticové kvantové systémy interagujúcich elektrónov. Tenzorové súčinové stavy kvantových hamiltoniánov v aproximácii renormalizačnej grupy. Analýza fázových prechodov na fraktálnych a hyperbolických kvantových systémoch. Tenzorová renormalizačná grupa vyššieho rádu. Renormalizácia matíc hustoty. Teória kvantového hardvéru v polovodičoch, návrhy a analýza implementácií kvantových bitov.

Najvýznamnejšie publikácie:

- J. Fabian, A. Matos-Abiague, C. Ertler, P. Stano, I. Zutic, Semiconductor spintronics, Acta Physica Slovaca 57, 565 (2007), 600+ citácií
- J. Klinovaja, P. Stano, A. Yazdani, D. Loss, Topological Superconductivity and Majorana Fermions in RKKY Systems, Phys. Rev. Lett, 111, 186805 (2013), 200+ citácií
- Rolando D. Somma, Daniel Nagaj, Maria Kieferova: Quantum Speedup by Quantum Annealing, Phys. Rev. Lett. 109, 050501 (2012), 35+ citácií
- Sergey Bravyi, Libor Caha, Ramis Movassagh, Daniel Nagaj, Peter Shor: Criticality without frustration for quantum spin-1 chains, Phys. Rev. Lett. 109, 207202 (2012), 35+ citácií
- Daniel Reitzner, Daniel Nagaj, Vladimír Bužek: Quantum walks, Acta Physica Slovaca 61, No.6, 603-725 (2011), 30+ citácií
- Roman Krčmár, Jozef Genzor, Yoju Lee, Hana Čenčariková, Tomotoshi Nishino, Andrej Gendiar: Tensor-network study of quantum phase transition on Sierpiński fractal, Phys. Rev. E 98, 062114 (2018).
- Andrej Gendiar, Tomotoshi Nishino: Phase diagram of the 3D Axial-Next-Nearest-Neighbor Ising model, Phys. Rev. B 71, 024404 (2005), 20+ citácií

Mgr. Andrej Gendiar, PhD (45) sa venuje vývoju efektívnych algoritmov na simulácie kvantových systémov, pomocou ktorých skúma fyzikálne a chemické vlastnosti a procesy v tuhých látkach. Absolvoval postdoktorandské stáže v Nemecku a Japonsku. Je spoluautor 44 publikácií, ktoré získali 280+ WOK citácií a jeho h-faktor je 11.

G3 Laboratórium kvantových meraní

Inštitúcie: FMFI UK, ELÚ SAV, FÚ SAV
Vedúci: Miroslav Grajcar

Riešitelia: Richard Hlubina, Peter Markoš, Pavol Neilinger, Vladimír Cambel, Dana Gregušová, Marek Ťapajna

Expertíza: Teória metamateriálov a šírenie vĺn v neusporiadaných štruktúrach, konštrukcia ultra-nízkošumových elektronických zosilňovačov a detektorov, supravodivé kvantové bity, mikrovlnná a optická spektroskopia, teória tuhých látok a topologických materiálov.

Najvýznamnejšie výsledky:

- Patent US 2003/0224944 A1, Miles F. H. Steininger, Alexandre M. Zagoskin, Miroslav Grajcar, Evgeni Il'ichev, Characterization and measurement of superconducting structures
- Patent US 2005/0256007 - Mohammad H. S. Amin, Miroslav Grajcar, Andrei A. Izmalkov, Evgeni Il'ichev, Miles F. H. Steininger, Adiabatic quantum computation with superconducting qubits
- M. Grajcar, S.H.W. Van Der Ploeg, A. Izmalkov, E. Il'ichev, H. -G. Meyer, A. Fedorov, A. Shnirman, G. Schoen Sisyphus cooling and amplification by a superconducting qubit Nature Physics 4, 612-616 , (2008).
- G.Oelsner, P. Macha, O. V. Astafiev, E. Il'ichev, M. Grajcar, U. Hubner, B. I. Ivanov, P. Neilinger, and H.-G. Meyer Dressed-State Amplification by a Single Superconducting Qubit Phys. Rev. Lett. 110, 053602 (2013).
- Z. Medvecká, T. Klein, V. Cambel, J. Šoltýs, G. Karapetrov, F. Levy-Bertrand, B. Michon, C. Marcenat, Z. Pribulová, and P. Samuely: Observation of a transverse Meissner effect in Cu_xTiSe_2 single crystals, Phys. Rev. B 93, 100501(R) (2016).

Prof. RNDr. Miroslav Grajcar, PhD (52) sa venuje supravodičovým kvantovým technológiám a supercitlivým kvantovým meraniam. Je spoluautorom 2 amerických patentov, 84 publikácií, má 1600+ WOK citácií, h-index 23.

G4 Laboratórium kvantového magnetizmu

Inštitúcie: ÚEF SAV, UPJŠ
Vedúci: Erik Čižmár

Riešitelia: Martin Orendáč, Alžbeta Orendáčová, Alexander Feher, Róbert Tarasenko, Vladimír Tkáč, Karol Flachbart, Slavomír Gabáni, Gabriel Pristáš, Vladimír Komanický

Expertíza: Technická základňa pre litografickú prípravu mezoskopických štruktúr na dizajn vlastných rezonátorov s vysokým faktorom kvality Q na báze tenkých filmov klasických a vysokoteplotných supravodičov, charakterizácia pomocou spinovo polarizovanej skenovacej tunelovej mikroskopie a elektrónovej paramagnetickej rezonancie.

Najvýznamnejšie výsledky:

- S.A. Zvyagin, M. Ozerov, E. Čižmár, D. Kamenskyi, S. Zherlitsyn, T. Herrmannsdörfer., J. Wosnitza, R. Wünsch, W. Seidel, Terahertz-range free-electron laser electron spin resonance spectroscopy: Techniques and applications in high magnetic fields, Rev. Sci. Instr. 80 (2009) 073102. 27 citácií
- S. Zhou, E. Čižmár, K. Potzger, M. Krause, T. Talut, M. Helm, J. Fassbender, S.A. Zvyagin, J. Wosnitza, H. Schmidt, Ferromagnetism in defective TiO2 single crystals, Phys. Rev. B 79 (2009) 113201. 120 citácií
- K. Siemensmeyer, E. Wulf, H.-J. Mikeska, K. Flachbart, S. Gabáni, S. Mat'aš, P. Priputen, A. Efdokimova, N. Shitsevalova, Fractional magnetization plateaus and magnetic order in the shastry-sutherland magnet TmB4, Phys. Rev. Lett. 101 (2008), 177201. 70+ citácií
- J.D.M. Champion, M.J. Harris, P.C.W. Holdsworth, A.S. Wills, G. Balakrishnan, S.T. Bramwell, E. Čižmár, T. Fennell, J.S. Gardner, J. Lago, D.F. McMorrow, M. Orendáč A. Orendáčová, D.M. Paul, R.I. Smith, M.T.F. Telling, A. Wildes, Er2Ti2O7: Evidence of quantum order by disorder in a frustrated antiferromagnet, Phys. Rev. B 68 (2003), 020401. 150+ citácií
- J. Černák, M. Orendáč, I. Potočňák, J. Chomič, A. Orendáčová, J. Skoršepa, A. Feher, Cyanocomplexes with one-dimensional structures: Preparations, crystal structures and magnetic properties, Coord. Chem. Rev. 224 (2002) 51-66. 300+ citácií

Doc. RNDr. Erik Čižmár, PhD. (45) absolvoval postdoka v USA a v Nemecku, venuje sa štúdiu kvantových magnetov a magnetickej rezonancii. Je spoluautorom 115 publikácií, ktoré získali 680+ citácií, h-index 16.

G5 Laboratórium fyziky nízkych teplôt

Inštitúcie: ÚEF SAV
Vedúci: Peter Skyba

Riešitelia: Marcel Človečko

Expertíza: Aparatúra jadrovej adiabatickej demagnetizácie umožňuje skúmať fundamentálne fyzikálne vlastnosti supratekutých fáz hélia-3 pomocou mechanických mikro a nanorezonátorov a rádiospektroskopických metód (NMR). Supratekuté hélium-3 je jedným z najčistejších modelových systémov. Dovoľuje simulovať fyzikálne procesy v kozmológii, astrofyzike, jadrovej fyzike a pod.

Najvýznamnejšie výsledky:

- M. Človečko, E. Gažo, S. Longauer, E. Múdra, P. Skyba, F. Vavrek, M. Vojtko, Vacuum Measurements of a Novel Micro-resonator Based on Tin Whiskers Performed at mK Temperatures, J. Low Temp. Phys. 175, 449 (2014)
- S. N. Fisher, G. R. Pickett, P. Skyba, N. Suramlishvili, Decay of persistent precessing domains in He-3-B at very low temperatures, Phys. Rev. B 86, 024506 (2012)
- P. Skyba, M. Kupka, BEC of magnons in superfluid He-3-B and symmetry breaking fields, Phys. Rev. B 85, 184529 (2012)
- M. Človecko, E. Gažo, M. Kupka, P. Skyba, New non-goldstone collective mode of BEC of magnons in superfluid (3)He-B, Phys. Rev. Lett. 100, 155301 (2008)
- R. Blaauwgeers, M. Blazkova, M. Človečko, V. B. Eltsov, R. de Graaf, J. Hosio, M. Krusius, D. Schmoranzer, W. Schoepe, L. Skrbek, P. Skyba, R. E. Solntsev, D. E. Zmeev, Quartz tuning fork: Thermometer, pressure- and viscometer for helium liquids, J. Low Temp. Phys. 146, 537 (2007)

RNDr. Peter Skyba, DrSc. (60) sa dlhodobo zaoberá fyzikou supratekutých fáz hélia-3. Je odborníkom na experimentálne metódy získavania ultranízkych teplôt a ich meranie s využitím spektroskopických metód (kontinuálna a impulzná jadrová magnetická rezonancia), ako aj s pomocou mechanických rezonátorov a iných techník. Je autorom 58 CC publikácií, na ktoré je viac ako 500 ohlasov, h-index 11.

G6 Laboratórium topologicky-chránených kvantových bitov

Inštitúcie: UPJŠ, ÚEF SAV,
Vedúci: Tomáš Samuely

Riešitelia: Vladimír Komanický, Pavol Szabo, Peter Samuely, Jozef Kačmarčík, Zuzana Vargaeštoková

Expertíza: Výskum a charakterizácia supravodivých materiálov makroskopickými experimentálnymi metódami. Príprava a charakterizácia supravodivých a magnetických nanoštruktúr pomocou skenovacích sondových mikroskopií.

Najvýznamnejšie výsledky:

- G. Zhang, T. Samuely, Z. Xu, J. K. Jochum, A. Volodin, S. Zhou, P. W. May, O. Onufriienko, J. Kačmarčík, J. A. Steele, J. Li, J. Vanacken, J. Vacík, P. Szabó, H. Yuan, M. B. J. Roeffaers, D. Cerbu, P. Samuely, J. Hofkens, and V. V. Moshchalkov, Superconducting Ferromagnetic Nanodiamond, ACS Nano 11, 5358 (2017)
- G. Zhang, T. Samuely, H. Du, Z. Xu, L. Liu, O. Onufriienko, P. W. May, J. Vanacken, P. Szabó, J. Kačmarčík, H. Yuan, P. Samuely, R. E. Dunin-Borkowski, J. Hofkens, and V. V. Moshchalkov, Bosonic Confinement and Coherence in Disordered Nanodiamond Arrays, ACS Nano 11, 11746 (2017)
- G. Zhang, S. Turner, E. A. Ekimov, J. Vanacken, M. Timmermans, T. Samuely, V. A. Sidorov, S. M. Stishov, Y. Lu, B. Deloof, B. Goderis, G. Van Tendeloo, J. Van De Vondel, and V. V. Moshchalkov, Global and local superconductivity in boron-doped granular diamond, Adv. Mater. 26, 2034 (2014).
- M. Timmermans, T. Samuely, B. Raes, J. Van De Vondel, and V. V. Moshchalkov, Dynamic visualization of nanoscale vortex orbits, ACS Nano 8, 2782 (2014).
- T. Samuely, S.-X. Liu, M. Haas, S. Decurtins, T. A. Jung, and M. Stöhr, Self-assembly of individually addressable complexes of C60 and phthalocyanines on a metal surface: Structural and electronic investigations, J. Phys. Chem. C (2009)
- P. Szabó, P. Samuely, J. Kačmarčík, A. G. Jansen, A. Briggs, A. Lafond, and A. Meerschaut, Interlayer transport in the highly anisotropic misfit-layer superconductor (LaSe)1.14(NbSe2), Phys. Rev. Lett. 86, 5990 (2001)

Mgr. Tomáš Samuely PhD (37) je odborník na skenovaciu tunelovú mikroskopiu a spektroskopiu supravodičov a nanoštruktúr pri nízkych teplotách a v ultravysokom vákuu. Doktorandské štúdium absolvoval na Univerzite v Bazileji, Švajčiarsku, neskôr absolvoval osemnásťmesačný postdoktorálny pobyt na KU Leuven v Belgicku. Je spoluautorom 23 CC publikácií s viac ako 200 citáciami, h-index 9.

G7 Laboratórium postkvantovej kryptografie

Inštitúcie: FEI STU, MÚ SAV
Vedúci: Pavol Zajac

Riešitelia: Otokar Grošek, Karol Nemoga, Tomáš Fabšič

Expertíza: Návrh a implementácia bezpečných kryptografických primitív a protokolov. Kryptoanalýza a matematická kryptografia. Praktická postkvantová kryptografia.

Najvýznamnejšie výsledky:

- T. Fabšič, V. Hromada, P. Stankovski, P. Zajac, Q. Guo, T. Johansson: A reaction attack on the qc-ldpc mceliece cryptosystem, International Workshop on Post-Quantum Cryptography, 51-68 (2017)
- T. Fabšič, O. Grošek, K. Nemoga, P. Zajac: On generating invertible circulant binary matrices with a prescribed number of ones, Cryptography and Communications 10 (1), 159-175 (2018)
- P. Zajac, Upper bounds on the complexity of algebraic cryptanalysis of ciphers with a low multiplicative complexity, Designs, Codes and Cryptography 82 (1-2), 43-56
- P. Zajac, A new method to solve MRHS equation systems and its connection to group factorization, Journal of Mathematical Cryptology 7 (4), 367–381 (2013)
- P. Horak, O. Grošek, A new approach towards the Golomb–Welch conjecture, European Journal of Combinatorics 38, 12-22 (2014)

Prof. Ing. Pavol Zajac, PhD (38) sa venuje praktickej kryptografii, kryptoanalýze a implementáciám post-kvantovej kryptografie. Je spoluautorom 20 CC publikácií s viac ako 34 citáciami, h-index 4.

G8 Skupina kvantového počítania a algoritmov

Inštitúcie: UPJŠ
Vedúci: Martin Gmitra

Riešitelia: Jozef Strečka, Gabriel Semanišin, Ondrej Hutník, Zuzana Bednárová, Ondrej Krídlo

Expertíza: Výpočet mier kvantového previazania, nelokálnosti a spoľahlivosti teleportácie. Návrh a implementácia kvantových algoritmov a počítania.

Najvýznamnejšie výsledky:

- W. Han, R. K. Kawakami, M. Gmitra, J. Fabian: Graphene spintronics, Nature Nanotechnology 9, 794–807 (2014), 480+ citácií
- J. Strečka, O. Rojas, T. Verkholyak, M.L. Lyra, Magnetization process, bipartite entanglement, and enhanced magnetocaloric effect of the exactly solved spin-1/2 Ising-Heisenberg tetrahedral chain, Phys. Rev. E 89, 022143 (2014).
- J. Strečka, R.C. Alécio, M.L. Lyra, O. Rojas, Spin frustration of a spin-1/2 Ising–Heisenberg three-leg tube as an indispensable ground for thermal entanglement, J. Magn. Magn. Mater. 409, 124-133 (2016).
- M. Hutníková, O. Hutník, Affine coherent states and Toeplitz operators, J. Phys. A: Math. Theor. 45(24) (2012), art. no 244021.
- O. Hutník, E. Maximenko, A. Mišková, Toeplitz localization operators: spectral functions density, Compl. Anal. Oper. Theory 10(8) (2016), 1757-1774.
- Ondrej Krídlo, Manuel Ojeda-Aciego, Formal Concept Analysis and Structures Underlying Quantum Logics, International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems, IPMU 2018: Information Processing and Management of Uncertainty in Knowledge-Based Systems. Theory and Foundations pp 574-584
- Ondrej Kridlo and Manuel Ojeda-Aciego, Relating Hilbert-Chu Correspondences and Big Toy Models for Quantum Mechanics, Accepted to book Computational Intelligence and Mathematics for tackling complex problems.

RNDr. Martin Gmitra, PhD. (40) postdok Univerzita A. Mickiewicza v Poznani Poľsko (Marie Curie fellow), postdok na Univerzite v Regensburgu, Nemecko (spoluriešiteľ SFB projektov), spoluautor 87 publikácii, 2100 citácií, h-index 17.

POĎAKOVANIE

Naše poďakovanie patrí Ministerstvu školstva, vedy, výskumu a športu Slovenskej republiky za iniciovanie Platformy QUTE a podpore pri vypracovaní tohoto materiálu. Autori ďakujú za pripomienky, spoluprácu a cenné rady všetkým členom Správnej rady platformy. Špeciálna vďaka patrí najmä Petrovi Staňovi, Gabrielovi Semanišinovi, Danielovi Reitznerovi, Anne Jenčovej, Pavlovi Zajacovi, Erikovi Čižmárovi a Petrovi Skybovi, ktorí svojou vecnou kritikou a návrhmi výraznou mierou prispeli ku konečnej podobe Akčného plánu.