Кам’янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет
Кафедра фізики

Дипломна робота

магістранта

на тему: **"Квантова телепортація та її практичне застосування"**

Виконав: студент 2 курсу, групи F1-M18
спеціальності 014 Середня освіта "Фізика"
Корнійчук Андрій Вікторович

Керівник: кандидат фізико – математичних наук, доцент, доцент кафедри фізики
Поведа Р.А.

Рецензент: кандидат педагогічних наук, доцент кафедри МВФ та ДТОГ
Білик Р.М.

м. Кам’янець-Подільський – 2019 рік

ЗМІСТ

ВСТУП

Квантова фізика — це теорія атомних явищ, яка вивчає закономірності мікросвіту, а також дає означення та поняття про рух елементарних частинок, ядер, атомів та молекул. За допомогою даного вчення можна з'ясувати природу фізичного зв'язку, пояснити та дослідити періодичну систему. Саме за допомогою квантової механіки виникли такі поняття, як феромагнетизм, надпровідність та надплинність.

Впродовж XX століття завдяки працям багатьох видатних фізиків (М.Планка, А.Ейнштейна, Н.Бора, пізніше де Бройля, Гейзенберга, Е.Шредінгера та інших) квантова фізика значно зросла в своїх обсягах та посіла важливе місце у житті людства.

Квантова фізика має міжпредметні зв'язки з біологією, хімією, астрономією та ін.. При вивченні зір та Всесвіту необхідний квантово-механічного опису фізичних процесів, що там відбуваються. В біології необхідною є при вивченні явищ, на молекулярному рівні.

На сучасному рівні квантова фізика - наш світогляд і наше розуміння Природи. Поширення та зацікавленість набуває квантова інформатика, що включає в себе такі розділи: квантова криптографія, квантова телепортація, квантові обчислення та інші.

Сьогодні дослідження в галузі квантової криптографії проводять багато дослідників, особливо потужних компаній: Toshiba, Mitsubishi, IBM, ID Quantique; навчальних закладів: технологічний інститут в Каліфорнії, лабораторія в Лос-Аламосі.

ID Quantique виготовляють обладнання квантового розподілу ключів та встановлюють його банкам, корпораціям та іншим відповідним компаніям.

Актуальність полягає в тому, що за допомогою вдосконалення квантових обчислень можна створити абсолютно новий тип обчислювальних механізмів.

Наприклад, квантова криптографія, яка дозволить гарантовано секретне передавання інформації та більш віддалена ціль — квантовий комп’ютер, що вирішить завдання з великою складність, за короткий термін, що навіть не характерне для сучасного потужного персонального комп’ютера. Дані, що передаватимуться таким комп’ютером, неможливо скопіювати та присвоїти. Це рішення зменшить затрати на створення засобів захисту інформації, засобів несанкціонованого доступу та ін.. Даний пристрій дозволить оперувати велику кількість інформації, що навіть важко уявити, порівнюючи з його фізичним розміром, інше завдання, з яким впорається квантовий комп’ютер — це моделювання квантових систем і молекул ДНК.

Предмет: формування та розширення знань **з** квантово розмірних вимірювань в сучасному світі.

Об'єкт: процес дослідження квантово розмірних вимірювань на сучасному етапі, аналіз останніх результатів та перспективи надсучасних винаходів.

Тема: ″ Квантова телепортація та її практичне застосування ″.

Ідея. Розглянути застосування на практиці квантово-розмірних досліджень:

1. ідеї розвитку досліджень відомими фізиками;
2. при виготовленні квантових комп’ютерів;
3. при застосування телепортації в крипто зв’язку;
4. в природі та сучасній електроніці.

Для досягнення мети роботи відповідно до гіпотези дослідження необхідно вирішити наступні **завдання:**

1. Проаналізувати літературу, виявити стан проблеми.

2. Позначити теоретичні основи дослідження.

3. Проаналізувати становлення квантової фізики та проблеми під час досліджень.

4. Пошук прийнятних рішень, що дозволять застосовувати квантові криптографічні методи, для передачі інформації без змоги її перехоплення,

використовуючи при цьому спеціальні ключі.

Наукова новизна дослідження і теоретична значущість дослідження полягають у наступному:

- уточнені поняття «квантово-розмірні виміри», «квантові комп’ютери», «крипто-зв'язок» та ін.;
- впровадження досліджень квантової фізики кардинально змінить напрям розвитку цивілізації та життя кожної людини;
- створить прорив в науці.

ВИСНОВКИ

Завдяки цій чудовій теорії, яка незабаром стала окремою наукою, ми отримали можливість досліджувати навколишню дійсність на рівні субатомних частинок. Це дрібний рівень з усіх можливих, абсолютно недоступний для нашого сприйняття. Що фізики раніше знали про наш світ, потребує термінового перегляду. З цим згодні абсолютно всі. Стало очевидно, що різні частинки можуть взаємодіяти один з одним на абсолютно немислимих відстанях, які ми можемо вимірювати лише шляхом складних математичних формул.

Крім того, квантова механіка (і квантова фізика) довела можливість існування безлічі паралельних реальностей, подорожей у часі і інших речей, які протягом всієї історії вважалися лише долею наукової фантастики. Це, безсумнівно, величезний вклад не тільки в науку, а й в майбутнє людства.

Отже, сьогодні квантовий комп’ютер та інші квантові технології це лише певні розробки, на початковій стадії. Якщо вчені створить повноцінний квантовий комп’ютер, це забезпечить прорив в науці, адже це найшвидша обчислювальна машина. Помилки в їх створення істотно просуваються, наближаючи момент, коли вже створиться надійній комп’ютер. Даний комп’ютер буде виконувати серйозні алгоритми, наприклад алгоритм Шора. Отже, слід очікувати, що повноцінний квантовий комп’ютер таки з’явиться, що відправить персональні комп’ютера на другий рівень.

Перешкодами в квантовій криптографії являються невеликі відстані, на які можна передавати інформацію, а також значна вартість та громіздкість обладнання. Для вирішення даної проблеми було вирішено створити повітряно-оптоволоконну систему, що буде використовувати супутниковий зв'язок. Використання штучних супутників для передачі фотонів через повітря відкриває можливість забезпечення секретними ключами клієнтів у будь-якій точці Землі. Технології квантової криптографії постійно вдосконалюються, адже програмісти та хакери постійно знаходять слабкі місця в системах

захисту, постійно з’являється інформація про випадку злому. Деякі методи та засоби квантової криптографії є запатентованими у різних країнах, що певне будуть реалізовані найближчим часом. Також питання щодо безпеки квантових ключів є активною сферою для дослідження, що привертають увагу багатьох дослідників.

Пост-квантові системи розвиваються набагато повільніше, однією із причин є те, що існує протиріччя «крипостійкі теоретично» і «крипостійкі практично» між системами асиметричного шифрування на основі задач теорії ґраток, що відкриває перспективний напрямок фундаментальних і прикладних математичних досліджень в галузі пост-квантової криптографії.

Квантові обчислення взяли свій початок в теоретичній фізиці, але їх майбутнє матиме великий вплив на наше суспільство. Сьогоднішній стан в дослідження нагадують 90-ті роки, коли лишень зароджувалась мережа Інтернет. У той час був виявлений лишень потенціал, який досягнув великого успіху.

В деяких системах телепортація зараз є просто інструментом, що використовується для виконання складніших завдань, для інших, що виникають, технологій залишаються виклики при підготовці та об'єднанні декількох квантових систем. Тим не менш, будь то комунікація чи обчислення, телепортація відіграє ключову роль у багатьох програмах, які обіцяють квантову перевагу, тобто надання того, що неможливо зробити класично, і це все вплине на суспільство, зокрема, на розділ про безпеку квантового спілкування. Сьогодні телепортація стала потужним інструментом, який застосовується щодня в лабораторіях по всьому світу та з деякими демонстраціями у реальних волоконних мережах. Завдання полягає в тому, щоб адаптувати це до нових технологій, що застосовуються для квантових ретрансляторів, щоб розширити відстані, на які ми можемо розподілити заплутаність та квантові ресурси.

Перші зразки на основі ядерного магнітного резонансу є усього лише лабораторними експериментами. Вдосконалені, вони, швидше за все,

використовуватимуться як співпроцесори для вирішення специфічних завдань, таких, як складні математичні проблеми, моделювання квантових систем і здійснення неструктурованого пошуку. Редагування тексту або рішення простих завдань набагато легше виконуються сучасними комп'ютерами. Проте, очевидно і те, що рано чи пізно, у міру подальшого зменшення розмірів, комп'ютерам нічого не залишиться зробити, як узяти на озброєння квантові технології - або лише для доповнення традиційних методів і прийомів, або ж для повної заміни нинішніх обчислювальних технологій.

"Квантова фізика відкриває двері не просто для мініатюрніших і швидкодіючих мікропроцесорів. Вона веде до принципово інших способів обчислень, які не можуть бути реалізовані в нинішніх комп'ютерах", - вважає Артур Экерт, глава Центру квантових обчислень Оксфордського університету. Своя думка про перспективи масового переходу людства до принципово інших технологій професор Дэвид Дойч (David Deutsch) з того ж центру, один з піонерів теорії квантових обчислень, виразив таким чином. Теорія класичних універсальних обчислень, відмічав він, була закладена Т'юрингом в 1936 році, отримала практичне втілення впродовж наступного десятиліття, в 1950-і набула комерційної цінності і спрямованості, а домінуючим чинником світової економіки стала до кінця 1980-х. Квантова інформаційна технологія є фундаментально новим способом використання можливостей природи.

На думку багатьох учених, працюючих в області квантового комп’ютера, результати наукових розробок наблизяться до стадії комерційного застосування приблизно до 2020 р.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вакарчук І. О. Найпростіші задачі квантової механіки // Квантова механіка. – 4. – Львів : ЛНУ імені Івана Франка, 2012. – 872 с.

2. Федорченко А. М. Квантова механіка, термодинаміка і статистична фізика // Теоретична фізика. – К. : Вища школа, 1993. – Т. 2. – 415 с.

3. Кучерук І. М., Горбачук І. Т.; за ред. Кучерука І. М. Загальний курс фізики. Том 3. (1999).pdf

4. Вікіпедія [Електронний ресурс]: – Режим доступу: https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D1%82_%D0%A8%D1%80%D0%B5%D0%B4%D1%96%D0%BD%D0%B3%D0%B5%D1%80%D0%B0 (дата звернення 13.07.2019).

5. Оленич І.Б. Фізичні основи нанотехнологій : навч. посібник / І. Б. Оленич. — Львів : ЛНУ імені Івана Франка, 2014. — 232 с.

6. Горячко А. М., Кулик С. П., Прокопенко О. В. Основи скануючої зондової мікроскопії та спектроскопії (Частина 1): Навчальний посібник. – К.: Радіофізичний факультет Київського національного університету імені Тараса Шевченка, 2011. – 133 с.

7. Анго А. Математика для электро- и радиоинженеров. – М.: Наука, 1967. – 780 с.

8. Квантова механіка та її використання у прикладній фізиці: підручник / В.І. Висоцький. — К.: Видавничо-поліграфічний центр "Київський університет", 2008. — 367 с.

9. E. Romero et al. Quantum coherence in photosynthesis for efficient solar-energy conversion // Nature Physics. 2014. Advanced online publication. DOI: 10.1038/nphys3017.

10. F. D. Fuller et al. Vibronic coherence in oxygenic photosynthesis // Nature Chemistry. 2014. Advanced online publication. DOI:10.1038/nchem.2005.

11. Науковий журнал Scientific Advances [Електронний ресурс]: – Режим доступу: https://advances.sciencemag.org/content/5/7/eaaw2563 (дата звернення

13.07.2019).

12. Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / С. П. Кулик, Е.А. Шапиро (пер. с англ.); С. П. Кулик, Т. А. Шмаонов (ред. пер.); Д. Боумейстер и др. (ред.). – М.: Постмаркет, 2002. – 358с.

13. Столлингс В. Криптография и защита сетей: принципы и практика, – 2- е изд.: Пер. с англ. – М.: ИД «Вильямс», 2001. – 672 с.

14. IDQ [Електронний ресурс]: [Інтернет-портал]. – Електронні дані. – [Швейцария: Женева: ID Quantique, 2001-2015]. — Режим доступу: http://wpidq.cremarc.com/.

15. MagiQ [Електронний ресурс]: [Інтернет-портал]. — Електронні дані. – [США: Нью-Йорк: Magiq Technologies, 1999—2015]. — Режим доступу: http://www.magiqtech.com/.

16. Los Alamos National Laboratory [Електронний ресурс]: [Інтернетпортал]. – Електронні дані. – [США, Лос-Аламос: Los Alamos National Laboratory, 1943-2015]. – Режим доступу: http://www.lanl.gov/projects/feynman-center/technologies/informationtechnology-communications/qkard-quantum-smart-card.php.

17. Вікіпедія [Електронний ресурс]: – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BB%D0%B0%D1%83%D1%80%D0%B5%D0%B0%D1%82%D1%96%D0%B2_%D0%9D%D0%BE%D0%B1%D0%B5%D0%BB%D1%96%D0%B2%D1%81%D1%8C%D0%BA%D0%BE%D1%97_%D0%BF%D1%80%D0%B5%D0%BC%D1%96%D1%97_%D0%B7_%D1%84%D1%96%D0%B7%D0%B8%D0%BA%D0%B8.

18. [Електронний ресурс]: — Режим доступу: An Atomic Clock with 10-18 Instability (N. Hinkley, J. A. Sherman, N. B. Phillips, M. Schioppo, N. D. Lemke, K. Beloy, M. Pizzocaro, C. W. Oates, A. D. Ludlow) / Published Online August 22 2013. Science 13 September 2013: Vol. 341, no. 6151, pp. 1215–1218/

19. Сверим часы. Краткая история появления атомных приборов измерения времени / Лента.ру, 11 апреля 2014, 10:45 [Електронний ресурс]: – Режим доступу: https://lenta.ru/articles/2014/04/11/atcl/.

20. PNAS. [Електронний ресурс]: – Режим доступу: https://www.pnas.org/content/113/3/532.full

21. Aharonov Y, Rohrlich D(2008) Quantum Paradoxes: Quantum Theory for the Perplexed

22. Einstein Podolsky Rosen (1935) Can quantum-mechanical description of physical reality be considered complete? Phys Rev 47:777–780.

23. Bell JS (2001) Einstein-Podolsky-Rosen experiments. John S Bell on the Foundations of Quantum Mechanics (World Scientific, Singapore), pp 74–83.

24. Bennett CH, et al. (1993) Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett 70:1895

25. Raussendorf RBriegel (2001) A one-way quantum computer. Phys Rev Lett 86:5188–5191.

26. Kimble (2008) The quantum internet. Nature 453:1023–1030.

27. Science Ukraine. [Електронний ресурс]: – Режим доступу: https://scienceukraine.com/allnews/physics-and-tech/cybernetics/quantum-internet-to-come/.

28. Гейзенберг Вернер. Физика и философия. Часть и целое. – М.: Наука. Главная редакция физико-математической литературы, 1989, с. 174.

29. A. I. Miller. Werner Heisenberg and the Beginning of Nuclear Physics // Physics Today. – 1985. – Vol. 38, № 11. – P.60-68.

30. PAM Dirac, Proc. Рой. Соц. A, 109642, (1925).

31. Дж. Фон Нойман, Mathematische Grundlagen der Quanten-Mechanik, Springer-Verlag, Берлін, 1932.

32. Trixler, F (2013). "Quantum tunnelling to the origin and evolution of life". Current Organic Chemistry 17 (16): 1758–1770. [Електронний ресурс]: – Режим доступу: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3768233/.

33. Cooper, WG (June 1993). Roles of Evolution, Quantum Mechanics and Point Mutations in Origins of Cancer. Cancer Biochemistry Biophysics 13 (3): 147–70. [Електронний ресурс]: – Режим доступу: https://www.ncbi.nlm.nih.gov/pubmed/8111728.

34. Taylor, J. (2004). Modern Physics for Scientists and Engineers. Prentice Hall. p. 479.

35. Crépeau, Claude; Joe, Kilian (1988). Achieving Oblivious Transfer Using Weakened Security Assumptions (Extended Abstract). FOCS 1988. IEEE. pp.42-52.

36. Kilian, Joe (1988). Founding cryptography on oblivious transfer. STOC 1988. ACM. pp. 20–31. Archived from the original on 24 December 2004.

37. Brassard, Gilles; Claude, Crépeau; Jozsa, Richard; Langlois, Denis (1993). A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties. FOCS 1993. IEEE. pp. 362-371.

38. Daniel J. Bernstein. "Introduction to post-quantum cryptography". Post-Quantum Cryptography. [Електронний ресурс]: – Режим доступу: http://www.pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf.

39. Daniel J. Bernstein."Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?" [Електронний ресурс]: – Режим доступу: http://cr.yp.to/hash/collisioncost-20090823.pdf.

40. Watrous, John (2009). "Zero-Knowledge against Quantum Attacks". SIAM Journal on Computing 39(1): 25-58.

41. Thapliyal, K.; Pathak, A. (2018). "Kak's three-stage protocol of secure quantum communication revisited". Quantum Information Processing.17 (9).