КВА́НТОВА ТЕО́РІЯ ІНФОРМА́ЦІЇ — когнітивна дисципліна на межі фізики, математики й інформатики, що вивчає процеси передавання та оброблення інформації з урахуванням квантової природи її носія, а також фізичні процеси та пристрої, необхідні для цього. Розділи К. т. і.: квантова переплутаність, телепортація квантових станів, квантові канали, квантова криптографія, корекція помилок, квантовий комп'ютер і квантові обчислення. Вперше ідею про можливість використання квантових властивостей носіїв інформації для прискорення обчислень висловив у 1980-х рр. амер. фізик Р.-Ф. Фейнман. Він запропонував використати складність квантових систем, яка унеможливлює їхній опис за допомогою класичних комп'ютерів, для пришвидшення оброблення класичної інформації. Важливе значення для створення К. т. і. мали праці, опубліковані у 2-й пол. 1980-х — на поч. 90-х рр., англ. фізика Д. Дойча й амер. фахівців у галузі інформатики Е. Бернштейна та В.-В. Вазірані, в яких на рівні принципів доведено універсальність квантової машини Тьюрінґа (математичне поняття абстрактного еквівалента алгоритму, або обчислюваної функції, яке увів 1936–37 англ. математик А.-М. Тьюрінґ), тобто її здатність виконувати довільне унітарне перетворення за допомогою обмеженого набору логічних операцій. Згодом амер. вчені П. Шор і Л. Ґровер розробили алгоритми, які повністю використовують квантову інтерференцію та переплутаність для суттєвого (порівняно з класичним) прискорення обчислень. Значний прогрес у К. т. і. наприкінці 20 — на поч. 21 ст. пов'язаний з розвитком методів і технологій квантової фізики, які дозволили маніпулювати окремими мікроскопічними частками, створювати та контролювати когерентні квантові стани в макроскопічних системах (Бозе–Айнштайнівські конденсати атомів, надпровідні системи тощо). Це призвело до експериментальної реалізації кубітів (квантових носіїв інформації) на різних системах і демонстрації можливості виконання основних квантових алгоритмів.

Основним поняттям К. т. і. є поняття переплутаності квантових станів. Вона виявляється в кореляції виміряних станів двох (або більше) квантових систем, причому ці кореляції не залежать від відстані між окремими системами. Переплутані стани не мають аналогів у класичній фізиці та вважаються головним ресурсом, який забезпечує можливість передавання квантової інформації (телепортації станів) і пришвидшеного її оброблення (квантовий паралелізм). Квантова телепортація використовує квантові кореляції для передавання в іншу точку простору невідомого квантового стану без переміщення носія інформації. Реалізація квантових алгоритмів вимагає виконання т. зв. непримітивних операцій, унаслідок яких створюються переплутані стани. Логічні операції над переплутаними станами дозволяють за невелику кількість кроків обробляти великі масиви даних і в такий спосіб забезпечувати паралельність обчислень. Переплутаність використовують і під час виправлення (корекції) помилок при квантових обчисленнях. Оскільки вимірювання (зчитування інформації) руйнує квантовий стан, то детектування помилки здійснюють за допомогою квантових кореляцій, що виникають між основним і допоміжним кубітом. Експериментальна перевірка існування переплутаних станів призвела до виникнення квантової криптографії. Її становлення пов'язують з іменами амер. фізика Ч. Беннетта, канад. фізика Ж. Брассарда та польс. і амер. фізика А.-К. Екерта (йому належить одна з перших праць у цій галузі).

У криптографії квантові кореляції застосовують як для розподілу секретної інформації між двома легітимними користувачами, так і в теорії, для аналізу захищеності протоколів відносно атак зловмисників. Визначення міри переплутаності для систем із більш ніж двома складовими, а також для зашумлених систем, що знаходяться в т. зв. мішаних станах, є окремою задачею К. т. і. Фундаментальні розроблення в цьому напрямі належать школі польських фізиків Городецьких. Існує думка, що визначення принципових обмежень на переплутаність, яку можна вивільнити для оброблення інформації, дасть змогу сформулювати постулати К. т. і. за аналогією з постулатами термодинаміки. Нині основною проблемою К. т. і. вважається подолання т. зв. квантової прірви — перехід від вже реалізованих комп'ютерів з 5–10 кубітами до машини, яка може створювати суперпозиційні та переплутані стани 1000 кубітів і виконувати (до розпаду стану) не менше 10^9 операцій. Дослідження з К. т. і. проводять в низці університетів і дослідницьких лабораторій світу. У Каліфорнійському інституті технологій (США) функціонує окремий Інститут К. т. і. Провідні вчені у цій галузі працюють в університетах і інститутах Німеччини (напр., в Університеті Ганновера) та Нідерландів, компаніях IBM, Google (обидві — США). На теренах колишнього СРСР проблеми К. т. і. активно вивчають в Білорусі (С. Кілін) та РФ (К. Валієв).

В Україні квантовою інформатикою вперше почали займатися у Фізико-технічному інституті низьких температур НАНУ (Харків; *В. Шнирков*, *О. Омельянчук*, *С. Шевченко*), де розроблено кубіт на основі джозефсонівських контактів із високим часом декогеренції. Розроблення в галузі квантових

алгоритмів виконано в Інституті проблем математичних машин і систем НАНУ (Київ; А. Бєляєв). К. т. і. також розвивають науковці Інституту фізики НАНУ (А. Семенов), Нац. авіац. університету (С. Гнатюк; обидва — Київ), Одес. академії зв'язку (Є. Василіу). Університетський курс із К. т. і. вперше розробив Дж. Прескіл із Каліфорнійського інституту технологій. Нині такі курси викладають майже в кожному університеті Європи та США. В Україні курс квантової інформатики започатковано у Фізико-технічному інституті Нац. тех. університету України «Київ. політех. інститут» (О. Гомонай), пізніше введено на фізичному і кібернетичному ф-тах Київ. університету, фізичному факультеті Таврій. університету (Сімферополь).

Рекомендована література

1. R. Feynman. Quantum mechanical computers, Simulating Physics with Computers, Keynote talk // International J. Theoretical Physics. 1982. Vol. 21;
2. D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer // Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences. 1985. Vol. 400;
3. R. Feynman. Tiny Computers Obeying Quantum Mechanical Laws // New Directions in Physics: The Los Alamos 40th Anniversary Volume. Orlando, 1987;
4. A. Ekert. Quantum cryptography based on Bell's theorem // Phys. Rev. Lett. 1991. Vol. 67;
5. E. Bernstein, U. Vazirani. Quantum complexity theory // Proceedings of the 25'th Annual ACM Symposium on the Theory of Computing. New York, 1993;
6. P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring // Proceedings of the 35'th Annual Symposium on Foundations of Computer Science. Los Alamitos, 1994;
7. J. I. Cirac, P. Zoller. Quantum Computations with Cold Trapped Ions // Phys. Rev. Lett. 1995. Vol. 74;
8. C. H. Bennett, P. W. Shor. Quantum information theory // Transactions on Information Theory. 1998. Vol. 44;
9. M. Horodecki, P. Horodecki, R. Horodecki. Unified Approach to Quantum Capacities: Towards Quantum Noisy Coding Theorem // Phys. Rev. Lett. 2000. Vol. 85;
10. M. A. Nielsen, I. L. Chuang. Quantum computation and quantum information. Cambridge, 2000;
11. Валиев К. А., Кокин А. А. Квантовые компьютеры: надежды и реальность. Москва, 2001;
12. Гомонай О. В. Лекції з квантової інформатики. В., 2006;
13. Квантовая криптография: идеи и практика. Минск, 2008;
14. V. I. Shnyrkov, D. Born, A. A. Soroka, W. Krech. Coherent Rabi response of a charge-phase qubit under microwave irradiation // Phys. Rev. B. 2009. Vol. 79.

О. В. Гомонай

Бібліографічний опис:
Квантова теорія інформації / О. В. Гомонай // Енциклопедія Сучасної України [Електронний ресурс] / Редкол.: І. М. Дзюба, А. І. Жуковський, М. Г. Железняк [та ін.] ; НАН України, НТШ. — К. : Інститут енциклопедичних досліджень НАН України, 2012. — Режим доступу: https://esu.com.ua/article-11530