42. Квантові комп’ютери та можливі їх застосування в криптології?

Робота окремих елементів квантового комп'ютера описується законами квантової фізики. Для звичайних обчислень(комп’ютера) стан окремого біта та передбаченністю результату операції над ним. Причому визначення стану біта (фізичне вимірювання) не впливає на його стан, різні фізичні реалізації логічної операції призводять до однакової зміни стану біта, і це робить можливим розглядати процес обчислень на класичному комп'ютері незалежно від його апаратного втілення.

В основі ж квантової механіки лежить *принцип невизначеності Гейзенберга* та ймовірностний характер станів окремих елементів, а також знищення стану квантового об'єкта (біта) при визначенні стану(вимірюванні)), що, здається, знаходиться в повному протиріччі із вимогою повної визначеності, однозначності та зворотності комп'ютерних операцій.

Однак, на початку 80-х Полю Беньоффу, Річарду Фейнману та Давіду Дейчу вдалось поєднати дві дисципліни, що досі вважались взаємовиключними, — квантову фізику та інформатику. Вони показали, що квантова теорія не тільки не обмежує обчислювальних можливостей, але дозволяє суттєво їх розширити. Беньофф висловив ідею універсального квантового комп'ютера — машини, яка здійснює логічні операції, спираючись на квантові алгоритми, що не мають аналогів в класичній фізиці; Фейнман показав, що квантовий комп'ютер повинен бути більш потужнім, аніж класичний, а Д. Дейч запровадив ідею квантового паралелизму, що описує здатність квантового комп'ютера працювати із квантовою суперпозицією чисел. Тим самим ці вчені заклали фундамент нової сучасної галузі досліджень — квантових інформаційних технологій, або квантової інформатики.

На початку 90-х квантова інформатика набула прикладного змісту завдяки роботам Екерта, Беннета та групи з Женевського університету. Виявилось, що такі "недоліки" квантового об'єкту, як можливість одночасного перебування у сукупності станів та суттєвий вплив процесу вимірювання на стан об'єкта, відкривають нові можливості в криптографії.

Досягнення фізики останніх років (бозе-ейнштейнівська конденсація атомів газу, квантовий ефект Хола, штучні періодичні структури – квантові точки, колодязі, тощо), а також розвиток лазерних та оптоволоконних технологій зробили можливим реалізацію найближчим часом квантового комп'ютера. На сьогодні квантова інформатика вбирає в себе досягнення різних дисциплін — фізики, теорії інформації, обчислювальних методів, телекомунікацій, матеріалознавства, тощо, і переживає період бурхливого розвитку, який можна порівняти тільки із розвитком ідей квантової фізики на кінці 19-го - початку 20-го сторіччя.

Квантова інформатика в повній мірі використовує властивості квантових об'єктів, такі, як здатність однієї частки перебувати в кількох станах одночасно (суперпозиція станів об'єкта), здатність системи із кількох часток перебувати в корельованиих (переплутаних) станах і пов'язана з цим

нелокальність, суттєвий вплив процесу вимірювання на стан об'єкта, неможливість клонування квантових станів.

Криптографія являє собою один із напрямків криптології –науки, що займається проблемами захисту інформації шляхом її перетворення. Основні напрямки застосування криптографічних методів – передача конфіденційної та достовірної інформації по каналах зв'язку (наприклад, через електронну мережу), встановлення достовірності та автентичності (достеменності) повідомлення, що передається, зберігання інформації (документів, баз даних) на носіях в зашифрованому вигляді, тощо.

Серед проблем, які вирішує криптографія, найбільш вразливою завжди була проблема розподілу ключів. Найскладнішою є вимога забезпечення абсолютної секретності ключа — навіть при передачі ключа по закритим каналам не виключена можливість непомітного для довірених сторін несанкціонованого втручання в канал сторонніх осіб (порушників).

Квантова криптографія значно полегшує задачу секретної передачі інформації.

Вона вирішує проблему розподілу ключів, використовуючи властивість квантових систем змінювати свій стан в процесі вимірювання та неможливість клонування квантових станів. Процес "підслуховування" передбачає можливість копіювання (відтворення) стану носія інформації, що в разі передачі інформації за допомогою суто квантових об'єктів неможливо. Отже, будь-яка спроба несанкціонованого втручання в канал передачі інформації буде виявлена.

Основні фундаментальні властивості квантових систем, які використовуються в квантовій криптографії :

1) Вимірювання фізичних характеристик квантових систем (спостережуваних).

У результаті процесу вимірювання деякої фізичної величини стан квантової системи змінюється. Це обумовлено впливом на квантовий об'єкт вимірювального приладу, який принципово неможливо зробити як завгодно слабким. Чим точніше вимірювання, тим сильніший вплив, що воно здійснює, і лише при вимірюваннях дуже малої точності вплив на об'єкт вимірювання може бути досить слабким.

Крім того, збурювання, яке вноситься взаємодією квантового об'єкта з вимірювальним приладом, може бути передбачено тільки статистично й тому не може бути виключено. Цей факт перебуває в різкому протиріччі із

класичною теорією вимірювань, яка базується на припущенні, що взаємодія між об'єктом і приладом якщо й не може бути зроблена як завгодно малою, то принаймні може бути точно врахованою й, отже, у принципі її можна виключити.

2) Неможливість точного клонування невідомих квантових станів (теорема про заборону клонування).

Внаслідок лінійності й унітарності квантової механіки, неможливо створити точну копію невідомого квантового стану. Таким чином, зловмисник не може виготовити точну копію кубітів або кудитів, що передаються по комунікаційному каналу, щоб провести вимірювання над копією, а оригінал переслати законному користувачеві каналу, не проводячи над ним вимірювання. Цей факт лежить в основі більшості протоколів квантової криптографії, тому що змушує зловмисника вимірювати передавані кудити, або переплутувати їх зі своїми допоміжними квантовими системами, що призводить до зміни станів цих кудитів. Ці зміни передаваних станів можуть виявити законні користувачі, виконуючи квантові вимірювання й обмінюючись результатами цих вимірювань по звичайному відкритому каналу зв'язку. Відзначимо, що ймовірність правильно клонувати довільний стан кубіту, створивши одну його копію, дорівнює 5/6. Якщо потрібно створити n копій невідомого стану кубіту, то ймовірність правильного клонування зменшується та при $n \to \infty$ прямує до 2/3.

3) Неортогональні квантові стани неможливо розрізнити.

Квантова система із двома станами – кубіт – може перебувати не тільки в базисних станах $|0\rangle$ та $|1\rangle$ (які відповідають, наприклад, вертикальній та горизонтальній поляризації окремого фотону), але й у стані лінійної суперпозиції

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

де α й β – комплексні числа, що задовольняють умові $|\alpha|^2 + |\beta|^2 = 1$. Вимірюючи стан кубіту, ми знайдемо, що кубіт з імовірністю $|\alpha|^2$ несе значення "0", а з імовірністю $|\beta|^2$ – значення "1".

Внаслідок законів квантової механіки неможливо виконати вимірювання, що дозволило б розрізнити стани $|\Psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ та $|\Psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$, крім випадку, коли скалярний добуток $\langle\Psi_1|\Psi_2\rangle = 0$, тобто стани $|\Psi_1\rangle$ й $|\Psi_2\rangle$ ортогональні.

Аналогічно, вимірюючи довільний стан кутриту

$$|\Phi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle,$$

ми отримаємо "0" з імовірністю $|\alpha|^2$, "1" з імовірністю $|\beta|^2$ та "2" з імовірністю $|\gamma|^2$.

Відзначимо, що суперпозиція квантових станів не має аналога в класичній фізиці.

4) Переплутування (квантові кореляції).

Дві або більше квантових системи можуть бути переплутані.Так, пара фотонів у синглетному поляризаційному стані

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 - |0\rangle_2|1\rangle_1\right),$$

де індекси позначають номери фотонів, –це приклад максимально переплутаного стану двох кубітів. Такий стан називають парою Ейнштейна–Подольського–Розена (ЕПР-парою).

Якщо вимірювання виконується над одним із двох переплутаних кубітів в стані $|\Psi^-\rangle$ (1.3), наприклад, в базисі $\{|0\rangle,|1\rangle\}$, який називається обчислювальним базисом, то результат буде "0" або "1" з однаковою ймовірністю 1/2. Стан другого кубіту антикорельований з першим, тобто якщо перший кубіт в результаті вимірювання перейшову стан $|0\rangle$, то другий

перейде в стан $|1\rangle$ і навпаки. Без проведення вимірювання, однак, жодний із цих двох кубітів не перебуває в певному стані. Відзначимо, що переплутування, як і суперпозиція станів, – винятково квантові ефекти, що не мають аналога для об'єктів класичної фізики.

Квантові протоколи розподілення секретних ключів пропонують інший підхід до вирішення цієї проблеми. Теоретично, квантова криптографія може забезпечити захищене від перехоплення розподілення ключа, оскільки, на відміну від класичної криптографії, вона заснована на законах фізики, а не на тому факті, що для успішного перехоплення потрібні були б величезні обчислювальні потужності. Внаслідок вищезазначених властивостей квантових систем, зловмисник вносить у передану окремими фотонами інформацію деяку кількість помилок, які можуть бути виявлені легітимними користувачами.Відзначимо, що закони квантової механіки дозволяють не тільки виявити збурювання станів, але й зв'язати рівень помилок при вимірюваннях у легітимних користувачів з кількістю інформації, що міг отриматизловмисник. Це дозволяє провести процедуру підсилення секретності, при якій довжина переданого ключа зменшується на деяке число біт, що залежить від рівня помилок при передачі. У результаті кількість інформації про ключ, що може мати зловмисник після цієї процедури, обмежена зверху як завгодно малою величиною, з імовірністю, як завгодно близької до одиниці. Таким чином, протоколи квантового розподілення ключів, на відміну від більшості класичних схем, мають теоретико-інформаційну стійкість, що не залежить від обчислювальних та інших технічних можливостей зловмисника.