

У процедурі типу дайджест-автентифікації для перевірок паролів клієнтів використовують метод «виклик-відповідь». (зазвичай його називають рукоштовуванням). Такий пароль повинен мати доступ у даному сервері, відповідно до цього, сервер повинен виступати у якості контролера – домену серверної мережі. Єдиний недолік, який помічений у таких типах конфігурацій полягає у наступному: Якщо зломисник отримає доступ та контроль над доменом – це може мати катастрофічні наслідки [2].

Список використаних джерел:

1. Храмцов П.Б., Брик С.А., Русак А.М., Сурин А.И. – Основы WEB-технологий. – М.: ИТУИТ.РУ, 2003. – 512 с.
2. Роджерс Д. – Программирование на Microsoft JScript.NET. «Вильямс», 2002. – 352 с.
3. Дунаев В.В. JavaScript. – СПб.: «Питер», 2003. – 394 с.
4. Старыгин А. XML: разработка Web-приложений. – СПб.: «БХВ-Петербург», 2003. – 585 с.
5. Троелсен Э. C# и платформа.NET. Библиотека программиста. – СПб.: «Питер», 2007. – 796 с.

Кухар О.О. Козлов Р.С.

студенти,

Національний авіаційний університет

ВИКОРИСТАННЯ ОДИНИЧНИХ КВАНТОВИХ СТАНІВ У РОЛІ ІНФОРМАЦІЙНОГО РЕСУРСУ

Якщо коротко звернутися до історії, то квантова теорія інформації розбивається на дві частини: це інформаційна та механічна теорія, які були створені на початку 20 століття.

Мета цих теорій дати можливість нам пізнавати про квантовомеханічні стани та вивчати їхні можливості виконувати функції переносу та обробки інформації. Цей новий вид науки був створений у 60 роках двадцятого століття під час масштабного розвитку обчислювальних машин як наслідок при частому зменшенні розмірів таких цікавих й складних апаратів з деяким часом прийде така необхідність проводити етапи використання одиничних квантових станів у ролі інформаційного ресурса. Поруч з цим схожа перспектива – це перші труднощі а найперше це посилений вплив квантового шуму, який вважався однозначно руйнівним фактором. Хоча при найбільш поглиблених дослідженнях, то можна дійти до висновку, що квантовий шум може давати природню допомогу у той час коли передається або обробляється така інформація [1].

Квантова теорія інформації працює з квантовими явищами, досліджує їх властивості або можливості та вивчає: які технології можна використовувати у повсякденному житті. Як результат зробився висновок, що під час використання квантових станів, така річ має можливість підняти швидкість

обчислень на новий рівень розвитку, з допомогою ідеї квантового комп'ютера, а також надавати гарантії абсолютної секретності поширення ключів квантової криптографії. Коротко про квантовий стан: Коли проводили перші дослідження елементарних частинок було пізнано таку річ, що їх поведінка набагато складніша аніж тодішні уяви про фізичні явища.

Хвильові функції та чисті стани: Існують декілька таких відмінностей природньої теорії та класичної і одне з таких типів відмінностей дає про себе знати вже у самому визначенні стану квантової частини. Уявлення про таку частинку, як про будь – яке тіло, яке вже має якісь координати, масу та розміри, які виявились неправильними, оскільки для деяких таких частинок не було уяви: у якій точці простору вони знаходяться? Але така теорія дає можливість передбачати поведінку таких частинок [2].

Але давайте повернемося до труднощів. Вони полягають у тому, що дати пояснення цій поведінці вдалося лише після завершення відмови від намагання обчислювати усе у повній точності так звані традиційні фізичні системи. Це призвело до того, що усілякі елементарні частинки отримали можливість бути представниками так званої хвильової функції принципового об'єкту.

Отже, на початку поясню визначення чистого квантового стану. Це вектор у Гілбертовому просторі позначається ψ з одиничною нормою. Під векторною нормою розуміється корінь з його скалярного квадрату

$$\|\psi\| = \sqrt{(\psi, \psi)} \quad \psi \in H$$

У даній роботі ми будемо розбирати лише кінцевомірні Гілбертові простори. Що стосується їх властивостей, то у цих речах варто зазначити, що важливим понад усе буде наявність скалярного добутку. Наприклад для вектора ψ властивість одиничної норми буде виглядати наступним чином $\psi^* \psi = 1$

Як ми побачили легко з'єднати дане визначення з традиційним формулюванням хвильових функцій, яким відповідає даний вектор ψ і та координата котрої дорівнюватиме амплітуді ймовірності знаходження шуканої частинки у i -й точці простору. Отже, переконаємося що задача пошуку простору є важливою і відображає найкращий образ відповідного умови задачі [3].

Ще одним найважливішим законом квантової механіки є таке явище, яке називається редукцією або колапс хвильової функції або ще як його часто називають редукцією фон Неймана. і означає про перехід стану після виміру у одне з інших станів виміру оператора виміру. Наприклад під час виміру $\{M_i\}$ та отримання результату і початковий стан буде перетворений відповідно за формулою: $\rho_{(i)} = \frac{M_i \rho M_i}{\text{Tr}(M_i \rho)}$

Насамперед це одне з найважливіших для квантової криптографії властивостей. Оскільки воно вказує на багато помилок та недоліків, які виникали під час намагання виміряти систему. З цього випливає, що того, хто намагатиметься перехопити інформацію завжди можна подетектувати за додатковими помилками на прийомній стороні. Надалі буде показано як насправді відбувається знаходження намагання підслуховування та за їх відповідними кількостями даються оцінки перехоплення визначеному злочинцю [4].

Отже, на звичайних курсах з квантової механіки ми навчалися під дослідженням розуміти лише ортогональні розклади одиниці, де оператори $\{M_i\}$ задовольняють виразу або відноsinам

$$M_i M_j = \sigma_{ij}$$

Дослідження такого плану у подальших реченнях називатимемо чіткими спостереженнями. Також вимоги спільної ортогональності усіх видів таких операторів не обов'язкові і у деяких випадках з погляду на отримання максимальної кількості інформації доволі вигідно користуватися спостережними, оскільки там не всі оператори ортогональні у взаємовідносинах один з одним. Спостереження такого плану називають нечіткими.

Розбір квантових систем, що складається з деяких частинок (такі частини називають складеними частинами), може стати як наслідком цікавих властивостей, які й досі не зустрічалися у класичному випадку. Ще у далекому 1935 році у збереженому листуванні Енштейна, Подольського, Розена були відмічені дуже незвичні властивості складених квантових систем, заперечення локальності: як результат, вийшло так, що дії над однією з підсистем можуть швидко показати свій вплив на іншу підсистему, незважаючи на відстань між ними далеко чи близько вони між собою. Детальне вивчення такої властивості призвело до виникнення формалізму таких квантових систем та властивостей завершених дій над ними [2].

На першому кроці ми розглянемо найелементарніший випадок двох кубітів. На рівні інтуїції стає цілком вірогідно те, що можливі два варіанти їх суцільного стану

- 1) обидва кубіти у стані $|0\rangle$
- 2) перший кубіт у стані $|0\rangle$, а другий у стані $|1\rangle$
- 3) перший кубіт у стані $|1\rangle$, а другий у стані $|0\rangle$
- 4) або ж обидва кубіти мають стан $|1\rangle$

Саме ці 4 вектори ми й будемо називати базисними у даному просторі двох вказаних кубітів. Найбільш формальне являється те, що ці речі звучать наступним чином. Якщо ми маємо простори H_1 H_2 з розмірами $d_{sub}(1)$ та $d_{sub}(2)$ та ортонормовані базиси $\{e_{sub}(i)\}$ та $\{f_{sub}(i)\}$ то зазвичай визначеним простором з базисом $\{e_{sub}(i), f_{sub}(i)\}$ де i виступає як значення від 1 до $d_{sub}(i)$ а вже j від 1 до $d_{sub}(2)$. Якщо вже ввести у новому просторі скалярний добуток за законом [3].

$$\langle e_{sub}(i) | f_{sub}(j) \rangle = \langle e_{sub}(i) | e_{sub}(m) \rangle \langle f_{sub}(j) | f_{sub}(n) \rangle = \langle e_{sub}(i) | e_{sub}(m) \rangle * \langle f_{sub}(j) | f_{sub}(n) \rangle$$

та звернувши на це увагу продовжити його по лінійності на інші вектори і як результат дістанемо Гільбертовий простір тензорного добутку $H_{sub}(1) \otimes H_{sub}(2)$ та позначається як $H_{sub}(1) \otimes H_{sub}(2)$. І тут стає цілком вірогідно, що розмірність цієї величини дорівнює $d_{sub}(1) d_{sub}(2)$.

Тензорний добуток операторів $A_{sub}(1) \otimes S(H_{sub}(1))$ або $A_{sub}(2) \otimes S(H_{sub}(2))$ оператор $A_{sub}(1) \otimes A_{sub}(2)$ у просторі $H_{sub}(1) \otimes H_{sub}(2)$ який діє за законом

$$(A_{sub}(1) \otimes A_{sub}(2)) | e_{sub}(1) \otimes e_{sub}(2) \rangle = (A_{sub}(1) | e_{sub}(1) \rangle) \otimes (A_{sub}(2) | e_{sub}(2) \rangle)$$

Раптом у цей момент може виникнути питання: Чи може будь – який стан у просторі $H_{\text{sub}}(1) \otimes H_{\text{sub}}(2)$ можна задати у вигляді тензорного добутку станів, які належать частковим просторам $H_{\text{sub}}(1)$ та $H_{\text{sub}}(2)$. Відповідь на це питання негативне бо класичним прикладом заперечення є стан двох кубітів у просторі $H_{\text{row}}(2) \otimes H_{\text{row}}(2)$ називають ЕПР по першим буквам прізвищ першовідкривачів.

$$|\psi_{\text{sub}}(\text{EPR})\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Досить легко помітити, що уявити цей стан як тензорний добуток одночастинних станів не можна.

$$|\psi_{\text{sub}}(\text{EPR})\rangle \neq (a_{\text{sub}}(1)|0\rangle + b_{\text{sub}}(1)|1\rangle) \otimes (a_{\text{sub}}(2)|0\rangle + b_{\text{sub}}(2)|1\rangle)$$

Але це лише початок, оскільки можна навести й другі приклади застосовування законів квантових вимірювань та складених квантових систем. Це такі ситуації, у яких квантові стани розбито поміж двома особами (або особою та оточенням), одні з яких роблять вимірювання над своїми підсистемами. Такі дії називають частковими вимірюваннями [5].

Під час того, коли вимірюється лише одна з підсистем на другою підсистемою ми не проводимо ніяких активних дій або операцій, тому у розкладі одиниці, які описують загальний вимір, усі типи операторів, які мають точне відношення до другої підсистеми будуть називатися тотожними. Наприклад, якщо перший учасник використовує вимірювання $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, то у складовій системі буде виведена наступна формула вимірювання

$$M_{\text{sub}}(0) = |0\rangle\langle 0|_{\text{sub}}(1) \otimes I_{\text{sub}}(2)$$

$$M_{\text{sub}}(1) = |1\rangle\langle 1|_{\text{sub}}(1) \otimes I_{\text{sub}}(2)$$

Цілком можна помітити те, що не дивлячись на тотожні вигляди операторів у правій частині, вимірювання першої такої підсистеми в усіх таких випадках має великий вплив на стан другої підсистеми. Це вже дуже важливий наслідок, оскільки властивість редукції хвильової функції буде розібрано трохи згодом.

Під час досліджень передачі інформації за допомогою квантових станів виникає список найважливіших питань, які дуже стосуються характеристики виконуючих квантових об'єктів каналів.

Список використаних джерел:

1. Килин С. Я., Хорошко Д. Б., Низовцев А. П. «Квантовая криптография: идеи и практика».
2. Килин С. Я. «Квантовая информация / Успехи Физических Наук» – 1999. – Т. 169. – С. 507–527 [3].
3. Красавин В. «Квантовая криптография».
4. Румянцев К. Е., Плєнкін А. П. Экспериментальные испытания телекоммуникационной сети с интегрированной системой квантового распределения ключей // Телекоммуникации. 2014. № 10. – С. 11–16.
5. Плєнкін А. П. Использование квантовых ключей для шифрования сетевого соединения // Десятая ежегодная научная конференция студентов и аспирантов базовых кафедр Южного научного центра РАН: Тезисы докладов (г. Ростов-на-Дону, 14-29 апреля 2014 г.). – Ростов н/Д: Изд-во ЮНЦ РАН, 2014. – 410 с. – С. 81–82.