показують, що ентропія системи завжди збільшується внаслідок невідомих факторів, які не можуть бути передбачені або контрольовані демоном Лапласа.

Таким чином, демон Лапласа є лише теоретичною конструкцією, яка допомагає розуміти принципи термодинаміки та їхні наслідки. Він допомагає уявити собі можливі шляхи вирішення складних проблем та викликів у фізиці та інших науках, але не має практичного значення в реальному світі.

Теоретично, існує можливість реалізувати демона Лапласа за допомогою комп'ютерного моделювання. Проте, така реалізація є вкрай складною і непрактичною, оскільки вимагає обробки величезної кількості даних та виконання великої кількості обчислень.

Одним з підходів до реалізації демона Лапласа є використання машинного навчання та штучного інтелекту. За допомогою таких алгоритмів можна навчити комп'ютер передбачати рух частинок у системі, виходячи з вхідних даних про їхні початкові параметри та взаємодії між ними. Проте, для цього потрібні великі обсяги даних та потужні обчислювальні ресурси.

Існують також інші підходи до реалізації демона Лапласа, такі як використання квантових комп'ютерів та нейроморфних систем. Проте, наразі ці технології є ще досить новими та експериментальними, і їхні можливості ще не повністю досліджені.

Отже, хоча існують теоретичні можливості для реалізації демона Лапласа за допомогою комп'ютерного моделювання, практична реалізація такої системи залишається вкрай складною та вимагає значних ресурсів.

Список літератури

1. Картина світу сучасної фізики. Квантова механіка, її інтерпретація. / / Http://nrc.edu.ru/est/r2/1.html

2. Нільс Бор. Квантова фізика і філософія. / / Http://mainhead.dorms.spbu.ru:8100/physics/books/bohr1/ar13.html

3. Kane, R. The Oxford handbook on free will [Electronic resource]. – Accessed mode: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780195178548.001.0001/oxfordhb9780195178548-e-1

4. Timple K. Demotivating Semi-Compatibilism / K. Timple // Ideas y Valores. – 2009. – Vol. 58, № 141. – P. 109-124 [Electronic resource]. – Accessed mode: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-00622009000300007

УДК 53.06

КВАНТОВА КРИПТОГРАФІЯ. ПРОТОКОЛ BB84

Р. Дяченко, зд. гр. КІ-22-1
Центральноукраїнський національний технічний університет

Як відомо, головним завданням криптографії є забезпечення конфіденційності, цілісності та автентичності інформації, застосовуючи при цьому математичні методи. Квантова криптографія є областю криптографії, що використовує не тільки математичні методи, а й фундаментальні закони природи.

Квантова криптографія використовує квантові біти(кубіти), які можуть знаходитися в суперпозиції двох або більше станів. Це дозволяє передавати інформацію з одного квантового біту на інший, без передачі на інші проміжні канали зв’язку. Ця передача здійснюється квантовою телепортацією.

Гілберт Беннетт і Чарльз Бессетт у 1984 році розробили протокол квантової криптографії BB84. Цей протокол заснований на принципі невизначеності, який пов’язаний з ефектом спостерігача(з точки зору фізики) – спостереження, що проводиться над системою впливає на цю системую. Отже ґрунтуючись на цьому, Беннет і Бессет запропонували

кодувати данні в квантових станах одиничних фотонів, наприклад, в поляризації. Так як, факт виміру квантових об'єктів впливає на стан цих об'єктів (в нашому випадку фотонів), то слідуючи цьому, якщо хтось намагається отримати передачу фотона, виміряти стан фотона, якими обмінюємося, то ми обов'язково це помітимо, тому що його стан зміниться. Отже, підключитися до каналу зв'язку з квантовою передачею даних неможливо, цьому не дозволяють фундаментальні закони квантової механіки.

ВВ84 працює так:

Зауваження: Аліса – відправник даних, Боб – приймає данні, Єва – перехоплює данні.

- Аліса відправляє фотони, що поляризовані в одному з двох ортогональних базисах: прямокутний та діагональний.
- Боб отримує фотони, що надіслала Аліса, обирає випадковий базис для їх виміру, записує результати вимірювання та базиси.
- Потім Боб та Аліса кажуть один одному про використанні базиси по публічному каналі. Далі якщо данні, що отриманні не співпадають з базисом, то вони є недійсніми. Залишаються тільки значення з співпалими базисами. (Цей процес називається просіюванням)
- Щоб визначити рівень помилок в ключі(відправлених даних), Аліса та Боб по публічному каналі порівнюють невелику частину ключа. Якщо рівень помилок менше 11%, то гарантується безпека лінії зв'язку
- Якщо Єва зможе перехопити фотон та виміряти його, та надішле копію Бобу, то враховуючи принцип невизначеності та ефект спостерігача, Боб та Аліса на етапі визначення помилок, зможуть виявити, що їх хтось прослуховує.

Варто зазначити, що перший експеремент по передачі по квантовому каналу Беннет та Бессет провели в 1989 році. Хоча їх ідею не сприйняли серйозно, вони вирішили самі створити прототип експеременталної установки. Перша установка передавала данні тільки на дистанцію в 32,5 сантиметра і була дуже шумною. Але не дивлячись на всі недоліки, установка працювала правильно.

В наш час квантовий зв'язок повністю безпечний, це зумовлено тим, щоб зламати його потрібно зламати закони квантової механіки. Але існують методи атаки на такий зв'язок, що вимагають багато зусиль і ресурсів, тому що кожна спроба взлому протоколу змінює його ключ, так що це робить цей вид атаки складним та неефективним.

Список літератури

1. Quantum cryptography: Public key distribution and coin tossing: веб-сайт. URL:https://arxiv.org/abs/2003.06557 (дата звернення 18.04.2023)

2. Справочная: квантовая криптография на пальцах: веб-сайт. URL: https://www.google.com/amp/s/habr.com/ru/amp/post/460165/ (дата звернення 18.04.2023)

УДК 530.1

«ПАРАДОКСИ» КВАНТОВОЇ МЕХАНІКИ

К. Голубовський, зд. гр. ЕЕ-22
Е. Козатков, зд. гр. ЕЕ-22
О. Гур'євська, канд. пед. наук, доцент
Центральноукраїнський національний технічний університет

Квантова модель природи, суперечить не тільки повсякденому досвіду, а й інтуїтивному розумінню реальності. Вона описує явища, які спостерігаються на атомному і субатомному рівнях, тобто на таких, які ми візуально не бачимо, не сприймаємо через органи чуття.

На фундаментальному рівні атомів та субатомних частинок, знайома «класична»