Szyfrowanie Kwantowe

Co to są kwanty? Co to są kubity?

Bit - to najmniejsza jednostka informacji w informatyce *klasycznej*. Przyjmuje wartości 0 albo 1.

Kubit - to najmniejsza jednostka informacji w informatyce *kwantowej*. Przyjmuje wartości pomiędzy superpozycją $(1, 0)$ a $(0, 1)$, a po pomiarze stanu kwantowego przyjmuje jedną z wartości 1 lub 0. Kubity można również łączyć poprzez splatanie kwantowe.

Kluczowe pojęcia

1. Superpozycja:
2. Zasada nieoznaczoności Heisenberga
3. Splątanie kwantowe

Superpozycja

W mechanice kwantowej cząstki mogą istnieć w wielu stanach jednocześnie. To zjawisko, znane jako superpozycja, umożliwia kodowanie znacznie większej ilości informacji na pojedynczym kubicie (podstawowej jednostce informacji kwantowej) w porównaniu z bitami w klasycznym komputerze.

Superpozycja c.d.

Kolokwialnie rzecz ujmując superpozycję, można przedstawić przy pomocy poniższego problemu:

> To jak kiedy próbujesz się zdecydować, czy chcesz jeść lody truskawkowe czy czekoladowe, i ktoś mówi, że możesz mieć
> trochę obu na raz. Dzięki temu komputery kwantowe mogą rozwiązywać trudne problemy szybciej niż zwykłe komputery, bo
> patrzą na wiele możliwości naraz, a nie tylko na jedną.

Zasada nieoznaczoności Heisenberga

Zasada nieoznaczoności Heisenberga to pomysł w fizyce kwantowej, który mówi nam, że istnieje pewne naturalne ograniczenie dotyczące tego, jak dokładnie możemy jednocześnie zmierzyć pewne właściwości cząstki. Konkretnie chodzi o pozycję i pęd cząstki.

Jeśli bardzo precyzyjnie zmierzymy pozycję cząstki, to nasza pewność co do jej pędu stanie się mniej precyzyjna, i odwrotnie. Innymi słowy, im bardziej dokładnie próbujemy określić jedną z tych dwóch rzeczy (pozycję lub pęd), tym bardziej niepewna staje się nasza wiedza na temat drugiej. To nie jest wina naszej technologii pomiarowej, ale fundamentalne ograniczenie natury kwantowej cząstek.

Zasada nieoznaczoności Heisenberga c.d.

W skrócie zasada nieoznaczoności mówi nam, że istnieje pewne zamieszanie, czyli niepewność związana z jednoczesnym pomiarowaniem niektórych właściwości cząstek, i nie ma możliwości całkowitego wyeliminowania tego zamieszania.

Tę zasadę opisuje wzór:

$$\Delta x \Delta p_x \geq \frac{\hbar}{2}$$

Splątanie kwantowe

Zjawisko splątania kwantowego to rodzaj powiązania między cząstkami w małej skali. Kiedy dwie cząstki zostaną splątane, ich stany kwantowe stają się wzajemnie zależne, nawet jeśli są od siebie oddzielone na duże odległości.

Co to oznacza? Jeśli wykonasz pomiar na jednej z tych splątanych cząstek, to natychmiast zdeterminuje on stan drugiej cząstki, bez względu na to, jak daleko się od siebie znajdują. To zdumiewające, ponieważ sugeruje, że informacja przemieszcza się między cząstkami szybciej niż światło, co jest sprzeczne z intuicją klasycznej fizyki.

Splątanie kwantowe c.d.

Einstein nazwał to upiornym działaniem na odległość, ponieważ wydawało mu się to niematerialne i nieintuicyjne. Jednak eksperymenty potwierdzające splątanie kwantowe były wielokrotnie przeprowadzane i potwierdzają, że jest to rzeczywiste zjawisko w świecie kwantowym.

Co to jest Szyfrowanie Kwantowe?

Szyfrowanie kwantowe to zaawansowana forma bezpiecznej komunikacji, która wykorzystuje zasady fizyki kwantowej, aby zabezpieczyć przesyłane informacje. Głównym celem jest ochrona informacji przed przechwyceniem i nieautoryzowanym dostępem, nawet przez potężne komputery, które mogą próbować złamać tradycyjne metody szyfrowania.

Szyfrowanie kwantowe wykorzystuje unikalne właściwości mikroświata kwantowego do utworzenia bezpiecznego kanału komunikacyjnego. Pomimo obecnych wyzwań technologicznych i praktycznych, taka forma szyfrowania ma potencjał zrewolucjonizowania dziedziny bezpieczeństwa komunikacji.

Zastosowania i problemy

- Kwantowa dystrybucja klucza (QKD)
- Model ograniczonego i zakłóconego przechowywania kwantowego
- Kryptografia kwantowa niezależna od urządzenia

Kwantowa Dystrybucja Klucza (QKD)

Kwantowa dystrybucja klucza (QKD - *Quantum Key Distribution*) to zaawansowana metoda bezpiecznego przesyłania tajnych kluczy do szyfrowania informacji między dwoma stronami. Podstawowym celem QKD jest umożliwienie dwóm stronom komunikacji ustalenia tajnego klucza w sposób, który jest odporny na przechwycenie przez potencjalnego przeciwnika.

Proces QKD wykorzystuje zasady fizyki kwantowej, takie jak zasada nieoznaczoności Heisenberga i splątanie kwantowe.

Kwantowa Dystrybucja Klucza (QKD) c.d.

Oto ogólny sposób działania QKD w prostych słowach:

1. **Przygotowanie klucza**
2. **Przesyłanie kwantowe**
3. **Monitorowanie bezpieczeństwa**
4. **Ustalanie klucza**

Model ograniczonego i zakłóconego przechowywania kwantowego

Model ograniczonego i zakłóconego przechowywania kwantowego mówi nam, że w praktyce przechowywanie informacji w systemach kwantowych jest ograniczone, a także podatne na zakłócenia czyli niepewności wynikające z oddziaływań z otoczeniem. Oznacza to, że utrzymanie dokładnych i długotrwałych kwantowych informacji jest trudne z powodu różnych czynników, takich jak fluktuacje środowiska, które mogą wprowadzać błędy i utratę informacji.

Wyzwania

- **Zasięg:** Komunikacja kwantowa na dużą skalę jest trudna do realizacji z powodu strat sygnału kwantowego (znanych jako dekoherencja) w kanałach transmisyjnych, takich jak światłowody.
- **Technologia:** Technologia kwantowa jest wciąż w fazie rozwoju, z wieloma wyzwaniami technicznymi i naukowymi do przezwyciężenia.
- **Koszt:** Obecne systemy kwantowe są kosztowne i zazwyczaj wymagają warunków pracy w niskich temperaturach lub próżni, co komplikuje ich wdrożenie na dużą skalę.

Przykład użycia (QKD)

Najbardziej znanym przykładem jest protokół **BB84**, opracowany przez Charlesa Bennetta i Gillesa Brassarda w 1984 roku.

1. **Wybór Bazy i Stanów Kwantowych**:
    - Nadawca (zwykle nazywany Alicją) generuje losowy ciąg bitów (np. 01011).
    - Dla każdego bitu Alicja losowo wybiera jedną z dwóch baz kwantowych:
        - bazę prostokątną (1)
        - bazę diagonalną (2)

Przykład użycia (QKD) c.d.

$$\begin{aligned} 0 \text{ jako } |0\rangle \\ 1 \text{ jako } |1\rangle \end{aligned} \tag{1}$$

$$0 \text{ jako } |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{2}$$

$$1 \text{ jako } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Przykład użycia (QKD) c.d.

2. **Wysyłanie Stanów Kwantowych**:
    - Alicja wysyła fotony reprezentujące wybrane bity w wybranych bazach do odbiorcy (nazywanego Bobem).
3. **Detekcja przez Odbiorcę**:
    - Bob, nie znając wyboru bazy Alicji, losowo wybiera bazę dla każdego fotonu, który otrzymuje, i dokonuje pomiaru.

Przykład użycia (QKD) c.d.

4. **Porównanie Baz**:
    - Alicja i Bob porównują publicznie wybrane przez siebie bazy. Zachowują tylko te bity, dla których wybrali tę samą bazę. Pozostałe bity są odrzucane.
5. **Weryfikacja i Finalny Klucz**:
    - Aby sprawdzić, czy nie doszło do podsłuchu, Alicja i Bob mogą porównać część swoich bitów. Jeśli bity są identyczne, mogą być pewni, że klucz jest bezpieczny. Klucz ten może być następnie użyty do zaszyfrowania komunikacji za pomocą klasycznego szyfrowania symetrycznego.

Podsumowanie

Szyfrowanie kwantowe oferuje obiecującą ścieżkę do bezpieczeństwa informacji w erze komputacji kwantowej. Chociaż technologia ta jest wciąż w fazie rozwoju, jej zdolność do zapewnienia bezpieczeństwa komunikacji jest niezrównana w porównaniu z klasyczną kryptografią.

Dziekujemy za uwage :3

- Szymon Jacoń
- Szymon Kaszuba-Gałka