

Popularnonaukowe streszczenie projektu

Cel- Opis zjawisk kwantowych oraz klasycznego świata makroskopowego różni się znacząco nie tylko pod względem używanego aparatu matematycznego, ale również pod względem fundamentalnych konceptów i filozoficznych konsekwencji. Albert Einstein by uzasadnić swój sprzeciw wobec mechaniki kwantowej powiedział kiedyś, *'Chciałbym myśleć, że Księżyc istnieje nawet gdy na niego nie patrzę'*. Później w przełomowych pracach autorstwa Bell-Kochen-Specker, pokazano niemożliwość pomiaru niezależnej obiektywnej rzeczywistości kwantowych obserwabli. Ta cecha, nazywana, 'kwantową kontekstualnością', sugeruje że intuicja Einsteina dotycząca podstawowej natury teorii kwantowej jest błędna. Tradycyjne pojęcie kwantowej kontekstualności pokazuje, że istnieją pomiary kwantowe których wynik nie może być określony z wyprzedzeniem w sposób niekontekstualny. Na przykład, niezależnie od kontekstu pomiaru pośród wyboru łącznych mierzalnych testów które mogą być przeprowadzone razem. Podczas gdy pojedynczy układ kwantowy wykazuje kontekstualność, teoria Bella pokazuje, że dwa podukłady większego układu posiadają bardziej zaskakujące nielocalne korelacje. Później zostało zaproponowane przez Spekkens'a bardziej fundamentalne pojęcie kontekstualności, mianowicie, kontekstualność przygotowująca stan (preparation contextuality). Jeżeli różne procedury przygotowania stanu mieszanego nie mogą być rozróżnione operacyjnie, wtedy, w niekontekstualnym modelu przygotowania stanu, realistyczny opis tych przygotowań jest taki sam. Zostało pokazane, że przygotowanie kontekstualności implikuje determinizm w pomiarze typu von Neumana. Kwantowa nielocalność i kontekstualność zrewolucjonizowała dziedzinę przetwarzania informacji w czasie ostatnich kilku dekad. Na przykład, nielocalne korelacje zapewniają bezwarunkowe bezpieczeństwo w kryptografii i generowaniu losowości mimo tego że, użytkownik nie musi ufać urządzeniu z którego korzysta. To podejście nazywane jest kryptografią niezależną od urządzania które jest używane w procesie komunikacji. Zasoby kwantowe umożliwiają również inne zdumiewające możliwości jak teleportacja, kodowanie gęste, przewagę w procesach złożoności obliczeniowej itp. Wymienione rozwiązania nie są możliwe do osiągnięcia za pomocą klasycznych metod komunikacji. Naszym głównym celem prezentowanego wniosku jest - (1) Przetwarzanie informacji kwantowej wraz z przygotowaniem kontekstualności, (2) badanie nowych cech kwantowej nielocalności opartych o niekontekstualność podukładów.

Badania- W pierwszej kolejności, proponujemy ogólne zadanie utajnionej wielowątkowości (oblivious multiplexing task) w scenariuszu przygotowania i pomiaru. W odniesieniu do tego modelu, scharakteryzujemy pełny zbiór prawdopodobieństw wszystkich możliwych wydarzeń w trzech różnych teoriach - teorie niekontekstualnych preparacji układu (preparation noncontextual theories), teoria kwantowa (quantum theory) oraz po-kwantowe ogólne teorie prawdopodobieństwa (post-quantum general probabilistic theories). W oparciu o utajone więzy w komunikacji pomiędzy urządzeniami przygotowującymi stan oraz urządzeniami pomiarowymi, proponujemy kwantowy sposób przetwarzania informacji który jest częściowo niezależny od urządzania. W tym podejściu nie zakładamy nic na temat jak działa wewnątrz używane przez nas urządzenie. W drugiej części wniosku będziemy badać w pełni nielocalne kwantowe korelacje oraz monogamiczne właściwości kwantowej nielocalności przy użyciu kontekstualności KS lokalnych podukładów.

Znaczenie badań- Zaproponowane kierunki badań mają istotne znaczenie nie tylko w zastosowaniach teorii kwantowej, w przetwarzaniu informacji i komunikacji ale również w zrozumieniu fundamentów mechaniki kwantowej. Podejście do przygotowania kontekstualności w ujęciu ogólnych operacyjnych zadań utajnionej wielowątkowości jest podstawowe w badaniu jej implikacji. W oparciu o badania, przygotowania kontekstualności może być określone ilościowo w sposób niezależny od teorii. Jako że, transfer utajniony (oblivious transfer) jest budulcem klasycznej kryptografii, prezentowana praca badawcza może wnieść istotny wkład w dziedzinę kryptografii. Całkowicie nielocalne korelacje oraz monogamiczne właściwości nielocalności są znaczące w scenariuszach kryptografii niezależnej od urządzania (device independent cryptographic scenarios) w których Alicja i Bob mogą zweryfikować wystarczające łamanie nierówności Bell'a by zagwarantować, że są bezpieczne przeciw systemom podsłuchującym. Dlatego nowe wyniki w tym kierunku badań będą miały wpływ na bezpieczeństwo przetwarzania informacji niezależnie od urządzania. Badania nad uogólnioną monogamią pomiędzy nielocalnością i lokalną kontekstualnością mogą doprowadzić do uniwersalnych kwantowych zasobów oraz mogą pomóc zrozumieć pochodzenie splątania kwantowego.