„Technologie kwantowe - opis stanu, wpływ na funkcjonowanie państwa”

Andrzej Walczak

Faculty of Cybernetics, Military University of Technology,
Gen. Sylwestra Kaliskiego 2 Str., 00-908 Warsaw, Poland

XXX Forum Teleinformatyki
19-20 września 2024

„ePolska po XXX latach – System informacyjny państwa vs sztuczna inteligencja”

Plan wykładu

1. Jakie były początki – co wynika z zasady Heisenberga
2. Model Einsteina – Podolskiego - Rosena
3. Nagroda Nobla z fizyki 2022 – stany splątane nowym przełomem
4. Niektóre cechy stanów splątanych
5. Obecny stan technologii – czy komputer kwantowy stanowi o technologii informacji kwantowej?
6. „State of the art” w zakresie obliczeń kwantowych – wybrane elementy
7. Czym jest klucz kwantowy i do czego służy?
8. Stan technologii informatyki i telekomunikacji kwantowej w kraju – wybrane elementy
9. Obecne wyzwania/korzyści dla technologii informatyki kwantowej w kraju

Jakie były początki – co wynika z zasady Heisenberga?

Zagadkę postawił przed nami wszystkimi Werner Heisenberg. Otóż stwierdził on, że jeśli chcemy się poruszać po świecie wielkości mierzalnych, realnie rejestrowanych, takich jak na przykład pęd p masy m (p=mv) i jej położenie x to nie uda nam się niektórych takich par, tworzących wielkości kanonicznie sprzężone, zmierzyć jednocześnie (**1927**).

Jakie były początki – co wynika z zasady Heisenberga?

Znamy to prawo jako zasadę Heisenberga (**1927**)

$$\Delta x \Delta p >= h/4\pi$$

$$\Delta E \Delta t >= h/4\pi$$

Gdzie h jest stałą Plancka. (h=6,62*10-34 J*s)

UWAGA: pojawia się w tej zasadzie nielokalność pomiaru oraz , w pewnym stopniu, brak realności pomiaru

Model Einsteina-Podolskiego-Rosena

Odpowiedź Einsteina: „..*Pan Bóg nie gra w kości*..”. Tym zdaniem zanegował probabilistyczną interpretację wynikająca z r. Sch., a także rezultat zasady Heisenberga. Usiłując pokazać, że mechanika kwantowa jest teorią niekompletną i nie wyjaśniającą zjawisk przyrody wraz ze swoimi współpracownikami Rosenem i Podolskim w **1935** roku rozwiązał r.Sch. dla dwóch różnych cząstek. Dla takich cząstek zasada Heisenberga nie obowiązuje bo to są dwa różne obiekty.

Model Einsteina-Podolskiego-Rosena

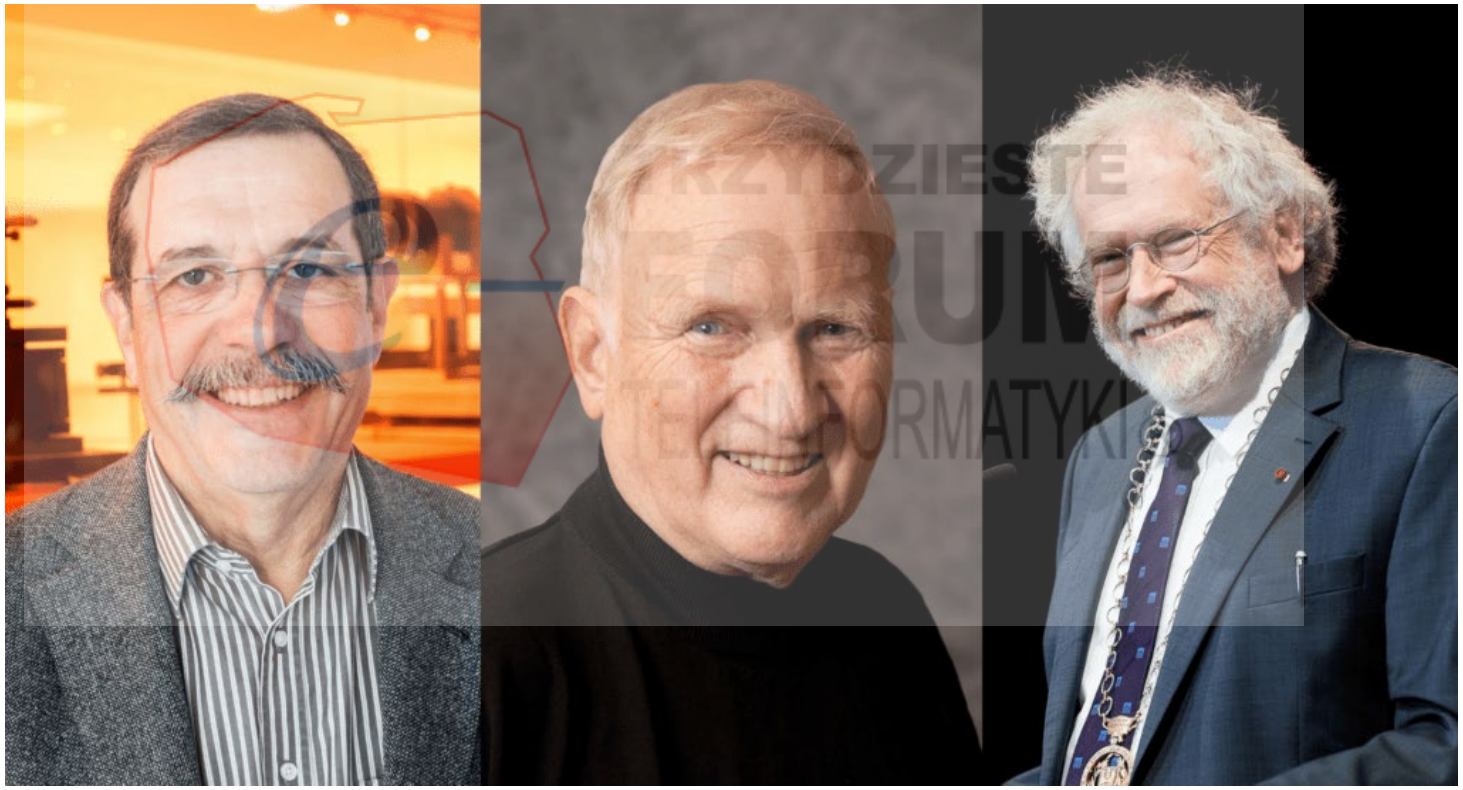
Z otrzymanego w modelu EPR rozwiązania wynikało, że w myśl zasady Heisenberga, jeśli można wyznaczyć pęd i położenie jednej z dwóch cząstek, to rozwiązanie EPR wskazywało, że w tej samej chwili wiemy, jakie jest położenie i pęd drugiej cząstki. Takie cząstki byłyby **nierozerwalnie splątane**. Nazwano to paradoksem EPR i zinterpretowano (**błędnie**), że cząstki powinny wobec tego ze sobą oddziaływać (przekazywać sobie informacje o swoim pędzie i położeniu) z prędkością większą od prędkości światła.

Nagroda Nobla z fizyki 2022

W licznych eksperymentach, prowadzonych niezależnie przez wiele lat Anton Zeilinger, Alan Aspect oraz John F.Clauser udowodnili istnienie stanów splątanych. Otrzymali w **2022** roku Nagrodę Nobla za „…**eksperymenty z kwantowym splątaniem fotonów, ustalenie naruszenia nierówności Bella i pionierskie dokonania w dziedzinie informatyki kwantowej…**”.

Military University of Technology

„Technologie kwantowe - opis stanu, wpływ na funkcjonowanie państwa” XXX Forum Teleinformatyki



Niektóre cechy stanów splątanych

- Wyzwaniem jest tworzenie i utrzymanie stanów splątanych ponieważ ich oddziaływanie z otoczeniem podlega procesowi tak zwanej **dekoherencji** (zjawisko fizyczne na poziomie kwantowym) co zmienia ich podstawową cechę ze stanów splątanych na stany, które skorelowane już nie są.
- **Na stanach splątanych możemy wykonywać operacje matematyczne wielokrotnie szybciej niż na klasycznych bitach we współczesnych komputerach (tzw. kodowanie gęste).**
- Jest wiele zjawisk fizycznych pozwalających na wytworzenie stanów splątanych. Jednak technologia ich wytworzenia zmusza do operowania stanami splątanymi w tej samej technologii, co technologia ich wytworzenia, a to nie we wszystkich przypadkach jest łatwe do wykonania.

Obecny stan technologii – czy komputer kwantowy stanowi o technologii informacji kwantowej?

Firma IBM w styczniu **2019** ogłosiła wprowadzenie do oferty sprzętowej urządzenia **IBM Q System One**. Pierwszy komercyjny komputer kwantowy IBM zbudowany jest na bazie 20 kubitowego chipa kwantowego, który został umieszczony w obudowie wykonanej z laminowanego szkła boro-krzemianowego jako izolacji.

Obecny stan technologii – czy komputer kwantowy stanowi o technologii informacji kwantowej?

System IBM Q System One może być umieszczony w praktycznie dowolnej serwerowni. Co jest ważne bo platforma obliczeniowa komputera kwantowego jako zintegrowany i samodzielny komponent pozwala na integrację z istniejącym już lokalnie środowiskiem obliczeniowym, które zapewnia komunikację z komputerem kwantowym.

Obecny stan technologii – czy komputer kwantowy stanowi o technologii informacji kwantowej?

Jednym z wyzwań systemów kwantowych jest konieczność utrzymania wysokiej jakości qubitów (najmniejszy stan splątany) wykorzystywanych do wykonywania obliczeń kwantowych. Wynika to z zakłóceń powstających w otoczeniu komputera, np. wibracji, wahań temperatury, fal elektromagnetycznych, etc.. Ochrona przed tymi zakłóceniami jest jednym z wielu powodów, dla których komputery kwantowe i ich komponenty wymagają ekstremalnie starannej inżynierii i izolacji oraz pracy (niektóre technologie) w temperaturach rzędu 20mK (-273.13 C). Tylko tak niska temperatura zapewnia środowisko do pracy całego urządzenia pozwalając na stabilną pracę przez ok. 100 mikrosekund.

Obecny stan technologii – czy komputer kwantowy stanowi o technologii informacji kwantowej?

IBM Quantum System One bazuje na procesorze Falcon o wydajności 27 kubitów. Obecnie dostępne są platformy 60 kubitowa i 127 kubitowa. W roku 2024 IBM ogłosił zbudowanie rejestru kwantowego 1000 kubitowego i przejście do technologii 10000.

Na targach CES w Las Vegas 2023 pokazano **komercyjną wersję** komputera 27 kubitowego do pracy nie tylko warunkach laboratoryjnych i zapowiedziano jej udostępnienie.

UWAGA: PRZEJŚCIE OD 20 DO 127 KUBITÓW pracujących stabilnie W OKRESIE 4 LAT

WNIOSEK: TREND INWESTOWANIA JEST USTALONY I NIEPRZERWANY

Dlaczego obliczenia kwantowe stały się tak popularne?

Algorytmy kryptografii asymetrycznej (obejmujące m. in. szyfrowanie z kluczem publicznym, protokoły uzgadniania kluczy, podpisu cyfrowego, uwierzytelniania) opierają się na problemach trudnych obliczeniowo takich jak problem faktoryzacji czyli znajdowania podzielników liczby naturalnej N. Można je uznać za dotychczas odporne na ataki z wykorzystaniem komputerów klasycznych. **Ich złożoność jest niewielomianowa dla dużych podzielników liczby N (najczęściej NP trudna) i na tym opiera się ich bezpieczeństwo**.

Sytuacja wygląda inaczej jeśli zaczniemy rozważać ich bezpieczeństwo w kontekście wykorzystania komputerów kwantowych. Opublikowany w **1994r**. algorytm Shora umożliwia rozkład danej liczby na czynniki pierwsze i znalezienie logarytmu dyskretnego ze złożonością $O((\log N)^3)$ {tzn. dla $N=k*10^9$ algorytm Shora wykona tylko ok. 729 operacji aby znaleźć wszystkie podzielniki}. Oznacza to znacznie krótszy czas znalezienia podzielników klucza publicznego. Algorytm Shora jest hybrydowy, składa się z części klasycznej i części, która jest algorytmem kwantowym i wymaga do przeprowadzenia obliczeń komputera kwantowego.

Dlaczego obliczenia kwantowe stały się ważne dla życia publicznego?

Jak widać obecne metody szyfrowania zostają zagrożone. Dotyczy to obszarów, które w działaniu **naszego otoczenia publicznego** znamy jako:

- wszelka ochrona danych (czyli także baz danych)
  - ⋆ dane na dyskach czyli wszelkie repozytoria (także w chmurze)
  - ⋆ przesyłanie danych poprzez linie narażone na podsłuch (to omówimy osobno)
- uwierzytelnianie dokumentów i osób
- ochrona prywatności korespondencji elektronicznej
- elektroniczny notariusz
- podpis cyfrowy
- pieniądze cyfrowe (płatności elektroniczne ale także bitcoin)
- wybory elektroniczne

Gdzie jeszcze stany splątane wpłyną na bezpieczeństwo danych?

Bezpieczeństwo przesyłania informacji czyli tradycyjnych protokołów dystrybucji klucza opiera się na złożoności obliczeniowej funkcji jednokierunkowych i **nie istnieje w tej technologii możliwość wykrycia podsłuchu bądź zagwarantowania bezpieczeństwa klucza.** Kruchym gwarantem bezpieczeństwa jest w tym wypadku tylko bardzo duża liczba operacji, które trzeba by wykonać w skończonym czasie aby zaszyfrowaną informację odczytać. **Tę barierę przełamują obliczenia kwantowe.**

Gdzie jeszcze stany splątane wpłyną na bezpieczeństwo danych?

Dwie strony komunikujące się ze sobą mogą treść komunikacji zabezpieczyć. Mogą stworzyć losowy niejawny dla osób postronnych klucz współdzielony kwantowy, który może być później wykorzystany do szyfrowania i deszyfrowania wiadomości. Jest to klucz jednorazowy. Ten sposób wykorzystuje cechy informacji (klucza) nazywane kwantowymi bo wykorzystuje zjawiska z zakresu fizyki kwantowej. **Każda próba odczytania klucza kwantowego zostaje natychmiast ujawniona. Odczyt uruchomi dekoherencję klucza.**

„State of the art” w zakresie obliczeń kwantowych – elementy wybrane

CZY MOŻLIWY JEST „KWANTOWY INTERNET” (głównie poczta)? **Odpowiedź brzmi tak** – **nie jest do tego potrzebny komputer kwantowy** tylko **kwantowy generator stanów losowych (QKG)** i kwantowy protokół transmisji klucza kwantowego (QKD). To rozwiązania, **znacząco tańsze od komputera kwantowego**, wykonywane już obecnie w wielu firmach na świecie (także w Polsce w ramach projektu OptoKrypt) i wykorzystywane (w Polsce obecnie w obszarze badawczym, przed aplikacyjnym) w cyberbezpieczeństwie.

Czym jest klucz kwantowy i do czego służy?

To – niestety - materiał na osobny wykład specjalistyczny

Stan technologii informatyki i telekomunikacji kwantowej w kraju

Wicepremier i minister cyfryzacji Krzysztof Gawkowski oraz minister nauki i szkolnictwa wyższego Dariusz Wieczorek podpisali Europejską Deklarację dot. Technologii Kwantowych, zwaną także Paktem Kwantowym. Pakt Kwantowy został wydany w grudniu 2023 roku przez Prezydencję Hiszpańską. Do marca została ona podpisana przez 18 krajów członkowskich Unii Europejskiej. **Polska i Czechy zbudują komputer kwantowy w Ostrawie. Komputer kwantowy będzie także budowany w PCSS. PCSS obecnie posiada hub do komputera IBM oraz dwa własne komputery kwantowe (ORCA PT-1) realizujące obliczenia w technologii optycznej (technologia Boson Sampler).**

Stan technologii informatyki i telekomunikacji kwantowej w kraju

Projekty działające: OptoKrypt – w jego ramach zbudowano polski QKG i wykonano dla potrzeb wojsk obrony cyberprzestrzni połączenia QKD wraz z uruchomieniem odpowiedniej pracowni badawczej (zadaniem zajmują się m.in. moi adiunkci i doktoranci), a także badane są w tym projekcie zjawiska fizyczne prowadzące do zbudowania rejestru kwantowego. Powinien on stać się zalążkiem krajowego komputera kwantowego.

Stan technologii informatyki i telekomunikacji kwantowej w kraju

- Jest rozwinięta **współpraca międzyuczelniana** i z przemysłem: konsorcjum Klaster Technologii Kwantowych . Daje to szanse na wspólne prace przy budowie komputera kwantowego, a także generatora QKG.

Stan technologii informatyki i telekomunikacji kwantowej w kraju

Organizacja dydaktyki: Obserwowany jest i sygnalizowany przez zainteresowane instytucje **dramatyczny brak kadr w zakresie informatyki i telekomunikacji kwantowej**. W WAT mamy unikalną sytuację kumulacji zespołów *kryptologicznych, technologii optycznych i telekomunikacyjnych (generacja QKG), stowarzyszonej inżynierii materiałowej i optoelektroniki, algorytmiki kwantowej.* Przy ich udziale uruchomimy w WCY WAT od nadchodzącego roku akademickiego 2024/2025 kształcenie w obszarze ***informatyki kwantowej w cyberbezpieczeństwie*** w wydaniu dla studentów studiów 2 stopnia, a także studiów podyplomowych dla kadry. Jest to możliwe dzięki potencjałowi ponad 20 osobowej kadry, której w takim przekroju kompetencji nie ma chyba żaden inny ośrodek akademicki w kraju.

W zamierzeniu dołączymy ten cykl wykładów na studiach MBA prowadzonym na Wydziale Cybernetyki w obszarze cyberbezpieczeństwa.

Obecne wyzwania/korzyści dla technologii informatyki kwantowej w kraju

- Potencjał badawczy (znaczący) **w obszarze fizyki jest**. Są to badania podstawowe z potencjałem na przejście do badań stosowanych.
- Potencjał badawczy i wykonawczy **w obszarze informatyki i telekomunikacji kwantowej jest** i został potwierdzony wytworzeniem QKG oraz transmisjami QKD w zespole prof. Marka Życzkowskiego w WAT oraz rozwiązaniami zrealizowanymi w PCSS na konstrukcjach zakupionych (IDQuantique).
- Ten drugi obszar badawczy otwiera drogę do ochrony całej telekomunikacji publicznej i zapewnić może stabilną ochronę działań w obszarze administracji państwowej poprzez zamknięte sieci **intranetu kwantowego**. Jest zaplecze laboratoryjne do przygotowania takich rozwiązań w WAT i PCSS.

Military University of Technology

„Technologie kwantowe - opis stanu, wpływ na funkcjonowanie państwa” XXX Forum Teleinformatyki

Kwantowy
Generator Liczb Losowych

Układ
Kwantowej Dystrybucji Klucza

Układ
Optycznego Kodowania Fazowego

System Modularnych Układów Kwantowej Kryptografii Optycznej