Komputer kwantowy – marzenie fizyka (cz. 2)

Tomasz Sowiński

Tomasz Sowiński jest fizykiem na Wydziale Biologii i Nauk o Środowisku UKSW i w Centrum Fizyki Teoretycznej PAN. W 2005 roku skończył studia na Wydziale Fizyki Uniwersytetu Warszawskiego w zakresie fizyki teoretycznej, a trzy lata później uzyskał tam stopień naukowy doktora. Od lat zajmuje się popularyzacją nauk przyrodniczych. W roku 2008 otrzymał tytuł Mistrza Popularyzacji Nauki „Złoty Umysł" w konkursie Prezesa Polskiej Akademii Nauk.

Przez ostatnich kilka miesięcy poznawaliśmy niesamowite zjawiska zachodzące w mikroświecie, które przebiegały jakby w zupełnej sprzeczności do naszej intuicji. Fotony w bardzo dziwny sposób przechodziły przez polaryzatory (MT 10/2009), potrafiły wykrywać wydawałoby się niewykrywalne sprawne bomby z okienkiem (MT 09/2009), a nawet generowały klucze kryptograficzne, których bezpieczeństwo gwarantowała sama przyroda (MT 02/2010). Na podstawie naszych opowieści zaczął się wyłaniać pewien obraz sugerujący, że sprytne wykorzystanie zjawisk zachodzących w nanoskali, czyli tam, gdzie rządzą prawa mechaniki kwantowej, może pomóc rozwiązywać problemy, które w dobrze nam znanym klasycznym świecie są trudno, jeśli w ogóle, rozwiązywalne.

Do tej pory nie podkreślałem tego zbyt mocno, ale jednym z głównych zadań, jakie stawiają sobie dziś fizycy, jest podejmowanie wszelkich prób wykorzystania zaskakujących naszą intuicję zjawisk subatomowych do rozwiązywania praktycznych problemów dnia codziennego. Powstała nawet wyspecjalizowana gałąź fizyki doświadczalnej nazywana często INŻYNIERIĄ KWANTOWĄ, której podstawowym celem jest dopracowanie do perfekcji sposobów uzyskiwania układów kwantowych składających się z pojedynczych atomów w konkretnym stanie kwantowym. Te umiejętności są nieocenione, gdy fizycy teoretycy wymyślają jakąś konfigurację kilku kwantowych cząstek mającą bardzo ciekawe własności. To właśnie inżynieria kwantowa dziś rozstrzyga, która z propozycji jest możliwa do zrealizowania w warunkach doświadczalnych i pozwala teoretyczne przewidywania weryfikować. Tak burzliwy rozwój inżynierii kwantowej jest poniekąd spowodowany dużym zainteresowaniem firm wysokich technologii, które już przeczuwają, że era dynamicznego rozwoju elektroniki opartej na tranzystorze nieubłaganie się kończy. Dalszy rozwój w reżimie starej elektroniki przestaje być możliwy i po sześćdziesięciu latach od udanych prac Bardeena i Housera stoimy przed najśmielszym wyzwaniem ludzkości – zbudowaniem komputera kwantowego.

Inżynier kwantowy

Komputer kwantowy z prawdziwego zdarzenia jeszcze nie został zbudowany. Trudno jest zatem dokładnie powiedzieć, co to jest. Tak jak przed zbudowaniem pierwszego samolotu bracia Wright nie potrafili dokładnie powiedzieć, co budują, tak my nie wiemy dokładnie, czym owy kwantowy komputer będzie. Wiemy jednak, czym będzie się on różnił od komputerów klasycznych. Jeśli zbudujemy urządzenie przetwarzające informację różniące się właśnie w ten konkretny sposób od komputera klasycznego, to będziemy mogli powiedzieć, że zbudowaliśmy komputer kwantowy. Jakie zatem są te różnice?

Komputer kwantowy z prawdziwego zdarzenia jeszcze nie został zbudowany. Trudno jest zatem dokładnie powiedzieć, co to jest.

NOŚNIKI INFORMACJI KLASYCZNEJ

Zasadnicza różnica pomiędzy komputerem klasycznym a kwantowym jest zawarta w samej koncepcji kodowania informacji. Najmniejszą porcją informacji klasycznej jest BIT – jeden znak, który może przyjmować w danym momencie jedną z dwóch wartości: „0" lub „1". Jest to oczywiście tylko teoretyczna definicja. W praktyce musimy ją skojarzyć z jakimś zjawiskiem fizycznym. Jeśli np. zapisujemy dane na dysku twardym, to nośnikiem bitu jest tam domena magnetyczna, a informacja jest zakodowana w kierunku jej magnetyzacji. Jeśli magnetyzacja jest „w górę",

Nośnik informacji klasycznej w światłowodzie

to mówimy, że domena koduje liczbę „1", jeśli „w dół", to liczbę „0". Oczywiście kierunki „w górę" i „w dół" są umowne i dobrane w taki sposób, aby były dość łatwo wyróżniane przez głowicę dysku czytającą dane. Jeśli informacja jest natomiast przesyłana światłowodem, to bity są zakodowane w impulsach światła. Szerokość każdego impulsu jest związana z prędkością przesyłania informacji i jest ściśle określona. Natomiast natężenie impulsu określa, z jaką wartością bitową mamy do czynienia. Jeśli impuls jest silny, to przypisujemy mu wartość „1", jeśli jest słaby (bądź nie ma go w ogóle), to „0". Te dwa nośniki klasycznej informacji (domena magnetyczna i impuls) mają zupełnie inną naturę fizyczną i tym samym inne zastosowania. Pierwszy z nich (domena magnetyczna) jest doskonałym nośnikiem w przypadku konieczności przechowania informacji. Raz ustawiona domena, jeśli tylko nie jest poddana silnemu zewnętrznemu polu magnetycznemu, może zapamiętać swoje namagnesowanie, a zatem dobrze zapamiętać wartość bitu, której przechowywanie jej powierzono. Impulsy światła w światłowodzie natomiast do przechowywania informacji nadają się bardzo słabo, ale są doskonałe, gdy informację chcemy szybko przesłać. Podróżujące z dużą prędkością impulsy przenoszą informację z jednego końca światłowodu na drugi na tyle szybko, że przesłanie kilkudziesięciotomowej encyklopedii z biblioteki amerykańskiego Kongresu do Warszawy trwa kilka sekund i kosztuje mniej niż jednego dolara.

W każdym z powyższych przykładów mamy do czynienia z bitem, ale jakby ich fizyczna natura jest zupełnie inna. Rozwój elektroniki informacyjnej to w dużej mierze wymyślanie coraz doskonalszych fizycznych nośników. Nie ma tu nic innowacyjnego, jeśli chodzi o samą teoretyczną koncepcję najmniejszej porcji informacji, czyli bitu. Bit zawsze ma tylko dwie możliwości: „0" lub „1".

KWANTOWY BIT, CZYLI KUBIT

Podstawowym nośnikiem informacji dla urządzenia, które nazwalibyśmy komputerem kwantowym, nie jest bit, ale jego bardziej skomplikowany kwantowy odpowiednik nazywany kubitem (ang. qubit). Tej nazwy użył jako pierwszy w 1995 roku amerykański fizyk Benjamin Schumacher w pracy, która okazała się podwaliną teoretycznych rozważań na temat kwantowego kodowania informacji. Precyzyjna definicja kubitu brzmi: kubit to taki układ kwantowy, którego przestrzeń stanów jest dwuwymiarową przestrzenią Hilberta. Zdaję sobie sprawę, że taka definicja nie za wiele mówi niewtajemniczonym i dlatego lepiej jest posłużyć się jakimś konkretnym przykładem. Okazuje się, że dobrze znamy przynajmniej jeden doskonały nośnik kubitu. Jest to foton!

Tak! Foton, a dokładniej mówiąc polaryzacja fotonu, to jedna z najprostszych fizycznych realizacji kubitu. Jak pamiętamy, każdy foton oprócz tego, że ma określoną energię, niesie również informacje o polaryzacji promieniowania, którego jest nośnikiem. Przypomnijmy, że poznanie polaryzacji fotonu nie zawsze jest do końca możliwe (MT 11/2009), choć w pewnych sytuacjach sprawa jest bardzo prosta. Jeśli foton jest spolaryzowany pionowo, to zawsze przechodzi przez pionowo ustawiony polaryzator i zawsze jest pochłaniany przez polaryzator ustawiony w poziomie.

Kwantowy BIT czyli KUBIT

Analogicznie jest z fotonem spolaryzowanym w poziomie (jest pochłaniany przez polaryzator ustawiony pionowo i zawsze przepuszczany przez polaryzator ustawiony poziomo). Jeśli zatem dopuszczalibyśmy tylko te dwa kierunki polaryzacji fotonu, to mielibyśmy do czynienia ze zwykłą klasyczną informacją, którą możemy dokładnie poznać. Foton pionowy moglibyśmy utożsamić z bitową wartością „1", a spolaryzowany poziomo z wartością „0". Za pomocą pionowo ustawionego polaryzatora moglibyśmy JEDNOZNACZNIE rozstrzygnąć, którą z wartości on reprezentuje.

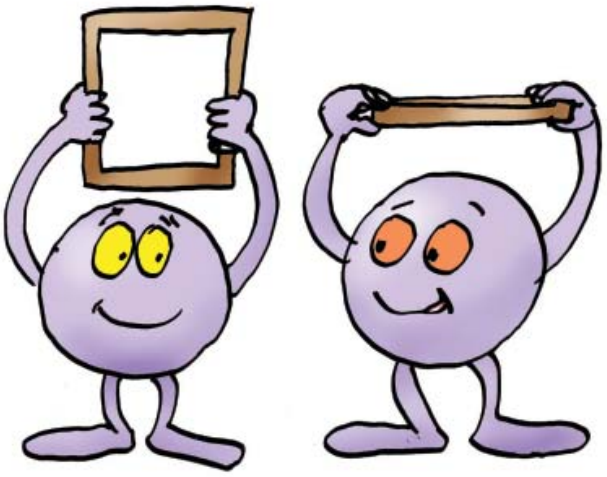
Przypomnijmy jednak (MT 12/2009), że foton oprócz dwóch wyróżnionych polaryzacji (pionowej i poziomej), może mieć również np. polaryzację pośrednią, którą nazywaliśmy skośną. W sytuacji, gdy taki foton pada na polaryzator ustawiony pionowo, nie ma pewności, jaki będzie rezultat. Jak pamiętamy, połowa takich fotonów przechodzi na drugą stronę polaryzatora, a druga połowa jest przez niego pochłaniana. Taki skośnie spolaryzowany foton jest jakby probabilistyczną mieszaniną (w tym przypadku z jednakowym prawdopodobieństwem) dwóch fotonów: pionowego i poziomego. Ale to przecież jeszcze nie wszystkie możliwości. Foton może być mieszaniną (fizycy nazywają to superpozycją) tych dwóch fotonów w dowolnych proporcjach. Tym samym JEDEN foton może jakby kodować nie tylko klasycznie rozróżnialne stany „0" i „1", ale również wszystkie stany kwantowe, które są ich kwantowymi superpozycjami. Foton może jakby jednocześnie być po trosze „zerem" i po trosze „jedynką" w proporcjach w jakich uznamy za stosowne.

Nie muszę chyba nikogo przekonywać, że taki sposób kodowania informacji to prawdziwa innowacja. Do tej pory każdy pojedynczy nośnik miał ściśle przypisany stan bitowy: „0" lub „1". Nośnik informacji kwantowej może również przyjmować te wartości. Ale może również być w takim fizycznym stanie kwantowym, że do czasu wykonania pomiaru wiadomo jedynie, jakie jest prawdopodobieństwo, że ma przypisany stan „0", a jakie, że stan „1". Nauczeni naszymi wcześniejszymi lekcjami wiemy, że taka niepewność nie wynika z tego, że zbyt słabo umiemy jego stan zmierzyć, ale wynika wprost z praw przyrody, które jego zachowaniem rządzą!

CZY GRA JEST WARTA ŚWIECZKI?

Polaryzacja fotonu to dobry nośnik kwantowej informacji, gdy chcemy tę informację przesyłać na odległość. Bardzo słabo nadaje się on natomiast jako nośnik służący do trwałego przechowywania informacji. Jest to zatem kwantowa innowacja w stosunku do impulsów światła przesyłanych za pomocą światłowodów. Krótko mówiąc, jeśli zamiast przesyłać klasyczne impulsy elektromagnetyczne światłowodem, zaczniemy przesyłać nim pojedyncze fotony, których kwantowy stan polaryzacyjny będziemy mogli dobrze kontrolować, to będziemy mieli możliwość przesyłania kwantowej informacji na odległość.

Można się teraz zatrzymać na chwilę i zastanowić, czy taka zmiana rzeczywiście jest dużą innowacją w porównaniu do tego, co mieliśmy wcześniej. W pewnym sensie wszystko zależy od tego, jak tę możliwość wykorzystamy. Jeśli nie będziemy dość roztropni, to może się szybko okazać, że takie otwarcie nowych możliwości jest jedynie uciążliwym dodatkiem, z którym ciężko jest sobie poradzić. Jednak jeśli na chwilę wrócimy np. do omawianego przez nas wcześniej protokołu BB-84 umożliwiającego generowanie absolutnie bezpiecznego klucza kryptograficznego (MT 02/2010), to szybko przekonamy się, że kubit to jednak nie jest wcale taka głupia sprawa.

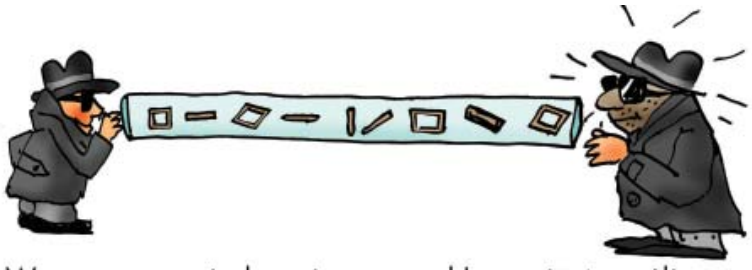


Polaryzacja fotonu, to jedna z najprostszych fizycznych realizacji kubitu

W tamtej sytuacji osoby A i B przesyłały sobie właśnie, choć w dość prymitywny sposób, kwantową informację. Wykorzystywały one bowiem tę dodatkową możliwość, którą dają kubity, a której nie mają zwykłe bity. Wykorzystywały one fakt, że polaryzacja fotonu nie musi być ani pozioma (zero), ani pionowa (jeden), ale może być również skośna albo antyskośna. To powodowało, że wygenerowanie bezpiecznego klucza było możliwe. A to jest jedynie najprostsze wykorzystanie nowych możliwości oferowanych przez kubity.

PRAWDZIWA INNOWACJA

Prawdziwa innowacja i ogromna przewaga kwantowego przetwarzania informacji pojawia się jednak dopiero wtedy, gdy przypomnimy sobie najbardziej fenomenalne zjawisko przewidywane przez mechanikę kwantową i potwierdzone eksperymentalnie. Chodzi mi oczywiście o kwantowe splątanie (MT 04/2010), które powoduje, że pomiędzy cząstkami kwantowymi mogą istnieć korelacje, które nie mają żadnych analogii w świecie klasycznym. Odpowiednie wykorzystanie zjawiska kwantowego splątania cząstek w mikroświecie, które w fizyce pojawiło się za sprawą Einsteina, Podolsky'ego i Rosena, otwiera niewyobrażalne możliwości i może naprawdę zrewolucjonizować cały świat współczesnej informatyki. Przypomnijmy, że w najprostszym przypadku – splątania tylko dwóch fotonów – możemy mieć do czynienia z sytuacją, w której wynik pomiaru polaryzacji każdego z nich osobno jest całkowicie losowy i nieosiągalny, a zarazem równoczesny pomiar polaryzacji obydwu fotonów jest bardzo silnie skorelowany, tzn. jeśli wykonamy pomiar na jednym z fotonów, którego wynik jest całkowicie losowy, to wykonanie pomiaru na drugim z nich w tej samej bazie polaryzacyjnej jest już całkowicie zdeterminowane. Jest tak pomimo tego, że gdybyśmy wykonali pomiar tylko na drugim fotonie, to wynik byłby wtedy całkowicie losowy. Splątanie kwantowe powoduje, że wykonanie pomiaru na jednym z fotonów całkowicie zmienia



Wygenerowanie bezpiecznego klucza jest możliwe

wyniki potencjalnych pomiarów na fotonie drugim i odwrotnie. Istnieje zatem bardzo silna zależność pomiędzy pomiarami wykonywanymi na dwóch fotonach równocześnie, choć zrealizowanie pomiaru tylko na jednym z nich jest całkowicie losowe.

Wydawać mogłoby się, że splątanie kwantowe jest raczej dużym skomplikowaniem procesu przetwarzania informacji niż pomocnym efektem. Tak też myśleli fizycy jeszcze kilkanaście lat temu. Jednak dziś znamy już przynajmniej jeden przykład, w którym splątanie kwantowe może diametralnie przyśpieszyć numeryczne rozwiązywanie problemu.

ALGORYTM SHORA

Zapewne, Drogi Czytelniku, pamiętasz podstawowe zagadnienie kryptografii klasycznej (MT 01/2010). Jej bezpieczeństwo jest oparte na naszym przekonaniu, że rozłożenie dużej liczby na czynniki pierwsze jest zadaniem bardzo trudnym i czasochłonnym (nawet dla najszybszych komputerów) w porównaniu do problemu odwrotnego – pomnożenia przez siebie liczb pierwszych. Jeśli ktoś umiałby rozkładać duże liczby na czynniki pierwsze w rozsądnym czasie, to mógłby łamać powszechnie dziś używane, np. w Internecie, klucze kryptograficzne. Choć nie jest to udowodnione, to wydaje się jednak prawdą, że czas potrzebny na rozłożenie danej liczby na czynniki pierwsze klasycznym algorytmem rośnie **wykładniczo** wraz z liczbą cyfr tworzących liczbę. Zwiększając zatem nieznacznie liczbę cyfr danej liczby złożonej, znacznie wydłużamy czas potrzebny na jej rozłożenie. To sprawia, że wiara w bezpieczeństwo klasycznej kryptografii wydaje się usprawiedliwiona.

W roku 1995 amerykański informatyk teoretyk Peter Shor opublikował pracę, w której wykazał, że gdyby istniało urządzenie, które wykorzystując kwantowe splątanie, potrafiłoby przetwarzać informację zapisaną w kubitach, to można byłoby je wykorzystać do rozkładania dużych liczb na czynniki pierwsze. W swojej pracy Shor podał po prostu algorytm, jak to urządzenie, w zgodzie z prawami mechaniki kwantowej, miałoby działać. Nie byłoby w tym może nic ciekawego, gdyby nie dodatkowy wniosek postawiony w tej pracy: zaproponowany kwantowy algorytm rozkładania liczb na czynniki pierwsze jest bardzo szybki i czas potrzebny na rozłożenie danej liczby rośnie jak **trzecia potęga** liczby cyfr tworzących tę liczbę. W odróżnieniu zatem od sytuacji poprzedniej rośnie **wielomianowo**, co oznacza, że jest to przyspieszenie niewyobrażalne.

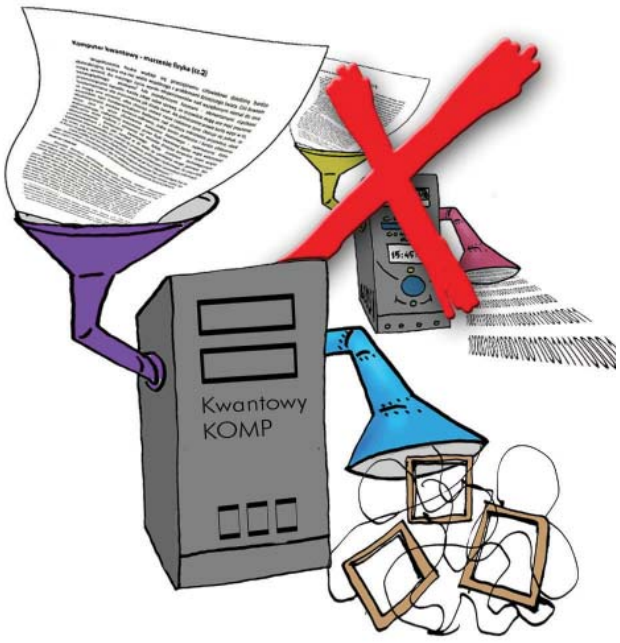
Wyobraźmy sobie dla przykładu, że oba algorytmy potrzebują tyle samo czasu, aby rozłożyć dziesięciocyfrową liczbę na czynniki pierwsze. Jeśli teraz zwiększymy liczbę cyfr tej liczby dwukrotnie (do dwudziestu), to algorytm klasyczny będzie potrzebował na jej rozłożenie ponad 20 000 razy czasu więcej. Algorytm kwantowy tylko 8 razy! Ale np. gdyby oba algorytmy potrzebowały takiego samego czasu na rozłożenie liczby pięćdziesięciocyfrowej, to rozłożenie liczby dwa razy dłuższej (czyli stucyfrowej) zajęłoby w przypadku klasycznym ponad 5 000 000 000 000 000 000 000 razy więcej czasu. Algorytm Shora na to zadanie potrzebowałby znów jedynie 8 razy więcej czasu!

Po publikacji Shora wszystkim naukowcom otwarły się szeroko oczy. Oto stało się dla wszystkich oczywiste, że jeśli nauczymy się przetwarzać informację w sposób kwantowy, to będziemy mogli rozwiązywać problemy, które do tej pory, ze względu na złożoność obliczeniową, wydawały się zupełnie nierozwiązywalne. Choćby takie problemy, jak dokładne i długoterminowe przewidywanie pogody, dokładne symulowanie procesów chemicznych w czasie rzeczywistym czy problem szybkiego analizowania informacji zakodowanej w niciach DNA, do tej pory są poza naszym zasięgiem. Możliwość przetwarzania informacji w sposób kwantowy sprawiłaby, że to w końcu dałoby się zrobić!

IDEA KOMPUTERA KWANTOWEGO

Teraz jesteśmy już gotowi, aby wyjaśnić, czym miałby być owy mityczny komputer kwantowy. Miałoby to być takie urządzenie, które potrafiłoby przetwarzać informację kwantową dostarczaną mu w postaci kubitów i na tej podstawie generować inną informację kwantową na swoim wyjściu. Krótko mówiąc, zamiast przetwarzania ciągu „zer" i „jedynek" miałby przetwarzać ciągi ich kwantowych superpozycji. Dobry komputer kwantowy mógłby również przetwarzać informację zapisaną w kwantowych stanach splątanych kilku kubitów. Dzięki temu mógłby wykorzystać w pełni możliwości, jakie daje mechanika kwantowa i na przykład z powodzeniem realizować algorytm Shora.

Do dziś komputera kwantowego z prawdziwego zdarzenia nie udało się skonstruować i prawdopodobnie jeszcze przez najbliższą dekadę to się nie powiedzie. Ale nasza wiara, że tak się w końcu stanie, jest bardzo duża. Chcielibyśmy bowiem po raz kolejny pokazać wszystkim niedowiarkom, że inwestowanie w badania podstawowe ma ogromne znaczenie dla naszego rozwoju. Nawet jeśli w pierwszym odruchu wydaje się to mało sensowne. ●



Idea komputera kwantowego