

Można spojrzeć na splątane kwantowo fotony wybiegające z kryształu oświetlonego laserem.



# W poszukiwaniu natury świata

Na PWr dysponujemy, działającą w ramach NLTK, jedyną w Polsce i jedną z nielicznych na świecie, w pełni wyposażoną pracownią kryptografii kwantowej, opartą zarówno na niesplątanych, jak i na splątanych kwantowo fotonach.

**K**ierownikiem NLTK na PWr jest jego organizator prof. Lucjan Jacak, który przedstawia swoją dziedzinę.

**Coraz częściej słyszy się terminy: informatyka kwantowa, komputer kwantowy, kropka kwantowa czy kryptografia kwantowa. Co to wszystko znaczy?**

■ Rzeczywiście, można spotkać obecnie liczne artykuły naukowe i popularne (te ostatnie między innymi w *Świecie Nauki*), odnoszące się do kwantowej natury nie tylko materii w mikroskopowej skali, ale też do coraz śmielej formułowanych opinii o kwantowych aspektach informatycznych, a nawet psychologicznych. To po części przejaw mody, a czasem nawet dziennikarskich nadinterpretacji, ale też od samego początku formułowania mechaniki kwantowej, w latach dwudziestych i trzydziestych

XX w., nie ulega wątpliwości, że mechanika kwantowa stanowi zupełnie nieintuicyjne ujęcie otaczającej nas rzeczywistości i ma dużo szersze odniesienia niż tylko opis dynamiki mikrocząstek. Nieklasyczny i przez to wymykający się intuicji charakter mechaniki kwantowej jest daleko bardziej niecodzienny niż relatywistyczny nurt teorii względności. Warto podkreślić, że obu tych koncepcji XX-wiecznej fizyki nie udało się dotąd pogodzić ze sobą, co wskazuje, że niewiele jeszcze wiemy o prawdziwej naturze świata. Fakt eksperymentalnego potwierdzenia mechaniki kwantowej w setkach szczegółowych fizycznych

*„Kwantowych komputerów wokół nas w przyrodzie wszędzie pełno – to one realizują rzeczywistość na mikroskopowym poziomie, ale nie chcę ani nas słuchać, ani dzielić się z nami swoimi możliwościami.”*



prof. Lucjan Jacak  
kierownik NLTK  
na PWr

realizacji umocnił przekonanie, że jej odmienność naprawdę odzwierciedla zaskakujące oblicze rzeczywistości. W ostatnich latach wraca się do dyskusji nad różnymi, znanymi już wcześniej, aspektami kwantowej mechaniki. Uwagę przyciąga np. nielokalny efekt kwantowego splątania, który manifestuje się nieklasycznym i przez to dziwnym związkiem na odległość, który jest obserwowany w licznych eksperymentach. Mechanika kwantowa dotyczy materii w skali atomowej, ale wydaje się mieć też znacznie szersze odniesienia. Przejawiają się one w nieklasycznym charakterze zachowania złożonych układów. Dziesiątki nagród Nobla w obszarze mechaniki kwantowej (także nagroda Nobla w 2012 r.) ugruntowały jej mocną pozycję w różnych dziedzinach: od fizyki poprzez nowoczesną technologię i informatykę po filozofię.

**Na czym polega ta moc mechaniki kwantowej?**

■ Trudno zapewne zawrzeć właściwą odpowiedź w jednym zdaniu – to wieloaspektowa, ogromna dziedzina. Jej podstawą jest znana powszechnie zasada nieoznaczoności, według której różne wielkości fizyczne podlegają prawidłowości: im dokładniej zdołamy poznać jedną wielkość, tym bardziej inne okazują się wtedy nie-



KAPITAŁ LUDZKI  
NARODOWA STRATEGIA SPÓJNOŚCI



Politechnika Wroclawska

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



określone. Oznacza to w istocie, że cząstka nie ma trajektorii (nie można określić równocześnie jej położenia i prędkości) – kwantowa cząstka nie jest zatem klasycznym punkcikiem. No a czym jest? – Jest bytem podlegającym pomiarom z ograniczeniami nieoznaczoności. Od ponad 80 lat trwają niekończące się dyskusje, jak to należy rozumieć. Mimo że nie osiągnięto tu zgody, znakomicie umiemy w praktyce przewidywać zachowanie tych kwantowych bytów i coraz lepiej obserwować je eksperymentalnie. Cała rzecz właśnie w eksperymencie, czyli pomiarze – pomiar kwantowy w odróżnieniu od zwykłego, klasycznego (jak mierzenie np. długości stołu) jest niszczący, niepowtarzalny i przez to wyróżniający obserwatora wykonującego ten pomiar. W przeciwieństwie do klasycznych pomiarów, które nie zmieniają stanu mierzonego obiektu, pomiar kwantowy niszczy nieodwracalnie stan mierzony i dostarcza bardzo fragmentarycznej informacji o tym stanie, który właśnie przestaje istnieć w wyniku pomiaru. Większość informacji jest bezpowrotnie tracona w czasie obserwacji. Równocześnie pomiar kreuje nowy stan mierzonego układu, zupełnie bez związku z jego przeszłością i w sposób całkowicie przypadkowy. Stąd płyną obawy, że przy takich przejściach kwantowych



Na ponad półtonowym stabilizowanym stole spektrometr ramanowski firmy Horiba-Yvone-Jobin o wyjątkowych możliwościach pomiarowych, kwarcowa optyka pozwala na pracę także w ultrafiolecie.

do uwagi, że „cień nie rzuca już cienia”, a właśnie cień to jakby wynik pomiaru kwantowego – niesie tylko część informacji o obiekcie rzucającym cień. Paradoks Zenona został potwierdzony eksperymentalnie – pilnie obserwowany przez fotony elektron nieruchomieje. Skoro jednak sami ru-

ki kwantowej w postaci wieloświatów, zaproponowana przez Hugh Everetta w 1957 r. Według tej koncepcji wieloświaty to istniejące realnie możliwe wyniki pomiarów, które są odwiedzone przez kwantowy układ właśnie w wyniku tych pomiarów. Ta uspokajająca koncepcja istnienia nie mówi nam jednak, gdzie te wieloświaty pomieścić. Niemniej znajduje do dziś wielu zwolenników. Bardziej powszechnie akceptowana jest jednak interpretacja kopenhaska, łączona z Nielsem Bohrem i podkreślająca probabilistyczny, nieprzewidywalny charakter pomiaru kwantowego. Te aspekty mechaniki kwantowej wyraźnie prowokują filozofów, ale mają i praktyczne odniesienia.



Zestaw kryptografii kwantowej na niesplątanych fotonach – na terminalach Alice i Boba szwajcarskiej firmy idQuantique, Alicja w krainie czarów i Bob Marley (w informatyce kwantowej przyjęto terminy Alice i Bob dla określenia stron kwantowej komunikacji, która może być utrudniana z kolei przez Eve (*eavesdropper*), choć to nie proste zadanie)

można by się zgubić w czasie i nigdy nie powrócić, bo kwantowe pomiary są niedeterministyczne. Nie rozumiemy, dlaczego rzeczywistość zachowuje się w taki sposób, ale też wszystkie doświadczenia prowadzone od ponad 80 lat potwierdzają ten scenariusz pomiaru nazywany kolapsem von Neumanna. Ciekawostką jest, że szybkie powtórzenie pomiaru tej samej wielkości zatrzymuje ewolucję – jest to kwantowy paradoks Zenona. Posługując się przenośnią, odnieść to można

szamy rękami, to pewnie nie jesteśmy obserwowani bez przerwy – albo przynajmniej nie kwantowo.

Kreowanie nowego stanu w wyniku pomiaru też jest nadzwyczaj zagadkowe. Nie bardzo pasuje do tradycyjnego wyobrażenia o istnieniu obiektywnej rzeczywistości, gdy okazuje się ona zależna od pomiaru (obserwacji) i modyfikowana jest w czasie tego pomiaru, do tego w przypadkowy sposób. Nic dziwnego, że dużą popularność zdobyła interpretacja mechani-

**No właśnie – na czym polegają te praktyczne odniesienia?**

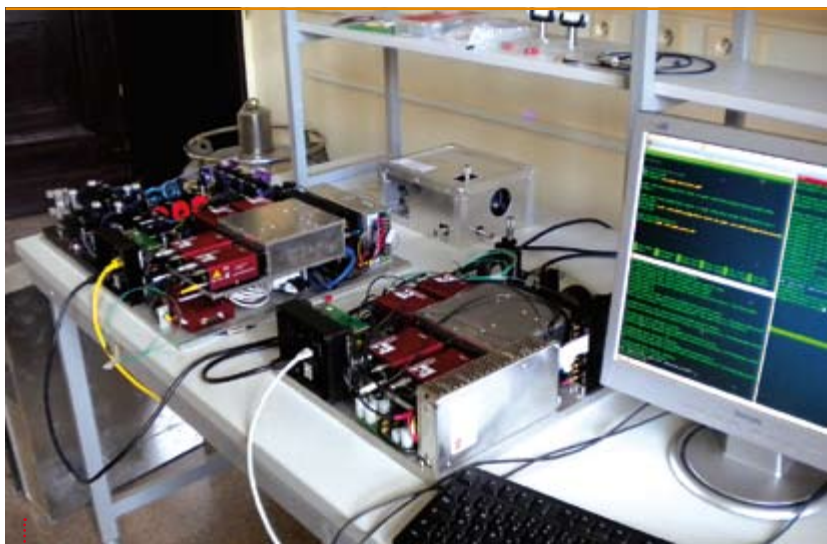
Jeśli zgodzić się, że cała materia ma mikroskopową atomową i subatomową strukturę, to mechanika kwantowa, obowiązująca w mikroskali, leży w tle całej postrzeganej rzeczywistości. W niektórych sytuacjach mikroskopowa struktura chowa się za makroskopowymi pozorami klasycznej fizyki, w wielu jednak przypadkach nie da się ukryć struktury kwantowej. Nadprzewodnictwo i nadciekłość to dobrze znane i zadziwiające manifestacje kwantowej mechaniki, których nie można właśnie ukryć na makroskopowym poziomie. Fakt niemożności zatrzymania nadciekłego lub nadprzewodzącego prądu siłami tego świata wynika z nieoznaczoności prędkości układu odniesienia i liczby cząstek. Jeśli nie możemy policzyć, ile jest cząstek w układzie, bo wszystkie mają np. energię równą zero i pęd równy zero, co daje w sumie zero niezależnie od ich liczby, jak w nadciekłym kondensacie, to ustala się – zgodnie z zasa-



► dą nieoznaczoności – konkretna prędkość układu odniesienia i nie można jej zmienić aż do momentu, gdy będziemy w stanie policzyć cząstki. W ustalonym wtedy układzie odniesienia kondensat ma określoną prędkość, co obserwujemy jako przepływ materii niepodlegający oporowi czy lepkości. Jeśli tylko wzbudzimy cząstki, np. przez podgrzanie, co pozwoli je rozróżnić i policzyć, nadprzewodnictwo znika. Reakcje jądrowe i wybuchy atomowe to też kwantowa mechanika. Wielkie i trochę przesadzone oczeki-

kwantowych komputerów wokół nas w przyrodzie wszędzie pełno – to one realizują rzeczywistość na mikroskopowym poziomie, ale nie chcą ani nas słuchać, ani dzielić się z nami swoimi możliwościami. Komputerem kwantowym jest dowolny układ kwantowy, którym możemy sterować w deterministyczny sposób, realizując specjalnie dobrany kwantowy algorytm. Umieemy to zrobić w ograniczony sposób – manipulując kwantowo cząstkami w liczbie nieprzekraczającej 10, niosącymi najwyżej 10 tzw. qubitów. Warto do-

wości informatyczne rosną bowiem eksponencjalnie z zasobami, a  $2^{1000}$  jest liczbą większą niż liczba cząstek we wszechświecie. Problem polega na tym, że wraz ze wzrostem liczby qubitów rośnie też eksponencjalnie dekoherencja – niekontrolowany wpływ informacji kwantowej na skutek nieuniknionych zaburzeń z otoczenia. Dekoherencja jest główną przeszkodą na drodze rozwoju kwantowej informatyki. W ostatnich latach wykazano (także przy naszym udziale), że niemożliwe jest opanowanie dekoherencji w technologii kropek kwantowych sterowanych światłem. Uwaga konstruktorów komputerów kwantowych zwróciła się zatem w stronę sterowania magnetycznego, zwłaszcza w nadprzewodzących strukturach. W 2012 r. „garażowa” firma kanadyjska D-wave zaoferowała pewien rodzaj komputera kwantowego, 128-qubitowego, wprawdzie nie pełnosprawnej maszyny wykorzystującej kwantowe splątanie (co jest sednem kwantowego przetwarzania informacji), ale urządzenia rozwiązującego zagadnienie optymalizacji poprzez kwantową procedurę. Kwantowy komputer D-wave można kupić za 10 mln dolarów (kupił go Lockheed Martin i ponoć też Google). Także w 2012 r. IBM zademonstrował 3-qubitową bramkę do skalowalnego komputera ze splątaniem kwantowym – obie konstrukcje w technologii nadprzewodnikowej. Pełnosprawny komputer kwantowy to wielce niebezpieczne urządzenie – nie dość, że bez kłopotu zapanowałby nad infrastrukturą światowej klasycznej informatyki, to zmieniłby z pewnością



System do kryptografii kwantowej na splątanych fotonach.

wania wiążą się z tzw. nanotechnologią, czyli manipulowaniem materią na poziomie prawie atomowym, ale już w takiej skali, w której niezbędny jest opis kwantowy. Kropki kwantowe to takie właśnie obiekty nanometrowych rozmiarów, opisywane przy pomocy mechaniki kwantowej i często stosowane do konstruowania nowych przyrządów, zwłaszcza półprzewodnikowych. Daleko tu jednak od spełnienia medialnie rozbudzonych oczekiwań o nanotechnologicznym panaceum na niemal wszystko.

**A informatyka kwantowa? Czy to też tylko medialny hallmark nowoczesnych trendów, czy może jednak coś więcej?**

■ Gdy uświadomiono sobie, że nie istnieje informacja bez fizycznego nośnika informacji, zwrócono uwagę na kwantowy, a nie tylko klasyczny – dotychczas stosowany w praktyce – nośnik informacji. Powstała w ten sposób koncepcja kwantowej informatyki. Ze względu na odmienną od klasycznego specyfikę kwantowego nośnika, zmiany są tu zasadnicze, a przewagi kwantowej informacji – bezdyskusyjne. Pozwala ona bowiem osiągnąć większą pojemność informatyczną i sprawność przetwarzania. Trudność polega jednak na tym, że o ile klasyczne nośniki informacji są świetnie opanowane technicznie, to z kwantowymi jest znacznie gorzej. Można powiedzieć, że

dać, że opanowanie manipulacji setką cząstek byłoby przełomem, a tysiącem cząstek – oznaczałoby już panowanie nad informatycznym światem. W komputerach kwantowych możli-

**Narodowe Laboratorium Technologii Kwantowych (NLTK)**

NLTK to ogólnopolska sieć nowoczesnych laboratoriów z zakresu kwantowych technologii ufundowana przez Narodowe Centrum Badań i Rozwoju.

Pomysł wsparcia krajowego eksperymentu w ultranowoczesnym obszarze powstał wśród fizyków teoretyków. Czołową rolę odegrało tu środowisko LFPPi, tj. sieci krajowej KBN pn. Laboratorium Fizycznych Podstaw Przetwarzania Informacji. Warto przypomnieć, że sieć ta utworzona została po części właśnie we Wrocławiu w 2003 r. na zorganizowanej specjalnie konferencji, w wyniku wspólnej inicjatywy Centrum Fizyki Teoretycznej PAN w Warszawie, PWr, UW, UJ, UG, UMK, UŁ i innych – łącznie ponad 20 czołowych instytucji naukowych w kraju. Sieć podjęła się następnie realizacji zamawianego projektu ministerstwa (wtedy MNiI) pn. *Kwantowa Informatyka i Kwantowa Inżynieria*.

Realizacja tego projektu okazała się dużym sukcesem o międzynarodowym znaczeniu. Wyniki opublikowano w około 150 pracach w najbardziej renomowanych czasopismach międzynarodowych. PWr miała też znaczący swój udział w tym osiągnięciu. Wątek projektu zamawianego, koordynowany przez Politechnikę Wrocławską, zaowocował około 1/3 z tych publikacji. Doceniając rozwój mechaniki kwantowej i aktywności środowiska krajowego w obszarze fizyki kwantowej (wspartej też kilkoma projektami FP EU) ministerstwo wraz z NCBR zdecydowało się na wielkoskalową in-

westycję w tej dziedzinie. Do zespołów LFPPi dołączyli także eksperymetatorzy, głównie zajmujący się optyką kwantową z Torunia (UMK i FAMO – Krajowe Laboratorium Fizyki Atomowej, Molekularnej i Optycznej w Toruniu), Warszawy (UW i IF PAN) i Krakowa (UJ). Z ogólnej kwoty blisko 50 mln zł projektu NLTK, 7,5 mln przypadło Politechnice Wrocławskiej.

Poza PWr laboratoria NLTK powstały też w PAN, na UW, UJ i UMK.

Laboratoria NLTK mają charakter otwarty. Oferują sprzęt najnowocześniejszy i często unikalny. W NLTK na PWr powstały cztery pracownie:

■ Pracownia kryptografii kwantowej – jedyna w Polsce, a i unikalna w skali światowej – wyposażona jest w zestawy kwantowej dystrybucji tajnego klucza kryptograficznego w technologii splątanych kwantowo i niesplątanych fotonów. Pracownia prowadzi współpracę z liderami światowymi w tej dziedzinie – idQuantique (spin-off Uniwersytetu w Genewie) i AIT (spin-off Uniwersytetu w Wiedniu). Obecnie w dziedzinie kryptografii kwantowej liczą się tylko jeszcze dwie firmy Qmagi (Raytheon, USA) i Toshiba (Cambridge); u nas prowadzone są teraz prace rozwojowe tej przyszłościowej technologii (kilka dużych projektów przy współpracy zewnętrznej). Badania te mają istotne znaczenie strategiczne dla oryginalnego udziału Polski w nowym obszarze bezpieczeństwa informatycznego. O znaczeniu

oblicze technologii i cywilizacji. Była by np. możliwa teleportacja, co prowadzić by mogło do trudnych do przewidzenia konsekwencji i zastosowań. Może lepiej, że nie jest łatwo zbudować taki komputer. Można by było jednak ograniczać władzę kwantowych komputerów, stosując kwantową kryptografię. Co ciekawe, ta technologia jest już w pełni dojrzała – nie stawia bowiem tak ostrych wymogów ograniczenia dekoherencji.

**Czy kryptografia kwantowa zatem jest strategiczną bronią wobec ewentualnego ataku kwantowej informatyki?**

■ Tak właśnie się wydaje. Obecnie kryptografia kwantowa oferuje bezwzględnie bezpieczny sposób dystrybucji klucza publicznego w systemach kryptograficznych, nawet dla klasycznej informatyki. Połączenia informatyczne o najwyższych standardach bezpieczeństwa to właśnie systemy QKD, czyli *quantum key distribution*. Na PWR dysponujemy, działającą w ramach NLTK, jedyną w Polsce i jedną z nielicznych na świecie, w pełni wyposażoną pracownią kryptografii kwantowej, opartą zarówno na niesplątanych, jak i na splątanych kwantowo fotonach. Warto zauważyć, że te ostatnie systemy są bardzo nieliczne: tylko cztery na świecie – jeden w Wiedniu, jeden na Dalekim Wschodzie, a dwa we Wrocławiu. Kryptografia kwantowa ma też jednak bardzo silne ograniczenia – jest techniką *one-to-one*, no a jej zasięg w światłowodach ogranicza się do rzędu 100 km (w kosmosie, w swobodnej przestrze-



Sztuczne słońce w pracowni fotowoltaiki wiernie odtwarza spektrum naszej gwiazdy.

Rozmawiała:  
Maria Kiska  
Zdjęcia:  
archiwum autora

ni, może być on większy). W Tokio i w Wiedniu zostały zainstalowane próbne metropolitalne połączenia, zabezpieczane tą techniką. We Wrocławiu prowadzimy prace rozwojowe w kierunku integracji QKD z komercyjnymi sieciami telecom.

kwantowej kryptografii być może przekonamy się wkrótce wobec postępującego rozwoju informatyki kwantowej. W przypadku praktycznej realizacji skalowalnego komputera kwantowego (coraz śmiało zapowiadane, m.in. przez IBM) klasyczne systemy informacyjne mogą okazać się bezbronne, a klasyczna kryptografia zupełnie nieskuteczna. Może wtedy powstać atrakcyjny rynek kryptografii kwantowej, bezwzględnie bezpiecznej i jedynej techniki zabezpieczania klasycznych systemów informacyjnych przed możliwym atakiem kwantowego komputera.

■ Pracownia fotowoltaiki, czy dokładniej mechanizmów transferu energii w nanostrukturach, znakomicie wyposażona. Warto tu wymienić najlepszej klasy spektrometr ramanowski firmy Horiba-Jobin-Yvone, czy mikroskopię AFM Parka (sił atomowych). Realizowane są tu projekty z nanofotowoltaiki i plazmoniki, mające na celu poszukiwanie usprawnienia ogniw słonecznych nowej generacji: półprzewodnikowych i organicznych „plastikowych”. Badania prowadzone są w kooperacji międzynarodowej i projekty mają charakter zarówno eksperymentalny, jak i bardziej nastawiony na współpracę z fizykami teoretykami.

■ Pracownia modelowania kwantowego – to rozproszony klaster wydajnych stacji roboczych Della z oprogramowaniem specjalistycznym. Jest to wsparcie numeryczne dla szeroko prowadzonych badań w podstawach mecha-

nikii kwantowej, ostatnio u nas ze znaczącymi sukcesami, a wspartych prestiżowymi projektami NCN.

■ Pracownia ultrashybkiej spektroskopii optycznej nanostruktur – tu NLTK doinwestowało istniejące już na PWR bardzo dobrze wyposażone laboratorium i uzupełniło je o cenną, wyjątkowej klasy aparaturę. Prowadzi się tu kilka projektów przy silnie rozbudowanej współpracy międzynarodowej.

NLTK to przede wszystkim oferta dla młodych, którzy mogą realizować w tym laboratorium ciekawe prace dyplomowe i doktorskie. Można korzystać ze sprzętu w całej sieci. Jest to wyjątkowa okazja dostępu i swobody badań na świetnym sprzęcie o światowych standardach w bardzo atrakcyjnych nowoczesnych dziedzinach fizyki kwantowej, coraz powszechniej postrzeganej jako technologia jutra.

Kierownikiem NLTK na PWR jest jej organizator prof. L. Jacak. Przy organizacji i prowadzeniu badań w NLTK nie sposób nie docenić udziału prof. E. Popko, prof. J. Misiewicz, dr. Z. Gumienego, prof. Z. Kuźnickiego (Strasbourg University), dr. A. Janutki, dr. P. Biegańskiego i wielu innych oraz osób zajmujących się administracją i przetargami, w tym bardzo pomocnej i miłej współpracy Biura Zamówień Publicznych PWR. Bardzo wyraźne i często konieczne było też wsparcie ze strony władz rektorskich i administracji centralnej Politechniki Wrocławskiej. Wszystkim im należą się ogromne podziękowania.

**Jak można by ocenić perspektywy kwantowych technologii?**

■ Coraz śmiało formułuje się poglądy, że kolejne rewolucje technologiczne będą silnie związane z mechaniką kwantową. Znaczne przyspieszenie w tym względzie na przełomie wieków związane było z coraz lepszym opanowaniem technik manipulacji kwantowymi stanami, w wyniku nagromadzenia doświadczeń, uzyskanych dzięki gwałtownej miniaturyzacji elektroniki i informatyki. Spintronika i nanotechnologia czerpią z mechaniki kwantowej, ale istotne przełomy zapewne jeszcze przed nami i trudno tu o realistyczne prognozy. Jak zwykle, obecne wysiłki tworzą raczej podstawy niż powodują natychmiastowy postęp – ten może pojawić się gdzieś zupełnie nieoczekiwanie. Mechanika kwantowa jako koncepcja zawładnęła całkowicie współczesną fizyką, ale i tu są poważne wyzwania. Nie wiadomo, jak pogodzić ten schemat z teorią względności, a zwłaszcza z grawitacją. Nie to, żeby nikt nic nie zaproponował – to dziedzina obsadzona od kilkudziesięciu lat przez najwybitniejszych specjalistów na świecie (nic dziwnego, bo lepsze zrozumienie w tym obszarze może oznaczać np. panowanie nad antymaterią). Mimo bezprecedensowych w historii nauki wysiłków w tym zakresie, nie osiągnięto zadowalającego sukcesu w postaci eksperymentalnego potwierdzenia którejśkolwiek z bardzo już abstrakcyjnych koncepcji, jak teoria strun, supersymetria, czy model holograficzny. Wyraźnie widać, że natura ukrywa tu swoje tajemnice i mimo pracy takich ogromnych instalacji jak LHC i coraz lepszych obserwacji astrofizycznych (istnieje bowiem związek skal astronomicznych i atomowych, choćby w czarnych dziurach), postęp na razie jest niewielki. Wszyscy się zgadzają, że problem leży w unikaniu lokalności zarówno przestrzeni, jak i czasu – ale bez eksperymentalnej wskazówki niewiele daje się zrobić – tymczasem obecny eksperyment nie dysponuje jeszcze odpowiednimi możliwościami. Jednak nawet wtedy, gdy zgodzimy się na niepełne poznanie rzeczywistości, musimy stwierdzić, że wykorzystanie kwantowej fizyki, w stopniu już obecnie zweryfikowanym eksperymentalnie, oznaczać może ogromne zmiany technologiczne i związane z tym postęp. «

