

# Umyślny idealny

Mechanika kwantowa dostarczyła ostatnio możliwości idealnego kodowania informacji. Dokładnie chodzi o to że można przesłać klucz jednorazowy w sposób który nie daje szans jakiegokolwiek podsłuchowi. Sprawa zasadza się na działaniu paradoksu EPR. Dzięki możliwości wyprodukowania splecionych ze sobą fotonów można podpatrywać zjawiska na poziomie pojedynczych cząstek elementarnych.

Istnieje możliwość zbudowania kanału informacji, który byłby całkowicie odporny na podsłuch. Oznacza to tyle, że po opuszczeniu urządzenia nadawczego, wszelkie próby wyciągnięcia choćby jednego fotonu skończą się alarmem. Maszynka może działać w oparciu o zjawisko interferencji.

Jest ono dobrze znane od bardzo dawna, a prawidłowo opisane zostało opisane przez Yunga z początkiem XIX w. Było sztandarowym dowodem na falową naturę światła. Wygląda to tak: gdy na drodze światła umieścimy przesłonę z dwoma wąskimi szczelinami w bardzo niewielkiej odległości, to za przesłoną otrzymamy zamiast dwu jasnych pasków, szereg prążków. Najjaśniejszy pojedynczy znajduje się dokładnie po środku, pomiędzy geometrycznym rzutem szczelin na ekran.

To dziwo jest znane dziś prawie wszystkim ze szkół. O wiele mniej znane są aparaty zwane interferometrami. Działają dzięki temu, że światło jest falą. Maszynaria jest nieco tajemnicza, gdy spytać o zasadę zachowania energii. Jak pokręcić śrubą to albo do detektora dociera prawie całe światło, albo nic. Z falogo punktu widzenia sprawa jest prosta: rozdziela się światło ze źródła na dwie wiązki o równym natężeniu. W zależności od przebytej drogi spotykają się one w detektorze albo „grzbiet w grzbiet, dolina w dolinę” czyli w fazie, albo „grzbiet z doliną” czyli w przeciwfazie. W pierwszym przypadku następuje wzmocnienie wiązki, w drugim wygaszenie.

Nieszczęśni uczestnicy wszelkiego rodzaju zajęć związanych z fizyką pamiętają zapewne *elegancki* wzór

$$n\lambda = d\sin\alpha$$

To jest właśnie wzór na położenie maksimum prążka w eksperymencie z dwoma szczelinami.

Sprawa była jasna do początku XX wieku. Wtedy fizycy wpadli na pomysł, jak mianowicie wszystko dokładnie zamieszać i wymyślili w ramach mechaniki kwantowej dualizm korpuskularno falowy. Znaczący poczwierne światło

objawia się raz jako cząstka, raz jako fala. Dla fizyków był to akt rozpacz (ten pomysł) by wyjaśnić kilka szczegółów naszego obserwowanego świata. Jednym z nich było oczywiście zjawisko fotoelektryczne. Wtedy Albert Einstein napisał wzór, za który dostał nagrodę Nobla

$$E = h\nu$$

Ciekawe, że jest to wzór de Broglie'a.

Jakoś łatwiej zmysłom znieść dualizm cząstek elementarnych, ale przyzwyczaić się do myśli, że np. kupka atomów może być falą, to już horror. By zgasić wszelką nadzieję, doświadczenia z tzw. laserem materii potwierdziły w całej rozciągłości paranoiczny obraz tego świata.

Paranoja jest niemal w dosłownym słowa tego znaczeniu: rozdwojenie, zwielokrotnienie, jednocześnie można być i tu i tam, nie będąc nigdzie „tak naprawdę”. To jest nieco poetyckie sformułowanie zasady, że pojęcie toru w mechanice kwantowej nie ma sensu.

Praktyczny skutek jest taki: weźmy sobie kojota który jest prawdziwie cool. Znać opowieść o kojocie który był cool? Jeśli nie, to pytajcie znajomych, kawał jest klasyczny i ktoś zna na pewno. Nasz kojot powinien być cool w skali Kelwina, jakieś ułamki stopnia. Mógłbym wyliczyć ile, ale z góry wiem że naraziłbym się animalsom: będzie to naprawdę bardzo mało. Kiedy dzięki ćwiczeniom Zen, ciekłemu azotowi, helowi i metodom o których strach wspominać osiągnie on ów stan, wyślemy go w drogę w kierunku przesłony z dwoma szczelinami.

Technicznie to jest nieco kłopotliwe do zrealizowania. Obliczałem kiedyś rozmiar interferometru dla kota. Wyszło nieco więcej, niż rozmiar wszechświata. Tym niemniej na nieco mniejszych obiektach eksperymentu dokonano. A rzecz się sprowadza do tego, że ów kojot będzie pokonywał drogę poprzez *obie szczeliny jednocześnie*. Ot taki drobiazg. Wyobraźmy sobie to: mur ceglany z dwoma bramkami w odległości np. 2 metrów. Po pokonaniu przeszkody w sporej (bardzo sporej) odległości na ścianie pokrytej niezaschłym jeszcze betonem nasz kojot zostawia odcisk łapy w miejscu zetknięcia się z nią. Jeśli będziemy mieć setkę takich kojotów i każdy równie cool zostawi swój odcisk, zobaczymy znane z doświadczenia ze światłem prążki. Dokładnie na kawałku muru pomiędzy szczelinami będzie ich najwięcej.

Warunkiem powodzenia ekspedycji jest to, by po drodze nie podglądać w żaden sposób, którędy kojot się przemieszcza. Wystarczy najślabszy błysk światła, można nawet dobrze obliczyć, jak słaby, a będzie po herbacie. Zamiast obrazu interferencyjnego na mokrym betonie będą rozmazane ślady dwu szczelin.

Nie kombinuj z zamykaniem jednej szczeliny, przed, po. Pan Bóg pierwszego dnia stworzenia musiał mieć albo jakiś wyjątkowo dobry antałek wina,

albo pokręcone poczucie humoru. Taka jest fundamentalna (jak dziś ją rozumiemy) zasada konstrukcji świata. To zasada nieoznaczoności. Mówi ona tyle: nie można jednocześnie znać dowolnie dokładnie pędu i położenia cząsteczki. Pisze się to tak

$$\Delta p \cdot \Delta x \geq \frac{h}{2\pi}$$

Tu trzeba powiedzieć występująca we wzorze *stała Plancka* jest naprawdę bardzo mała

$h = 6.6 \cdot 10^{34} \frac{J}{s}$  Proporcje jednak są takie, że gdy wiemy dobrze gdzie cząstka jest (małe  $\Delta x$ ) nie znamy jej pędu ( $\Delta p$  jest duże). Związek pędu z interferencją wydaje się dziwny: o tym za chwilę. Konsekwencja: tor cząstki nie istnieje. Możemy tylko wskazać pewną przestrzeń, gdzie ustawiony detektor ma znacznie większą szansę niż gdzie indziej tyknąć na skutek tego, że cząstka wpadnie do niego. Nie ma to jednak wiele wspólnego z torem cząstki, bo jak tyknie, to koniec z lotem dalej.

Nie ma innego wyjścia: trzeba sobie wyobrazić tak: nawet nasz cool kojot o masie kilkunastu kg pokonuje trasę w formie fali materii. Jak każda fala jest nieco rozmazany i przechodzi o zgrozo jednocześnie obie szczeliny naraz. Ja mu przywalimy w celu przekonania się gdzie jest bodaj jednym fotonem i to o sporej długości, zdechł cool kojot, zostanie zlokalizowany.

Kolejny wzór de Broglie'a pozwoli wyliczyć dosyć dokładnie parametry tego eksperymentu i jak się policzy, to można zważyć, że to się da przeprowadzić. Długość fali materii związanej z kojotem wynosi

$$\lambda = \frac{h}{p}$$

Dlatego że *stałą Plancka* tak mała,  $p$  jest iloczynem masy i prędkości kojota: dla „ludzkich” wielkości długość fali  $\lambda$  będzie koszmarnie mała. Z tej przyczyny wystarczy „kopniak” od pojedynczego fotonu, by cały eksperyment zaburzyć.

Ten związek wiąże zasadę nieoznaczoności z doświadczeniem z dwoma szczelinami. Znajomość pędu oznacza znajomość długości fali, tę zaś można wyznaczyć z obrazu interferencyjnego za pomocą wzoru *eleganckiego*  $n \cdot \lambda = d \cdot \sin \alpha$ . Był już na początku.

Oznacza to właśnie taki paranoiczny obraz świata: coś jest (choć nie *jest a może być*) jednocześnie w dwu miejscach. Jak się uniemożliwi temu czemuś być w jednym z tych miejsc, wszystko zaczyna przebiegać zupełnie inaczej.

W realnej aparaturze nie musimy posługiwać się obiektami z komiksów: fotony są wystarczająco cool. Idea jest taka: wysyłamy światło po dwu

drogach i na końcu sprawdzamy, czy mamy interferencję. Jeśli mamy, tor jest czysty, nikt nas nie podgląda.

Konstrukcja nie jest niestety wolna od technicznych zależności. Im dokładniejsza aparatura, tym jesteśmy bezpieczniejsi. Kiedy jednak zejdziemy do transmisji pojedynczych fotonów, wówczas nie sposobu na szpiegowanie: większej dokładności już nie potrzeba.

Jak to zrealizować w praktyce? Zaczniemy od nieco gorszego rozwiązania. Po prostu połączmy stację odbiorczą i nadawczą dwoma światłowodami. W stacji odbiorczej ustawiamy interferometr tak by w jednym detektorze było zupełnie ciemno, a w drugim całkiem jasno. Jeśli ktoś zacznie się dobierać do jednego ze światłowodów, do ciemnego detektora zaczęą docierać natychmiast fotony. Dzieje się tak, bo jeśli tylko po drodze został ustawiony detektor, to wiemy którą drogą pobiegł foton, a to oznacza lokalizację i koniec interferencji.

W konstrukcji jest poważna dziura: można oczywiście przeciąć oba światłowody, odbierać sygnały i emitować swoją własną ich replikę. Z technicznego punktu widzenia jest dosyć karkołomne. Rozsądnie do realizacji takiej łączności jest wybrać połączenia biegnące zupełnie różnymi drogami, kilkanaście kilometrów od siebie. Wykonanie szpiegowskiego połączenia w takich warunkach może być trudne, zwłaszcza, że trzeba je wyjustować z dokładnością do kawałka długości fali.

Nawet z taką teoretyczną konstrukcją można sobie poradzić. Weźmy np. w stacji nadawczej podłączmy inny interferometr do toru. Zrobimy tak: przepuścimy światło przez obie połówki naszego połączenia i jednocześnie przez inny światłowod o zbliżonej długości, który może sobie leżeć spokojnie na podłodze w stacji nadawczej. Drobiazg: w stacji odbiorczej trzeba połączyć ze sobą oba kawałki światłowodu i podczas inspekcji nie można niczego odbierać.

Teraz już można stwierdzić z całą pewnością, czy ktoś nas podpatruje. Jeśli tylko nie oda się uzyskać interferencji, znak, że łapać kałasze i... na Soplicę!

Całkiem do niedawna nie była możliwa łączność za pomocą pojedynczych fotonów. Dokładniej mówiąc dalej nie jest możliwa. Przyczyną są te same zasady mechaniki kwantowej, które nie pozwalają podpatrywać bezkarnie cząstki lub kojoty. Całkiem niedawno udało się wykonać urządzenie *dzielące fotony na pół*. Urządzenie, jest to szumnie powiedziane: chodzi o kryształ o takich dziwnych własnościach. Rezultat działania jest banalny: wpuszczamy wąskim strumyczkiem światło i otrzymujemy dwie wiązki mocno czerwone. Cała operacja nie da się ogarnąć wzrokiem. Krótkofalowy kraniec czułości naszego oka to ok. 400 nm. Siedemset nanometrów to już głęboka czerwień, tymczasem z naszego urządzenia wybiegną fotony w podczerwieni o długości

800 nm.

Maszyneria nie nada się do nadawania informacji alfabetem Morse'a. Fotony lecą bowiem swoim własnym rytmem. Można natomiast dzięki owym kryształom, wiedzieć, co zostało nadane. Czy to się do czegokolwiek może nadać? Owszem do przesłania klucza do zakodowania informacji.

Sprawa jest znana od bardzo dawna, ale sprowadza się do prostej wiedzy, że jeśli stosuje się klucz jednokrotny, inaczej mówiąc każdy znak informacji (nie alfabetu) jest kodowany w inny sposób to nie ma sposobu na złamanie szyfru. Dopóki jednak operacja wymaga za każdym razem przesyłania w jakiś nader wyrafinowany sposób owego klucza, to jest do kitu.

Mechanika kwantowa ten sposób podaje na talerzu. Jeśli wyślemy w drogę pojedyncze kwanty, to nie będzie dobrego sposobu na podglądanie. Po pierwsze: albo foton zostanie przez szpiega, albo przez naszego korespondenta. Jeśli odbierze go szpieg, to zostanie zepsuty kod do przesłania informacji.

Jeśli wszystkie kwanty dotrą do korespondenta, to szpieg nie będzie miał sposobu na odszyfrowanie informacji. Istnieją pomysły, jak to zrobić jeszcze sprytniej. Jest to jednak materiał na kolejny długi artykuł.