Podstawowym elementem bezpiecznej komunikacji jest posiadanie tajnego klucza, który pozwala wiadomość szyfrować. Niestety bezpieczeństwo współcześnie wykorzystywanych metod kryptograficznych opiera się na zaufaniu, że nikt nie potrafi rozkładać dużych liczb na czynniki pierwsze w rozsądnym czasie (MT 01/2010). Gdy tylko ktoś taką umiejętność posiądzie, zaufanie w bezpieczeństwo korespondencji zostanie bardzo nadszarpnięte. Na szczęście istnieje inny sposób generowania klucza kryptograficznego, który jest absolutnie bezpieczny. Jego bezpieczeństwo wyrasta wprost z fundamentalnych praw, jakie rządzą mikroświatem (MT 02/2010). Aby choć troszkę zrozumieć, dlaczego tak się dzieje, spróbujmy wymyślić jakiś sposób sforsowania tej metody kryptograficznej.

Czy można podsłuchać fotony?

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.

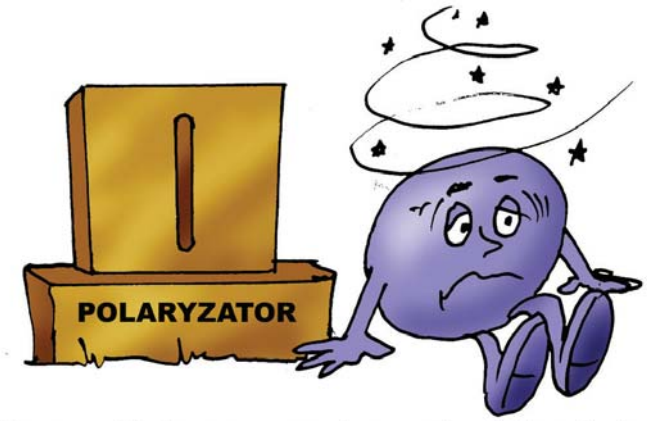
NIEDOSTĘPNOŚĆ INFORMACJI KWANTOWEJ

Podstawowym elementem, na którym opiera się kwantowy protokół generowania klucza kryptograficznego (nazywa się go BB-84, patrz MT 02/2010), jest fundamentalny fakt, że nie możemy mieć pełnej wiedzy o zjawiskach zachodzących w mikroświecie. Ta niewiedza nie wynika z naszej nieumiejętności wykonania dokładnych pomiarów, ale płynie wprost z samej natury praw rządzących mikroświatem. Najlepszą manifestacją tego, że nie wszystko możemy się dowiedzieć, jest fakt, że nie możemy dokładnie poznać polaryzacji nieznanego nam fotonu.

Badanie polaryzacji fotonu możemy bowiem przeprowadzić jedynie za pomocą polaryzatora, a ten, jak pamiętamy, rozróżnia tylko dwa spośród nieskończenie wielu kierunków, w jakich może być spolaryzowany foton. Przepuszczając nieznany foton przez polaryzator, otrzymujemy jedynie statystyczną odpowiedź na temat jego polaryzacji i tylko dwa przypadki są stuprocentowo pewne. Jeśli foton przejdzie na drugą stronę polaryzatora, to wiemy, że na pewno nie miał polaryzacji prostopadłej do jego osi. Jeśli zostanie pochłonięty, to wiemy na pewno, że nie miał polaryzacji zgodnej z osią polaryzatora. Wszystkie inne kwestie są jedynie znane z pewnym prawdopodobieństwem. Na domiar złego po przejściu przez polaryzator foton już nie pamięta swojej pierwotnej polaryzacji. Od tej chwili jego polaryzacja jest dokładnie taka sama jak kierunek, w którym zwrócona jest oś polaryzatora. Tym samym informacja o tym, jaka była polaryzacja fotonu, jest całkowicie zniszczona.

W tym miejscu warto podkreślić, że takie dziwne zachowanie się pojedynczych fotonów przepuszczanych przez polaryzator zostało wielokrotnie potwierdzone eksperymentalnie i nie znamy żadnej (poza jedną) teorii, która w sposób prawidłowy to opisuje. Jedyną dziś znaną teorią, która poprawnie opisuje zachowanie nie tylko fotonów, ale również i innych obiektów z mikroświata, jest mechanika kwantowa. I choć istnieje ona od ponad stu lat, to nie znaleźliśmy

Czy można podsłuchać fotony?



Po przejściu przez polaryzator foton już nie pamięta swojej pierwotnej polaryzacji

do dziś żadnego eksperymentalnego od niej odstępstwa.

Zasadniczą podwaliną tej teorii fizycznej – mechaniki kwantowej – jest stwierdzenie, że o zjawiskach zachodzących w mikroświecie nie można dowiedzieć się wszystkiego, gdyż ich przebieg diametralnie zależy od tego, jakie wykonujemy pomiary. Każdy pomiar zawsze niszczy przynajmniej część informacji o układzie i sprawia, że jego powtórzenie mija się z celem. Dodatkowo nie istnieje pomiar, którego wykonanie mogłoby całą informację o stanie układu nam dostarczyć. Te właśnie trzy fakty, wpisane w aksjomaty mechaniki kwantowej:

1. zmiana stanu układu pod wpływem pomiaru,
2. nieodwracalne niszczenie informacji o stanie układu poprzez wykonanie pomiaru,
3. brak pomiaru kompleksowego (tzn. dostarczającego pełnej informacji o stanie układu),

prowadzą w konsekwencji do niemożności uzyskania pełnej informacji o układzie. W przypadku fotonów taką informacją jest właśnie ich polaryzacja, którą możemy częściowo (ale nigdy nie w całości) poznać za pomocą polaryzatorów.

PROTOKÓŁ BB-84

Wróćmy teraz do problemu bezpiecznego generowania klucza kryptograficznego za pomocą fotonów. Jak pamiętamy, cały pomysł protokołu BB-84 opiera się na losowym wysyłaniu fotonów o czterech różnych polaryzacjach przez nadawcę i na losowym pomiarze ich polaryzacji przez odbiorcę. Cała procedura jest przemyślana w ten sposób, że nadawca A nigdy nie zdradza, w jakiej polaryzacji fotony wysyła, a odbiorca B nigdy nie zdradza, jaka jest domniemana przez niego polaryzacja zarejestrowanego fotonu. Dzięki wprowadzeniu dwóch grup polaryzacyjnych i ich porównaniu osoby A i B mogą jednak wygenerować ten sam klucz kryptograficzny. Zdradzają oni jedynie grupy polaryzacyjne, do których zawsze należą dwa fotony o prostopadłych polaryzacjach (MT 02/2010).

Procedura generowania klucza jest bardzo prosta i wydaje się bezpieczna do czasu, aż pojawi się trzecia osoba C, która chciałaby poznać tajemnice osób A i B. Oczywiście największą tajemnicą jest klucz kryptograficzny, którego znajomość pozwala poznać treść korespondencji. Zastanówmy się zatem, czy podsłuchująca osoba, majstrując coś przy kanale, którym przesyłane są fotony, może jakoś poznać tajny klucz.

SCENARIUSZ 1: PRZECHWYT FOTONU

Na początku rozpatrzmy sytuację, w której osoba C, mająca wrogie zamiary, ma dostęp do kanału (np. światłowodu), którym są przesyłane fotony. Wie ona, że kanałem tym przelatują fotony o czterech różnych polaryzacjach i wie, jakie wartości logiczne są przypisane każdej z nich. Mogła to bowiem podsłuchać w zupełnie niezabezpieczonej rozmowie telefonicznej wykonanej na początku całej procedury. Przypomnijmy, że podczas tej rozmowy osoby A i B ustaliły, jakie będą polaryzacje przesyłanych fotonów i jakie wartości logiczne zostają im przypisane.

Osoba C mogłaby na drodze pomiędzy A i B ustawić swój polaryzator w jednej z czterech uzgodnionych polaryzacji i dokonać pomiaru. Tym samym posiadłaby część tajnej wiedzy o fotonie. Następnie może wyprodukować swój foton w jednej z czterech polaryzacji i wysłać go w kierunku osoby B. Ponieważ osoba B nie wie, jaki foton został wysłany przez osobę A, to sytuacja dla niej będzie na pierwszy rzut oka całkiem standardowa. Dla osoby B sytuacja, w której foton jest wysłany przez osobę podsłuchującą C, wydaje się nieodróżnialna od sytuacji, w której nadlatujący do niej foton byłby wysłany przez osobę A. Osoba A przecież nigdy nie zdradzi, jaki foton wysłała. W późniejszej rozmowie zdradzi jedynie grupę polaryzacyjną, do jakiej dany foton należał. Wykrycie

podsłuchu wydaje się zatem bardzo trudne.

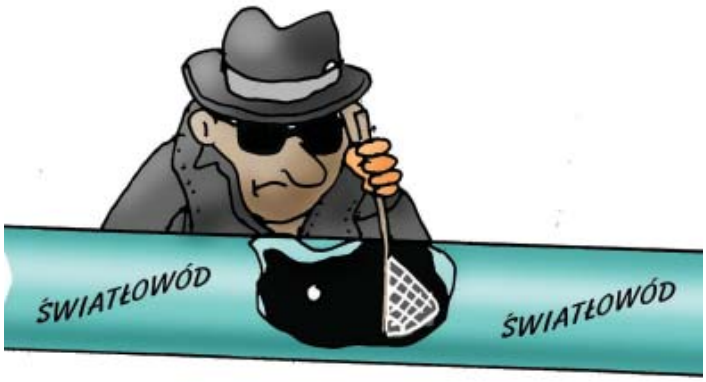
Okazuje się jednak, że sytuacja wcale nie jest taka zła i jest znacznie lepiej, niż przypuszczaliśmy. Aby zrozumieć, dlaczego tak jest, posłużmy się przykładem. Załóżmy na początku, że osoba C „nie podsłuchiwała" przelatujących fotonów. Mamy wtedy do czynienia z klasyczną sytuacją już przez nas opisaną poprzednim razem (MT 02/2010). Załóżmy, że po końcowym uzgodnieniu grup polaryzacyjnych osoby A i B dysponują następującymi informacjami:

A	wartość	1	0	1	0	0	1
	grupa	⊕	⊗	⊗	⊕	⊗	⊕
B	grupa	⊕	⊗	⊗	⊕	⊗	⊕
	wynik pomiaru	1	0	1	0	0	1

Dzięki wprowadzeniu dwóch grup polaryzacyjnych i ich porównaniu osoby A i B mogą wygenerować ten sam klucz kryptograficzny

Krótko mówiąc: w wyniku całej procedury, tak bardzo wnikliwie opisanej przez nas poprzednim razem, osoby A i B uzgodniły tajny klucz kryptograficzny w postaci ciągu liczb: **1 0 1 0 0 1**.

Dość łatwo jest zauważyć, że w sytuacji, w której osoba C podsłuchuje przelatujące fotony w sposób opisany przed chwilą, sprawa dramatycznie ulega zmianie. Załóżmy, że osoba C przechwyciła jakoś pierwszy foton. Oczywiście tak jak osoba B nie zna ona grupy polaryzacyjnej, do której on należy. Tylko przypadek sprawił, że osoba B wylosowała akurat tę grupę, w której osoba A foton wysłała. Osoba C jest w bardzo trudnej sytuacji. Aby mogła się ona cokolwiek dowiedzieć o polaryzacji fotonu, musi dokonać pomiaru za pomocą polaryzatora, ale zupełnie nie wie, jak go ustawić. Musi zatem zdecydować całkowicie losowo. Jeśli akurat będzie miała szczęście i wylosuje grupę ⊕, to w wyniku pomiaru na pewno otrzyma wartość 1. Taką bowiem wartość reprezentuje ten foton w tej bazie. Foton po przejściu przez polaryzator nie zmieni swojej polaryzacji i będzie nadal pionowy.



Scenariusz 1: przechwyt fotonu

Osoba C nie wie jednak, czy foton przeszedł, dlatego że dobrze wylosowała bazę polaryzacyjną, czy być może bazę wylosowała źle, ale foton akurat przeszedł na drugą stronę, mając na to tylko 50% szans. Tak czy owak osoba C, aby nie zostać zbyt szybko zdekonspirowana, musi wysłać jakiś foton do osoby B. Najlepiej, aby był on taki, jaki został wysłany przez osobę A. Ale niestety jedyne, co osoba C wie o fotonie, to fakt, że na pewno nie był on w polaryzacji poziomej. Czy był on natomiast w polaryzacji pionowej, skośnej, czy antyskośnej, nie może mieć pewności. Jeśli wyśle do osoby B foton w złej polaryzacji (tylko jedna z tych trzech jest prawidłowa), to istnieje bardzo duże prawdopodobieństwo, że osoba B, mierząc foton swoim polaryzatorem w bazie ⊕, otrzyma wartość logiczną 0. Otrzyma ona zatem inną wartość logiczną niż osoba A. Będzie tak pomimo, że grupa polaryzacyjna nadawcy A i grupa polaryzacyjna odbiorcy B jest dokładnie taka sama.

Całkowicie analogicznie będzie, jeśli foton zostanie na polaryzatorze osoby C pochłonięty. Wtedy jedynie wiadomo, że foton nie był dokładnie pionowy. Ale czy był w polaryzacji poziomej, skośnej, czy antyskośnej, nie jest do sprawdzenia. To właśnie jest przejaw działania tych ogólnych postulatów mechaniki kwantowej. Z jednej strony nie można pojedynczym pomiarem uzyskać wszystkich informacji o polaryzacji fotonu. Z drugiej strony już pojedynczy pomiar sprawia, że przeprowadzenie kolejnych pomiarów nic nie daje, gdyż informacja o początkowej polaryzacji zostaje zatracona. Niezależnie od tego, co zrobi osoba C, zawsze istnieje duża szansa na to, że jej podsłuch sprawi, że choć osoby A i B mają te same grupy polaryzacyjne, to mają przeciwnie przypisane wartości logiczne do konkretnych fotonów. To oznacza, że ich kody kryptograficzne przestają być takie same.

Zdekonspirowanie szpiega jest zatem bardzo proste. Wystarczy tylko, że osoby A i B ujawnią fragmenty swoich tajnych kluczy kryptograficznych. Jeśli w jakimś miejscu nie będą one zgodne, choć takie być powinny, będzie to oznaczało jedno: na kanale kwantowym jest podsłuch! W ten sposób można odkryć, że ktoś podsłuchuje nasz przekaz i natychmiast przerwać transmisję.

SCENARIUSZ 2: KOPIOWANIE FOTONU

Poprzedni scenariusz opierał się na założeniu, że osoba C przechwytuje foton, wykonuje na nim swój pomiar, a następnie do osoby B wysyła inny foton przez siebie spreparowany. Można jednak teoretycznie wyobrazić sobie, że osoba C jest bardziej cwana niż w opisanym przed chwilą scenariuszu. Gdyby na przykład osoba C umiała skopiować nadlatujący foton, to mogłoby być to bardzo niebezpieczne dla tajemnicy osób A i B. Osoba C w takiej sytuacji mogłaby bowiem foton oryginalny przesłać dalej do osoby B w niezmienionej formie, a jego kopię zanalizować za pomocą swojego polaryzatora. Tym samym do osoby B doleciałby foton w stanie takim, w jakim osoba A go wyprodukowała. To w konsekwencji oznaczałoby, że osoby A i B wygenerowałyby taki sam klucz kryptograficzny i nie mogłyby się zorientować, że są podsłuchiwane. Mało tego, osoba C, posiadająca umiejętność kopiowania fotonów, mogłaby wykonać wiele kopii tego samego fotonu. Tym samym mogłaby poznać zachowanie fotonu przepuszczanego przez różnie ustawione polaryzatory i być przygoto-

Osoby A i B uzgodniły tajny klucz kryptograficzny w postaci ciągu liczb: 1 0 1 0 0 1

wana na każdą ewentualność. Podsłuchując późniejszą rozmowę pomiędzy osobami A i B, podczas której uzgadniają one swoje grupy polaryzacyjne, mogłaby zatem całkowicie odtworzyć ustalony przez nie klucz kryptograficzny!

Ten scenariusz jest rzeczywiście bardzo niebezpieczny. Podkreślmy to jeszcze raz. W sytuacji, w której osoba C umiałaby kopiować kwantowy stan przelatującego fotonu, mogłaby odtworzyć całkowicie klucz kryptograficzny ustalony pomiędzy osobami A i B. Na dodatek osoby A i B nie miałyby żadnej możliwości, aby stwierdzić, czy nie są podsłuchiwane. Czyżby twórcy protokołu BB-84 nie wzięli takiej możliwości pod uwagę?

nie, do którego z jednej strony wpada jakiś foton, a z drugiej strony wylatują dwa fotony, które są dokładnie w takim samym stanie jak foton wlatujący. Stan kwantowy obiektu możemy jedynie przenosić z jednego obiektu na drugi. Nie możemy go natomiast skopiować.

Z tego punktu widzenia stan kwantowy to coś w rodzaju czystej informacji. Nie możemy jej rozmnożyć, możemy ją jedynie przenieść z jednego nośnika na drugi. Jednak podczas tego przenoszenia informacja zawarta na nośniku źródłowym zostaje nieodwracalnie zatarta i nie ma przed tym żadnej obrony.

Niemożność kopiowania stanu kwantowego jest bardzo ważną konsekwencją formalizmu mecha-

Scenariusz 2: kopiowanie fotonu

KWANTOWY ZAKAZ KLONOWANIA

Oczywiście nie! Twórcy BB-84 (Bennett i Brassard) wiedzieli bowiem troszkę więcej o mechanice kwantowej, niż udało mi się do tej pory przekazać na łamach „Młodego Technika". Otóż w roku 1982 na łamach prestiżowego czasopisma „Nature" pojawił się dwustronicowy, bardzo prosty artykuł, w którym dwóch fizyków, Polak Wojciech Żurek i Amerykanin William Wootters, formalnie udowodniło, że wykonywanie kopii nieznanego stanu kwantowego byłoby sprzeczne z podstawowymi aksjomatami mechaniki kwantowej. Krótko mówiąc, oznacza to, że skopiowanie przez osobę C przelatującego fotonu jest niemożliwe. Jest niemożliwe, bo zabraniają tego fundamentalne prawa przyrody. Nie istnieje takie urządze-

Kwantowy zakaz klonowania

niki kwantowej. Oto po raz kolejny okazało się, że możemy powiedzieć znacznie więcej o prawach przyrody działających w mikroświecie niż tylko to, co udało nam się zaobserwować w doświadczeniu. Wcale nie musimy budować kolejnych, bardzo wymyślnych maszyn i sprawdzać, czy być może nie umieją one kopiować stanów kwantowych. Nie musimy tego robić, bo wiemy, że takie maszyny istnieć po prostu nie mogą. Byłoby to bowiem sprzeczne z podstawami mechaniki kwantowej. Taka kopiująca stan kwantowy maszyna to coś w rodzaju perpetuum mobile. Jeśli ktoś mi powie, że wymyślił urządzenie kopiujące stan kwantowy, to nie muszę tego sprawdzać. Od razu wiem, że to nie jest możliwe. Tak samo jak wiem, że nie istnieje maszyna, która więcej pracy wykonuje, niż energii pobiera. •