Fotony zagubione w szumie

15 lutego 2017

Kryptografia kwantowa – już stosowana np. w bankowości – pozwala na bezpieczne przesyłanie poufnych informacji. Na razie jednak takie informacje przesyłane są niezbyt efektywnie – fotony kodujące informacje łatwo zgubić w szumie tła. A Polacy odkryli, jak te cząstki wytwarzać, żeby potem łatwiej je było znaleźć.

Mechanika kwantowa rządzi się innymi prawami niż te, które znamy ze świata makroskopowego. A prawa te pozwalają na przesyłanie poufnych informacji. Dlatego technologia kwantowa wkroczyła już do banków w postaci układów do tworzenia klucza kryptograficznego. Takie układy połączone ze sobą światłowodem, instaluje się np. w banku i w jego filii. „Plotka głosi, że światłowód, którym przesyła się informację kwantową, łączy też Pentagon z Białym Domem" – uśmiecha się dr Piotr Kolenderski z Krajowego Laboratorium Fizyki Atomowej, Molekularnej i Optycznej (KL FAMO) w Instytucie Fizyki Uniwersytetu Mikołaja Kopernika w Toruniu. Badacz pracuje nad możliwościami udoskonalenia takich systemów.

Fizyk w rozmowie z PAP wyjaśnia, na czym polega działanie takich układów. Pomiędzy urządzeniami przesyła się pary tzw. splątanych fotonów – jedna cząstka z tej pary dociera do jednego układu, a druga do drugiego. Cząstki te powstają jednocześnie i są trochę jak bliźniaki, ale zbuntowane – kiedy więc okaże się, że jedna z nich ma pewną własność – polaryzację oznaczoną jako 1, wiadomo, że druga musi mieć polaryzację przeciwną oznaczoną jako 0. Dzięki temu, dokonując pomiaru na swoim fotonie, jedna ze stron może zyskać pewność, jaka informacja dotarła do drugiej strony. Co więcej, z reguł fizyki kwantowej wynika, że każda próba przechwycenia po drodze jednego z fotonów zmieni właściwości drugiego z nich. A wtedy łatwo wykryć, że istnieje podsłuch. Wiadomo więc już, że takiego podsłuchanego komunikatu nie można użyć np. jako

poufnego klucza do zaszyfrowania wiadomości.

Działanie tego typu bezpiecznych połączeń jest jednak ograniczone. Im dłuższy dystans mają do pokonania pojedyncze fotony, tym łatwiej je po drodze „zgubić" w szumie tła. Dlatego urządzenia do tworzenia kwantowego klucza kryptograficznego nie mogą stać dowolnie daleko od siebie.

„My sprawdziliśmy, czym powinny się charakteryzować fotony, żeby jak najlepiej uniknąć zakłóceń" – mówi w rozmowie z PAP dr Piotr Kolenderski. Wyniki badań jego zespołu ukazały się w czasopiśmie „Optica". Zaproponowane przez badaczy z Torunia rozwiązania sprawiają, że fotony będzie można przekazywać o 10-20 proc. dalej niż do tej pory. A jeśli nie zależy nam na oddalaniu urządzeń kryptograficznych od siebie, to ten sam sposób można będzie równie dobrze wykorzystać do tego, by przekazywać o 10-20 proc. więcej informacji niż dotąd w ustalonym odcinku czasu.

„Zwykle w kryptografii kwantowej używa się fotonów, które są skorelowane jedynie w polaryzacjach. Jeśli więc jeden użytkownik zarejestruje jedną polaryzację, to wie, że drugi użytkownik zarejestrował inną polaryzację. To splątanie służy nam do wymiany klucza kryptograficznego. A u nas wykorzystujemy fotony, które dodatkowo splątane są jeszcze w długościach fal. I to nam służy do tego, aby lepiej rozpoznawać te cząstki w szumie" – zaznacza fizyk.

Długości fal fotonów są powiązane z ich kolorami. Nie jest jednak tak, że przed pomiarem dany foton ma jakąś konkretną barwę – ma jedynie pewien prawdopodobny rozkład długości fal. „Jeśli mamy dwa splątane fotony to te rozkłady mogą być ze sobą powiązane. Jeśli długość fali jednej z tych cząstek jest mniejsza, to drugiego będzie większa" – opowiada dr Kolenderski. Można więc powiedzieć, że jeśli jeden foton z pary tych „antybliźniaków" okaże się bardziej czerwony, to wiadomo, że ten drugi musi się okazać bardziej niebieski.

Okazuje się, że takie „barwne” splątanie sprawia, że pary fotony są prostsze w obyciu – lepiej wiadomo, jak się będą zachowywać i kiedy dokładnie dotrą do detektora. A dzięki temu można wyciszyć mnóstwo niepotrzebnego szumu. To z kolei sprawia, że komunikacja między układami kryptograficznymi jest znacznie sprawniejsza.

Naukowiec uważa, że aby wprowadzić to rozwiązanie w życie, niekoniecznie trzeba budować całkiem nowe urządzenia – wystarczy trochę przebudować istniejące już układy – m.in. zmienić parametry ich pracy czy wymienić elementy optyczne.

Autorami opublikowanego w piśmie „Optica” artykułu są także: mgr Karolina Sędziak oraz dr Mikołaj Lasota z UMK. Badania były współfinansowane w ramach grantów FNP Homing Plus oraz MNiSW Iuventus Plus.

Autorstwo: Ludwika Tomala
Źródło: NaukawPolsce.PAP.pl