Kryptografia kwantowa nie jest wybredna, udowadniają polscy fizycy

2011-02-02

Szyfrowanie kwantowe będzie można realizować za pomocą źródeł zaszumionego splątania. Na zdjęciu od lewej prof. dr hab. Paweł Horodecki (PG), dr Rafał Demkowicz-Dobrzański (FUW) i doktorant Michał Karpiński (FUW). (Źródło: NLTK, Grzegorz Krzyżewski)

W czasach masowej wymiany danych poufność transmitowanych informacji ma podstawowe znaczenie. Całkowitą prywatność transmisji, gwarantowaną przez fundamentalne cechy cząstek kwantowych, może zapewnić kryptografia kwantowa. Obecnie podczas szyfrowania kwantowego stosuje się źródła cząstek, w których pewne cechy cząstek są ze sobą ściśle i idealnie związane maksymalnie splątane. Grupa fizyków współpracujących w ramach Narodowego Laboratorium Technologii Kwantowych po raz pierwszy wykazała doświadczalnie, że do bezpiecznej transmisji klucza kryptograficznego można wykorzystać także pozornie nieprzydatne źródła, w których splątanie cząstek jest znacząco zaszumione.

Klucz kryptograficzny to przypadkowy ciąg liczb, przez nadawcę używany do szyfrowania informacji, przez odbiorcę do ich odszyfrowania. Aby obie strony mogły poufnie wymieniać dane, muszą dysponować tym samym, znanym tylko im kluczem. Kryptografię kwantową stosuje się obecnie właśnie w tym celu: do bezpiecznego przekazywania klucza między nadawcą a odbiorcą.

W 1991 roku polski fizyk Artur Ekert opracował protokół E91 kwantowej dystrybucji klucza, wykorzystujący splątane cząstki kwantowe. Splątanie oznacza, że pewne cechy cząstek są wzajemnie powiązane. Na przykład w krysztale nieliniowym można wytworzyć pary fotonów o splątanych polaryzacjach. Oznacza to, że jeśli nadawca dla swojego fotonu zaobserwuje polaryzację w płaszczyźnie pionowej, ma pewność, że drugi foton był u odbiorcy spolaryzowany poziomo. Analogiczne zjawisko zajdzie dla dowolnej innej pary prostopadłych kierunków. Dla nadawcy i odbiorcy rezultaty ich własnych pomiarów wyglądają na całkowicie przypadkowe. Jeśli jednak obaj porównają wyniki, natychmiast zauważą, że istnieją między nimi korelacje wynikające ze splątania. Ten mechanizm wykorzystuje kryptografia kwantowa. Gdyby ktoś próbował podsłuchiwać przekaz, zniszczyłby splątanie i doskonałe

korelacje między wynikami u nadawcy i odbiorcy zniknęłyby. Szpieg zostałby natychmiast wykryty.

Opisana sytuacja to przypadek idealny, gdy splątanie między obiektami jest maksymalne. W rzeczywistości splątanie często nie jest maksymalne, korelacje między wynikami nie są doskonałe i coraz trudniej ustalić, czy przekaz był podsłuchiwany. Standardową procedurą jest wówczas przeprowadzenie destylacji splątania, procedury pozwalającej otrzymać ze stanów zaszumionych pewną liczbę stanów o splątaniu maksymalnym. Istnieje jednak wiele stanów, z których destylacja splątania jest niemożliwa lub bardzo niewydajna. Przez długi czas stany te były traktowane jako nieprzydatne dla kryptografii kwantowej. Jednak w 2005 roku w Gdańsku fizycy z rodziny Horodeckich i Jonathan Oppenheim na drodze teoretycznej wykazali, że w pewnych sytuacjach klucz kryptograficzny można wydajnie przesłać mimo trudności z destylacją splątania.

Naukowcy współpracujący w ramach Narodowego Laboratorium Technologii Kwantowych sprawdzili przypuszczenie gdańskich fizyków w starannie zaplanowanym eksperymencie. Zrealizował go zespół koordynowany przez profesorów Konrada Banaszka z Wydziału Fizyki Uniwersytetu Warszawskiego (FUW) i Pawła Horodeckiego z Wydziału Fizyki Technicznej i Matematyki Stosowanej Politechniki Gdańskiej (PG). Za stronę eksperymentalną odpowiadał dr Krzysztof Dobek, przebywający na stażu naukowym w Krajowym Laboratorium Fizyki Atomowej, Molekularnej i Optycznej przy Uniwersytecie Mikołaja Kopernika w Toruniu.

W doświadczeniu korzystano z lasera, wysyłającego z dużą częstotliwością krótkie impulsy światła do kryształu nieliniowego. Co pewien czas z kryształu wylatywały cząstki splątane. Najczęściej były to pary fotonów (do 6 tys. na sekundę), znacznie rzadziej czwórki (zaledwie dwie na sekundę). Aparaturę elektroniczną skonfigurowano w taki sposób, aby rejestrowała polaryzację tylko czwórek fotonów. W trwającym cztery doby eksperymencie zarejestrowano kilkaset tysięcy takich zdarzeń.

Analizą danych i teoretyczną rekonstrukcją zarejestrowanych stanów kwantowych zajmowali się dr Rafał Demkowicz-Dobrzański i mgr Michał Karpiński, obaj z FUW. Dokładna analiza danych z eksperymentu była w tym przypadku szczególnie istotna. Musieliśmy mieć statystyczną pewność, że wygenerowany stan kwantowy był rzeczywiście tym stanem, o który nam chodziło wyjaśnia Rafał Demkowicz-Dobrzański. Wykazano, że mimo zaszumienia splątania, w każdej czwórce fotonów można było bezpiecznie przesłać średnio 0,7 bita klucza kryptograficznego.

Eksperyment może mieć istotne znaczenie dla praktycznej kryptografii kwantowej. Obecnie przy szyfrowaniu stosuje się źródła stanów czystych, maksymalnie splątanych. Doświadczenie polskich fizyków pokazuje, że przyszłe źródła splątanych cząstek będzie można wykorzystać do przesyłania kwantowego klucza kryptograficznego nawet w sytuacji, gdy generowane splątanie jest zaszumione i trudne do destylacji. Doświadczalnie udowodniliśmy, że o przydatności źródeł splątania w kryptografii nie musi decydować ich perfekcyjność. Jeśli nowe źródło będzie wytwarzać splątanie z szumem, lecz okaże się bardziej wydajne lub tańsze od obecnych, nadal będzie można je z powodzeniem wykorzystać podsumowuje prof. Banaszek.

Artykuł opisujący eksperyment i analizę danych ukazał się w najnowszym wydaniu znanego czasopisma naukowego Physics Review Letters. Badania przeprowadzono w ramach projektów CORNER i Q-ESSENCE finansowanych ze środków 7. Programu Ramowego Unii Europejskiej, przy wsparciu programu TEAM Fundacji na rzecz Nauki Polskiej oraz Ministerstwa Nauki i Szkolnictwa Wyższego.

UWAGI DLA REDAKTORÓW:

W pojedynczym fizycznym akcie transferu informacji nie można przesłać ułamkowych wartości bitu. Podana w informacji prasowej ułamkowa wartość jest wartością statystyczną, wynikającą z podzielenia liczby (całkowitej) wytworzonych stanów kwantowych przez liczbę (także całkowitą) przesłanych bitów.

Z tego powodu przy podawaniu ułamkowej wartości bita niezbędna jest obecność wyrazu średnio lub statystycznie.

INFORMACJE DODATKOWE:

Narodowe Laboratorium Technologii Kwantowych (nltk.fuw.edu.pl) to konsorcjum złożone z wiodących w kraju jednostek naukowych zajmujących się badaniami w zakresie technologii kwantowych, w tym informatyki kwantowej, inżynierii kwantowej oraz dziedzin pokrewnych. W skład NLTK wchodzą: Uniwersytet Warszawski, Politechnika Wrocławska, Instytut Fizyki PAN, Uniwersytet Mikołaja Kopernika w Toruniu, Uniwersytet Jagielloński, Uniwersytet Gdański, Uniwersytet Łódzki i Centrum Fizyki Teoretycznej PAN. W pięciu spośród ośmiu instytucji tworzących konsorcjum NLTK (UW, PWr, IF PAN, UMK, UJ) jest realizowany projekt o tej samej nazwie, którego celem jest utworzenie i wyposażenie członkowskich jednostek naukowych w sprzęt niezbędny do prowadzenia wspólnych badań naukowych oraz badawczo-rozwojowych na światowym poziomie. Projekt Narodowe Laboratorium Technologii Kwantowych jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka, lata 2007-2013, Priorytet 2. Infrastruktura sfery B+R, Działanie 2.2 Wsparcie tworzenia wspólnej infrastruktury badawczej jednostek naukowych.

MATERIAŁY GRAFICZNE:

HR: Szyfrowanie kwantowe będzie można realizować za pomocą źródeł zaszumionego splątania. Na zdjęciu od lewej prof. dr hab. Paweł Horodecki (PG), dr Rafał Demkowicz-Dobrzański (FUW) i doktorant Michał Karpiński (FUW). (Źródło: NLTK, Grzegorz Krzyżewski)

UZNANIE AUTORSTWA

POWIĄZANE STRONY WWW:

Narodowe Laboratorium Technologii Kwantowych.

PRACE NAUKOWE:

Experimental Extraction of Secure Correlations from a Noisy Private State; K. Dobek, M. Karpiński, R. Demkowicz-Dobrzański, K. Banaszek, P. Horodecki; *Physical Review Letters* **106**, 030501 (2011), preprint.