

[Akceptuje](#)

W ramach naszej witryny stosujemy pliki cookies w celu świadczenia państwu usług na najwyższym poziomie, w tym w sposób dostosowany do indywidualnych potrzeb. Korzystanie z witryny bez zmiany ustawień dotyczących cookies oznacza, że będą one zamieszczone w Państwa urządzeniu końcowym. Możecie Państwo dokonać w każdym czasie zmiany ustawień dotyczących cookies. Więcej szczegółów w naszej [Polityce Prywatności](#)

[Portal](#) [Informacje](#) [Katalog firm](#) [Praca](#) [Szkolenia](#) [Wydarzenia](#) [Porównania międzylaboratoryjne](#)
[Kontakt](#)



[Laboratoria](#)
[.net](#)
[Innowacje](#)
[Nauka](#)
[Technologie](#)

[Logowanie](#) [Rejestracja](#) [pl](#)

Newsletter

zapisz się



Naukowy styl życia

Nauka i biznes

- [Nowe technologie](#)
- [Felieton](#)
- [Tygodnik "Nature"](#)
- [Edukacja](#)
- [Artykuły](#)
- [Przemysł](#)

[Strona główna](#) > [Informacje](#)

Kryptografia kwantowa nie jest wybredna, udowadniają polscy fizycy

W czasach masowej wymiany danych poufność transmitowanych informacji ma postawowe 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 kryształach nieliniowych 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.

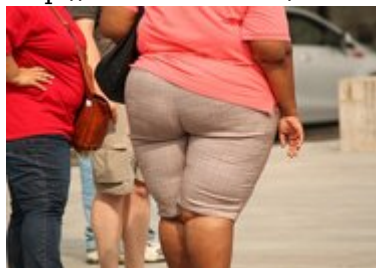
Eksperyment może mieć istotne znaczenie dla praktycznej kryptografii kwantowej. Obecnie przy szyfrowaniu stosuje się źródła stanów czystych, maksymalnie splątanych. Doświadczenie polskich fizyków pokazuje, że przyszłe źródła splątanych cząstek będzie można wykorzystać do przesyłania kwantowego klucza 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.

Fizyka i astronomia na Uniwersytecie Warszawskim pojawiły się w 1816 roku w ramach ówczesnego Wydziału Filozofii. W roku 1825 powstało Obserwatorium Astronomiczne. Obecnie w skład Wydziału Fizyki UW wchodzi Instytuty: Fizyki Doświadczalnej, Fizyki Teoretycznej, Geofizyki, Katedra Metod Matematycznych oraz Obserwatorium Astronomiczne. Badania pokrywają niemal wszystkie dziedziny współczesnej fizyki, w skalach od kwantowej do kosmologicznej. Kadra naukowo-dydaktyczna Wydziału składa się z ponad 200 nauczycieli akademickich, wśród których jest 70 pracowników z tytułem profesora. Na Wydziale Fizyki UW studiuje prawie 700 studentów i ok. 150 doktorantów.

<http://forumakademickie.pl/>

<http://laboratoria.net/aktualnosci/5400.html>



21-08-2019

Jakie są przyczyny otyłości?

Współczesny świat nie pomaga w utrzymaniu prawidłowej wagi. Sprawdź, dlaczego tyjemy na potęgę.



21-08-2019

[Hipercholesterolemia rodzinna: ryzyko zawału w młodym wieku](#)

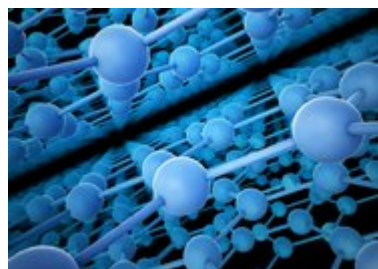
Wysoki cholesterol znacząco zwiększa ryzyko rozwoju miażdżycy i epizodu sercowo-naczyniowego: zawału serca lub udaru mózgu.



21-08-2019

[Uprawy bananów bezpieczniejsze dzięki sztucznej inteligencji](#)

Łatwe do wykorzystania narzędzie bazujące na sztucznej inteligencji pomoże w wykrywaniu chorób i szkodników bananowców.



21-08-2019

[Magnetyczne nanorurki mogą usuwać mikroplastiki z wody](#)

Skęczone w spiralę węglowe nanorurki mogą oczyścić wodę z mikroplastiku, a dzięki magnetycznym domieszkom nadają się do regeneracji.



21-08-2019

[Alkohol pity podczas ciąży zmienia DNA noworodka](#)

Prenatalna ekspozycja na umiarkowane lub duże ilości alkoholu sprzyja długotrwałym zmianom genetycznym u nowo narodzonych dzieci.



21-08-2019

[Otwarty dostęp do ponad 300 tys. artykułów w Bibliotece Nauki](#)

Już ponad 300 tys. artykułów z tysiąca czasopism udostępnia Biblioteka Nauki, największy polski serwis internetowy gromadzący czasopisma naukowe.



14-08-2019

[Proteza ręki - wynalazek z "ciągiem dalszym"](#)

MindHand to bioniczna proteza ręki, która powstaje, aby ułatwić życie niepełnosprawnym i osobom po amputacji.



14-08-2019

Nadciągająca burza? Szukaj schronienia!

Lato to w Polsce najbardziej burzowy sezon. Warto pamiętać, żeby w czasie burz unikać otwartej przestrzeni, nie stawać pod drzewami, a także chronić sprzęt elektryczny.

Informacje dnia: [Jakie są przyczyny otyłości?](#) [Hipercholesterolemia rodzinna: ryzyko zawału w młodym wieku](#) [Uprawy bananów bezpieczniejsze dzięki sztucznej inteligencji](#) [Magnetyczne nanorurki mogą usuwać mikroplastiki z wody](#) [Alkohol pity podczas ciąży zmienia DNA noworodka](#) [Otwarty dostęp do ponad 300 tys. artykułów w Bibliotece Nauki](#) [Jakie są przyczyny otyłości?](#) [Hipercholesterolemia rodzinna: ryzyko zawału w młodym wieku](#) [Uprawy bananów bezpieczniejsze dzięki sztucznej inteligencji](#) [Magnetyczne nanorurki mogą usuwać mikroplastiki z wody](#) [Alkohol pity podczas ciąży zmienia DNA noworodka](#) [Otwarty dostęp do ponad 300 tys. artykułów w Bibliotece Nauki](#)

Partnerzy



-
- [Baza wiedzy](#)
- [Forum](#)
- [Humor](#)
- [Regulamin](#)
- [Oferta reklamy](#)
- [O nas](#)
-

Copyright © 2013 by Laboratoria.net | Aktualizacja: 21.08.2019 09:37