Przyspieszyli kwantową kryptografię

8 kwietnia 2016

University of Cambridge i Toshiba Research Europe zaprezentowały system dystrybucji kwantowych kluczy szyfrujących, który jest o 2-6 rzędów wielkości szybszy niż dotychczasowe kwantowe systemy kryptograficzne.

Szyfrowanie przesyłanych informacji to chleb powszedni współczesnej komunikacji. W konwencjonalnej kryptografii nadawca i odbiorca informacji ustalają między sobą tajny klucz, za pomocą którego tylko oni mogą odczytać przesyłane dane. Jednak wraz z wzrostem wydajności komputerów konieczne jest stosowanie coraz dłuższych kluczy szyfrujących, gdyż te krótsze można odgadnąć w rozsądnym czasie. Nad szyframi wisi też poważne niebezpieczeństwo w postaci komputerów kwantowych. Maszyny te będą tak szybkie, że błyskawicznie złamią współczesne klucze. Rozwiązaniem problemu ma być kwantowa kryptografia. Nadawca informacji wysyła do odbiorcy spolaryzowane fotony. Odbiorca je odbiera i jeśli posiada odpowiednio ustawiony czujnik, jest w stanie odczytać z fotonów dane. Siła kryptografii kwantowej polega – w teorii – na tym, że gdy pomiędzy nadawcą a odbiorcą znajdzie się osoba podsłuchująca, która będzie próbowała przechwycić informację kwantową, natychmiast ulegnie ona zmianie.

„Teoretycznie napastnik mógłby dysponować całą możliwą w fizyce mocą obliczeniową, a nie byłby w stanie złamać kodu” – mówi Lucian Comandar z University of Cambridge. Problem jednak w tym, że to tylko teoria, a niedociągnięcia w systemach kwantowych powodują, że informację wciąż można przechwycić i złamać.

Najczęściej atakowanym urządzeniem w systemach kryptografii kwantowej jest czujnik fotonów. Czujniki takie to niezwykle

złożone, bardzo wrażliwe urządzenia, a zwykle im bardziej skomplikowane urządzenie, tym bardziej podatne na atak. Dlatego też opracowany specjalny protokół nazwany niezależnym od urządzenia pomiarowego systemem dystrybucji kluczy kwantowych (MDI-QKD, measurement-device-independent quntum key distribution). MDI-QKD został już eksperymentalnie zademonstrowany, jednak protokół ten pracuje na tyle powoli, że nie nadaje się do praktycznych zastosowań. Problem w tym, że impulsy laserowe wykorzystywane w tym protokole muszą być stosunkowo długie, zatem tempo przesyłania danych wynosi zaledwie kilkaset bitów na sekundę. Naukowcy z Cambridge i Toshiba Research poradzili sobie z tym problemem wykorzystując technikę, w której jeden laser „wstrzykuje" fotony w strumień fotonów drugiego lasera. Dzięki temu możliwe jest wysyłanie bardzo krótkich impulsów, a więc przyspieszenie przesyłania danych. Ponadto technika ta umożliwia błyskawiczne losowe zmiany fazy światła. W wyniku tego MDI-QKD osiąga wydajność dochodzącą do 1 Mb/s.

„Protokół ten zapewnia największe możliwe bezpieczeństwo i szybkie przesyłanie danych. Przeciera on drogę w kierunku praktycznego zastosowania kryptografii kwantowej" – dodaje Comandar.

Autorstwo: Mariusz Błoński
Na podstawie: Cam.ac.uk
Źródło: KopalniaWiedzy.pl