Pryzmat - Wiadomości PWr

KONFERENCJE, TARGI, SEMINARIA

Przyszłość już puka do naszych drzwi

27.01.2014 | Aktualizacja: 20.02.2014 11:42

Sympozjum o kryptografii kwantowej na Politechnice Wrocławskiej. Od lewej: profesor Lucjan Jacak, rektor PWr profesor Tadeusz Więckowski i profesor Vadim Makarov (fot. Krzysztof Mazur)




Na Politechnice Wrocławskiej rozpoczęła się międzynarodowa konferencja poświęcona najnowszym osiągnięciom kryptografii kwantowej. Spotkali się uczeni i praktycy oraz przedstawiciele firm, które wdrażają nową, rewolucyjną technologię.

Kryptografia kwantowa do zapewnienia pełnej poufność przesyłanych w sieciach informacji wykorzystuje mechanizmy fizyki kwantowej. Nośnikami informacji są fotony, pozbawione masy cząstki elementarne światła, najmniejsze porcje energii, czyli kwanty pola elektromagnetycznego.

Rozmowa z profesorem Lucjanem Jacakiem, jednym z organizatorów konferencji, kierownikiem wrocławskiej grupy krajowego konsorcjum Laboratorium Fizycznych Podstaw Przetwarzania Informacji oraz Narodowego Laboratorium Technologii Kwantowych.
Z zaawansowania prac nad praktycznymi rozwiązaniami kwantowego szyfrowania można by wywnioskować, że klasyczne sposoby kodowania nie zapewniają już bezpieczeństwa. Ale przecież nie istnieją jeszcze owe potężne komputery kwantowe, dla których złamanie stosowanych obecnie protokołów szyfrowania będzie drobnostką.
Profesor Lucjan Jacak: - Właśnie potężne, ale i niebezpieczne. Komputery kwantowe będą miały nowe, zupełnie nieoczekiwane możliwości. Będą potrafiły nie tylko łamać szyfry. One będą mogły na przykład sprawić, że materialny obiekt w jednym miejscu zniknie, a pojawi się w innym.
W laboratoriach stoją już niewielkie prototypy. W Kanadzie, zbudowany przez „garażową" firmę D-

Wave, większy kwantowy komputer demonstruje swoje możliwości. Został zakupiony przez firmę Lockheed Martin, a NASA z Google uruchomiły w ubiegłym roku laboratorium komputerów kwantowych. Przyszłość już puka do naszych drzwi.

Mogę jeszcze przez chwilę nie lękać się teleportacji czołgu do mojego ogródka, ale o przelewy internetowe powinnam się już niepokoić?

Przelewy też można na razie robić spokojnie. Hakerzy nie dysponują dostatecznie silnymi komputerami, aby łamać szyfry jednokrotnego stosowania lub wykorzystujące duże liczby pierwsze. Jednak Szwajcarzy już wdrażają dla banków systemy informatyczne wykorzystujące kryptografię kwantową. W Japonii jedna z firm proponuje telefony, które dzięki zastosowaniu mechanizmów kwantowych gwarantują absolutną poufność prowadzonych rozmów.

O, to coś dla kanclerz Angeli Merkel. Słyszałam jednak, że równolegle z kwantowym szyfrowaniem rozwija się kwantowe hakerstwo. Jak to możliwe, przecież bezpieczeństwo gwarantuje nam natura procesów kwantowych?

Nie da się niepostrzeżenie przechwycić kwantowego klucza, potrzebnego do rozszyfrowania komunikatu. Gdy wysyłamy zaszyfrowany komunikat, musimy dostarczyć odbiorcy również klucz, który pozwoli mu informację odkodować. Bezpieczny klucz to klucz wygenerowany losowo. Ten klucz ustalany jest na odległość z odbiorcą właśnie kwantową komunikacją. Otóż, żeby przejąć kwantowy klucz, trzeba zmierzyć pewne cechy fotonów, a natura ich jest taka, że przed pomiarem są nieokreślone, a po zmierzeniu – ulegają zmianie. Dokonujący pomiarów haker nieuchronnie spowoduje zakłócenia, które zauważy nadawca. Zacznie uzgadniać z odbiorcą nowy klucz. I tak aż do skutku. Oczywiście taki ciąg uzgodnień odbywa się automatycznie. Słabości mogą jednak kryć się w niedoskonałościach sprzętowych, które są jednak coraz skuteczniej eliminowane.

Na nasze sympozjum przyjechał bardzo znany kwantowy haker profesor Vadim Makarov. Na wykładzie opowie zapewne o swoim hakerskim wyczynie, który polegał na oślepieniu detektorów pojedynczych fotonów wiązką silnego światła i wykorzystywaniu pewnej luki technicznej do ingerencji w kanał kwantowy. Po tym eksperymencie Kanadyjczycy ufundowali profesorowi Makarovowi prawdziwe laboratorium kwantowego hakerstwa, a Toshiba opracowała odpowiednie zabezpieczenie przed oślepianiem detektorów.

Zaprosiliście na sympozjum nie tylko uczonych i firmy, które zaprezentują najnowocześniejszy sprzęt do kryptografii kwantowej, ale także potencjalnych użytkowników - przedstawicieli administracji publicznej, wojskowych, bankowców. Ilu z nich zainteresowało się nową technologią?

Udział zadeklarowało blisko 100 osób, w tym kilku wojskowych wysokiej rangi. Zdziwiło mnie stosunkowo małe zainteresowanie bankowców. Pokażemy im nasz sprzęt, aby każdy mógł sam się przekonać, że jego obsługa jest prosta. Ot, wystarczy odpowiednio uruchomić zestawy, przycisnąć guziki i wszystko dzieje się automatycznie. Szkolenie będzie prowadzone w języku polskim.

Jakimi urządzeniami dysponujecie?

Mamy cztery zestawy do kryptografii kwantowej, dwa splątaniowe i dwa bezsplątaniowe. Splątaniowe wykorzystują zadziwiający efekt kwantowego związku między fotonami, który trwa nawet po ich rozłączeniu i powoduje, że zamiana stanu jednego z bliźniaków wywołuje natychmiastową zmianę drugiego mimo oddalenia. To zupełnie nieintuicyjny efekt i pozornie sprzeczny z ograniczeniami teorii względności. Einstein dopatrywał się w tym paradoksu i nazywał splątanie upiornym oddziaływaniem na odległość. Jednak wszystko jest zgodne z relatywistycznymi ograniczeniami. Najprościej mówiąc, ograniczenia te nie dotyczą informacji kwantowej, a tylko klasycznej. W naszych zestawach splątaną cechą komunikowaną na odległość jest polaryzacja fotonów. W zestawach bezsplątaniowych dokonywany jest natomiast pomiar przesunięcia fazowego. W tej chwili na całym świecie są tylko cztery zestawy splątaniowe, oprócz tych dwóch u nas, po jednym w Wiedniu i Singapurze.

Są drogie?

Na razie tak. Zestaw splątaniowy koszuje około 600 tys. zł, a fazowy ponad 300 tysięcy. Splątaniowe zakupiliśmy w Austrii, a bezsplątaniowe w Szwajcarii. Sprzęt będzie taniał. Dla naszego bezpieczeństwa jest jednak ważne, abyśmy takie urządzenia nauczyli się produkować sami. Żeby się do tego przygotować, realizowaliśmy w ciągu ostatnich lat dwa spore projekty badawcze. Dotyczyły one rozwoju koncepcji protokołowych kryptografii kwantowej, nowych algorytmów komunikacji opartej na splątaniu, rozwiązań sprzętowych i nie mniej istotnych w kryptografii kwantowej programowalnych warstw logicznych, takich jak procedury korekty błędów i tzw. wzmocnienia prywatności.

Odległości, na jakie umiemy przekazywać w kontrolowany sposób zapisane w fotonach informacje, nie są imponujące. Profesor Anton Zeilinger przeprowadził słynną teleportację

stanu między splątanymi fotonami z La Palmy na Teneryfę, czyli na odległość niespełna 150 km. To na razie rekord. A we Wrocławiu jak daleko przekazujemy kwantowe klucze?

Testy laboratoryjne przeprowadzamy na wielokilometrowych, standardowo używanych w sieciach telekomunikacyjnych wiązkach światłowodowych z licznymi spawami. Praktyczne połączenie realizujemy z budynku NOT-u przy ul. Piłsudskiego do budynków przy ul. Racławickiej. Tam mieszczą się firmy wdrożeniowe CompSecur i seQre, w których pracują nasi absolwenci. Usiłujemy właśnie rozbudować sieć o połączenie z gmachem głównym Politechniki Wrocławskiej. Główna trudność polega na nieoczekiwanych oporach Działu Informatyzacji naszej uczelni *[śmiech]*.

Może to nie są imponujące odległości, ale w tej chwili tylko w trzech miastach na świecie stosuje się kryptografię kwantową w zwykłej, publicznie dostępnej, miejskiej sieci światłowodowej. Dwa pozostałe miasta to Tokio i Wiedeń, w tym ostatnim pracuje właśnie profesor Zeilinger.

Dla pojedynczych fotonów, które są nośnikami informacji, miejskie światłowody to drogi bardzo wyboiste. Przeszkodami są wszystkie niedoskonałości, jak np. spawy szklanych nitek światłowodowych, które nie miały żadnego znaczenia dla silniejszych wiązek światła. Oczywiście niepublicznych połączeń jest więcej. Można tu wskazać na działające już zabezpieczenia banków szwajcarskich czy luksemburskich, w których kryptografia kwantowa strzeże krytycznych połączeń między centrami rozliczeniowymi i archiwizacji. Podejrzewam, że kryptografia kwantowa jest wykorzystywana w komunikacji między Białym Domem a Pentagonem. Dobrze by było, żeby u nas zastosowano takie rozwiązanie między Pałacem Prezydenckim a Sztabem Generalnym.

Jest pan fizykiem teoretykiem, zajmuje się pan problemami podstawowymi o charakterze czysto poznawczym. Nie żal panu odrywać się od pięknych teorii, poświęcać czas kablom i metalowym skrzynkom?

Rzeczywiście zajmujemy się głównie bardziej teoretycznymi projektami, obecnie z zakresu plazmoniki, a także z podstaw mechaniki kwantowej. Jednak wbrew pozorom wielu teoretyków tęskni czasem do eksperymentów, lubi dla równowagi zająć się czymś, czego można dotknąć.

rozmawiała Małgorzata Porada-Labuda

5. Międzynarodowe Sympozjum LFPPI: Progress in Quantum Cryptography „seQre2014”, 27-28 stycznia, początek o godz. 10 w auli gmachu głównego (bud. A-1, wybrzeże Wyspiańskiego 27). Wstęp wolny.