To dobry moment, by inwestować w kryptografię kwantową

1 sierpnia 2019

To dobry moment, by inwestować w kryptografię kwantową. Polska ma w tej dziedzinie dobrych specjalistów. Wymaganiom mogłyby sprostać nawet małe firmy – mówi w rozmowie z PAP współtwórca kwantowej kryptografii, prof. Artur Ekert z Uniwersytetu Oksfordzkiego. Prof. Artur Ekert to fizyk, współodkrywca nowej dziedziny, jaką jest kryptografia kwantowa. Studiował na UJ, ale od końca lat 1980. związany jest z Uniwersytetem Oksfordzkim. Warszawę odwiedził w ramach warsztatów European Study Groups with Industry, podczas których matematycy rozwiązują zadania dla przemysłu.

– Proszę się pochwalić: jaką rolę odegrał pan już w dziedzinie, jaką jest kryptografia kwantowa?

– Współuczestniczyłem w odkryciu szyfrów kryptografii kwantowej. Dwójka moich kolegów z Ameryki Północnej – Charles Bennett i Gilles Brassard – w połowie lat 80. wpadła na pomysł, żeby opracować szyfry dla kryptografii kwantowej. Ja na podobny pomysł wpadłem pięć lat później, niespecjalnie wiedząc o ich badaniach. Dopiero później się poznaliśmy. Teraz się przyjmuje, że we trójkę stworzyliśmy dziedzinę kryptografii kwantowej. Szyfry, które zaproponowaliśmy, są różne. Oni proponowali wykorzystanie w szyfrowaniu zasady nieoznaczoności Heisenberga. Moja metoda wykorzystuje zaś zjawisko, jakim jest splątanie kwantowe. Była to metoda trudniejsza do implementacji, ale prowadzi ona do opracowania bezpieczniejszych szyfrów kryptografii kwantowej. Z czasem technologia się rozwinęła i teraz moja metoda jest bardziej popularna.

– Po co ludziom kryptografia kwantowa?

– To szersze pytanie: po co komu ochrona danych. Od czasów starożytności ludzie zawsze chcieli coś szyfrować. Teraz też każdy ma swoje sekrety: potrzebna jest nam ochrona naszych danych medycznych, transakcji online, kart kredytowych. Szyfrowanie danych potrzebne jest też w wojsku czy biznesie.

– Jak wygląda przekazywanie informacji z wykorzystaniem kryptografii kwantowej?

– W kryptografii obowiązuje zasada, że zanim dwie strony zaczną się komunikować, to muszą się wymienić tajnym, znanym tylko im, kluczem kryptograficznym. Stanowi on przepis na to, jak później odczytać wiadomość. W naszym przypadku klucz to przypadkowy ciąg zer i jedynek. Pytanie brzmi: jak ten klucz bezpiecznie przesłać, np. z Oksfordu do Warszawy. W tradycyjnych rozwiązaniach nigdy nie mamy gwarancji, że ktoś tego klucza w czasie transmisji nie podejrzy. Dlatego w moim systemie wykorzystuje się efekty kwantowe, które dają pewną informację, czy ktoś po drodze klucza nie podejrzał. Generujemy parę splątanych fotonów – jeden trafia do jednej osoby, a drugi do drugiej. Obie osoby muszą dokonać detekcji w tym samym czasie. Fotony są splątane, a więc jeśli zna się właściwości jednego – wiadomo, jakie właściwości ma drugi. Mierząc te właściwości, ustala się kolejne cyfry klucza. Zjawisko splątania fotonów sprawia, że jeśli ktoś podejrzy komunikację, obie strony od razu będą w stanie się zorientować, że coś jest nie tak. W kryptografii kwantowej zawsze więc da się odkryć, czy ktoś nas podsłuchuje.

– Jaką jeszcze przewagę daje kryptografia kwantowa?

– Jest ona odporna na ataki za pomocą komputerów kwantowych. Bo jeśli komputer kwantowy w końcu powstanie, to będzie mógł rozszyfrować algorytmy szyfrujące, algorytmy klucza publicznego, których obecnie używamy.

– Ale komputery kwantowe nie są konieczne, żeby korzystać z

kryptografii kwantowej?

– Nie. Komputery kwantowe i kryptografia kwantowa to dwie różne rzeczy. Mają wspólny mianownik – w obu z nich używa się efektów kwantowych, żeby coś robić z informacją. Kwantowa kryptografia używa efektów kwantowych do bezpiecznego przesyłania informacji. A komputery kwantowe mają na celu przetwarzanie informacji w sposób bardziej efektywny. Kryptografia kwantowa jest łatwiejsza do implementacji. Każde dobre laboratorium optyki kwantowej dałoby sobie radę zaimplementować kryptografię kwantową w najprostszej postaci. Dlatego na rynku istnieją już firmy sprzedające zestawy do kryptografii kwantowej. Natomiast komputery kwantowe to urządzenia znacznie bardziej skomplikowane. Prawda jest taka, że nie mamy jeszcze czegoś, co można byłoby nazwać komputerem kwantowym.

– To raczej kwantowe liczydła?

– Właśnie.

– Jak w praktyce wygląda przesyłanie tajnych danych w kryptografii kwantowej?

– Na rynku jest już dostępne urządzenie, w którego skład wchodzi źródło splątanych fotonów. Po drugiej stronie – u odbiorcy – są fotodetektory, które odbierają sygnały. Jest też elektronika, która pozwala na implementację protokołu. Fotony można przesłać za pośrednictwem światłowodów. Ale w mojej metodzie źródło splątanych fotonów można umieścić nawet na satelicie. Chińczycy już uruchomili satelitę Micius, która wysyła do odbiorców takie splątane fotony. Tam właśnie zastosowano mój protokół. Inwestując w kryptografię kwantową Chińczycy pokazują światu, jakie mają możliwości.

– Gdzie jeszcze kryptografia kwantowa jest już używana?

– W Tokio podczas zbliżającej się olimpiady duża część komunikacji prowadzona będzie za pomocą kryptografii

kwantowej. Kryptografię kwantową zastosowano również w czasie niedawnych mistrzostw sportowych w Durbanie w RPA.

– To znaczy, że technologia zaczyna być używana na masową skalę?

– Nie wiem, czy już na masową, ale ludzie zaczynają jej używać. Zwłaszcza bardziej rozwinięte kraje chcą zademonstrować, że można z tych technologii korzystać. I tak np. w Singapurze jest plan, by cały kraj objąć siecią światłowodową, która będzie mogła służyć do dystrybucji kluczy w kryptografii kwantowej.

– Czy aby korzystać z kryptografii kwantowej, trzeba przeprojektować istniejącą internetową sieć światłowodową?

– Niekoniecznie. Można wykorzystywać sieci istniejące. Trzeba jednak móc podłączyć urządzenia kwantowe do tej sieci.

– Co pan z tego ma, że pana rozwiązaniami zaczyna się interesować cały świat?

– Przede wszystkim satysfakcję. To nie jest rzecz, z której człowiek zarabia pieniądze. Swoje badania realizowałem w ramach rozprawy doktorskiej. Nikt wtedy nie brał tego na poważnie.

– Opatentował pan swój pomysł?

– Nie. Opublikowałem to. Wtedy nie wydawało się, że to jest pomysł, który można opatentować. Patenty przyszły później i dotyczyły szczegółowych rozwiązań. Nie spodziewałem się, że to wszystko się tak szybko rozwinie. Ale to już nie moja zasługa. To zasługa tych, którzy widzieli, że coś w tych rozwiązaniach jest.

– Czy z punktu widzenia przemysłu jest w tych rozwiązaniach coś wartego uwagi?

– Wydaje mi się, że to dobry moment, aby z tymi technologiami

eksperymentować. Dużo osób, które teraz w to inwestują – odpadnie. Jednak pewna grupa firm zostanie i będzie dominować w technologii kwantowej. To na pewno nastąpi, nie ma wątpliwości, kwestią pozostaje: kiedy.

– Myśli pan, że jest sens, by w Polsce inwestować w kryptografię kwantową?

– Nie jestem guru biznesu, ale wydaje mi się, że jest na to rynek. Nawet małe firmy potrafiłyby tym wymaganiom sprostać. Poza tym Polska może sobie pozwolić, by robić badania eksperymentalne w tym zakresie. Akurat dziedzina, na której bazuje kryptografia kwantowa – optyka kwantowa – jest w Polsce mocna. Polska ma świetnych fizyków, gównie teoretyków. A w tej dziedzinie zawsze coś znaczyła.

– Jak może wyglądać rynek kryptografii kwantowej w przyszłości? Jak pan myśli, będzie to sprzedaż urządzeń?

– Pewnie będą urządzenia do generowania kluczy kryptograficznych. Będzie też pewnie możliwość podpięcia się, np. za pomocą satelity, do serwera generującego takie klucze. Przewidywania biorą jednak w pewnym momencie w łeb. To tak, jak z elektrycznością. Kiedy Michaela Faradaya pytano, do czego to posłuży – odpowiedział, że nie wie, ale że da się to opodatkować. I myślę, że podobnie będzie z technologią kwantową. Nie wiem, do czego może to służyć, ale wierzę, że prędzej czy później rządy będą to opodatkowywać.

– Czy pan wraz z kolegami stworzył nowy obszar wiedzy?

– Tak, to się nazywa kwantowa informacja, która została uznana za dziedzinę samą w sobie. Ona mieści w sobie kwantową kryptografię, kwantowe komputery i inne kwantowe operacje, pozwalające na kwantowe przetwarzanie informacji i przesyłanie danych itp. Jest to dziedzina interdyscyplinarna, łącząca w sobie fizykę, fizykę kwantową, teorię informacji, kryptologię, informatykę czy inżynierię.

– Na wszystkich tych dziedzinach się pan zna?

– Historycznie podzieliliśmy sobie wiedzę na szufladki, takie jak matematyka, fizyka czy informatyka. Przyroda nie wie jednak o tym podziale. Pomiędzy tymi obszarami jest dużo ciekawych rzeczy do odkrycia – właśnie ze względu na tradycję kształcenia w obszarach. Uniwersytety dodatkowo ten podział usztywniają. Dużym szczęściem było to, że mogłem to robić swoje badania w Oksfordzie. Tam można łatwiej robić badania interdyscyplinarne. I tak np. w moim koledżu byli matematycy, ludzie, którzy zajmowali się informatyką, kryptologią, historią. Łatwo można z nimi porozmawiać w czasie lunchu czy obiadu. W ten nieformalny sposób człowiek wiele rzeczy się dowiaduje. Nie znam się na tych dziedzinach, ale dzięki tym rozmowom trochę się o nich dowiedziałem. Warto, by był rzeczywisty kontakt z ludźmi z innych dziedzin.

Z prof. Arturem Ekertem rozmawiała Ludwika Tomala
Źródło: NaukawPolsce.PAP.pl