Kwantowa dystrybucja klucza. Postępy i problemy

dr inż. WOJCIECH NOWAKOWSKI

Instytut Maszyn Matematycznych, Warszawa

W kryptografii kwantowej klucz może być przesyłany kanałem publicznym, ponieważ każda próba przechwycenia transmitowanej informacji wprowadza zmiany, ujawniające fakt podsłuchu. Rozróżnia się dwa główne typy kryptosystemów kwantowych:

- pierwszy, zasygnalizowany przez Stephena Wiesnera w latach 70. i rozwinięty w 1984 r. przez Charlesa H. Bennetta oraz Gillesa Brassarda [1], wykorzystuje fakt, iż pomiar dowolnego stanu mikroobiektu nieodwracalnie zmienia ten stan. Kryptosystemy tego typu, z kodowaniem opartym na pomiarze jednej z dwóch możliwych wielkości reprezentowanych przez niekomutujące (nieprzemienne) operatory hermitowskie, np. protokół BB84, przedstawiono pokrótce w [2],
- drugi, zarazem lepiej rokujący, został opisany w 1991 r. przez Artura Ekerta [3], polskiego profesora fizyki kwantowej, pracującego w Oksfordzie (i w Singapurze), opiera się na zjawisku stanów splątanych par cząstek (a właściwie ich spinów), tzw. singletów (czyli związanych nierównością Bella par EPR), które mają taką właściwość, że gdy zmierzymy pewną składową spinu jednej z nich, to pomiar da nam nie tylko jej wartość, ale jednocześnie wartość identycznej składowej spinu drugiej cząstki. Bezpieczeństwo kryptosystemu kwantowego Ekerta polega przede wszystkim na tym, że informacja definiująca klucz pojawia się nie podczas procesu przesyłania, lecz dopiero po pomiarach dokonanych przez nadawcę i odbiorcę. Dla nadawcy i odbiorcy rezultaty ich własnych pomiarów wyglądają na całkowicie przypadkowe. Jeśli jednak obaj porównają wyniki, okaże się, że istnieją między nimi korelacje wynikające ze splątania. W uproszczeniu zasadę tego typu kryptosytemu kwantowego opisano w [4].

Rys. 1. Artur Ekert (pl.wikipedia.org/wiki/Artur_Ekert)
Fig. 1. Artur Ekert (en.wikipedia.org/wiki/Artur_Ekert)

Powyższa zasada dotyczy przypadków idealnych, gdy splątanie jest maksymalne. W rzeczywistości splątanie jest zaszumione i korelacje nie są doskonałe. Ustalenie czy przekaz był podsłuchiwany, jest trudne. Są wprawdzie procedury pozwalające uzyskać ze stanów zaszumionych pewną liczbę stanów o splątaniu maksymalnym, istnieje jednak wiele stanów, z których destylacja splątania jest niemożliwa (w roku 1997 fizycy z Gdańska: Ryszard, Michał i Paweł Horodeccy [5] wykazali istnienie związanych stanów splątanych, których nie da się przekształcić w stany maksymalnie splątane). Przez długi czas stany te były traktowane jako nieprzydatne dla kryptografii kwantowej. Jednak w 2005 r. uczeni z tej samej grupy teoretycznie wykazali, że niekiedy klucz kryptograficzny można wydajnie przesłać mimo braku splątania maksymalnego.

Zespół naukowy koordynowany przez prof. prof. Konrada Banaszka z Wydziału Fizyki Uniwersytetu Warszawskiego (FUW) i Pawła Horodeckiego z Wydziału Fizyki Technicznej i Matematyki Stosowanej Politechniki Gdańskiej (PG), przy udziale dr Krzysztofa Dobka, stażysty w Krajowym Laboratorium Fizyki Atomowej, Molekularnej i Optycznej przy Uniwersytecie Mikołaja Kopernika w Toruniu, pracujący w ramach Narodowego Laboratorium Technologii Kwantowych (http://nltk.home.pl), sprawdzili eksperymentalnie teoretyczne prace gdańskich fizyków [6].

Rys. 2. Szyfrowanie kwantowe 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)

Fig. 2. Quantum encryption by means of sources of noisy entanglement. In the picture from the left: Prof. Paweł Horodecki (PG), Rafał Demkowicz-Dobrzański, PhD (FUW) and Michał Karpiński, PhD student (FUW) (Source: NLTK, Grzegorz Krzyżewski)

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. Analizę danych i teoretyczną rekonstrukcję zarejestrowanych stanów kwantowych przeprowadzili dr Rafał Demkowicz-Dobrzański i mgr Michał Karpiński (FUW). Wykazano, że mimo zaszumienia splątania, w każdej czwórce fotonów można było bezpiecznie przesłać średnio 0,7 bita klucza kryptograficznego. Opis eksperymentu i analizę danych opublikowano w [7, 8].

Eksperyment ten może mieć istotne znaczenie dla praktycznej kryptografii kwantowej, która wychodzi już z laboratoriów. Obecnie przy szyfrowaniu stosuje się źródła stanów czystych, maksymalnie splątanych. Opisane doświadczenie polskich fizyków wykazuje, że przyszłe źródła cząstek splątanych będzie można wykorzystać do przesyłania kwantowego klucza kryptograficznego nawet w sytuacji, gdy generowane splątanie jest zaszumione i trudne do destylacji.

Wiodącym ośrodkiem badawczym w dziedzinie kryptografii kwantowej w Europie jest Cambridge Research Laboratory (CRL), pierwsze zagraniczne laboratorium badawczo-rozwojowe koncernu Toshiba. Laboratorium to wchodzi w skład klastra innowacyjnego (badawczego) w Cambridge, w ścisłej współpracy z tamtejszym Uniwersytetem. CRL składa się obecnie z trzech zespołów badawczych: Informatyki Kwantowej, Technologii Mowy i Computer Vision (budowania dokładnych modeli 3D obiektów z obrazów i wideo). CRL zaprezentowało 15 kwietnia 2010 roku wysoce bezpieczny kanał kwantowej dystrybucji kluczy dedykowany np. dla banków, szpitali i organizacji rządowych [9]. Udało się uzyskać kwantową transmisję klucza z prędkością przekraczającą 1 Mb/s na odległość ponad 50 km. Jest to 100-1000 razy szybciej niż uzyskiwano dotychczas na takiej odległości. Wyniki takie osiągnięto dzięki wprowadzeniu dwóch innowacji opracowanych przez zespół Cambridge: nowego szybkiego detektora światła oraz systemu sprzężenia zwrotnego, który utrzymuje wysoką szybkość transmisji i nie wymaga ręcznej obsługi i regulacji. Toshiba zrealizowała także swój kanał kwantowej dystrybucji kluczy w sieci kryptografii kwantowej utworzonej w obszarze metropolitalnym Tokio w październiku 2010 roku. W serii prób uzyskano bezpieczną szybkość transmisji 304 kb/s, średnio w okresie 24-godzinnym na 45-kilometrowym światłowodzie, pomimo stosunkowo dużych strat na łączu (14,5 dB).

Rys. 3. Serwer klucza kwantowego w łączu Toshiby

Fig. 3. Quantum Key Server consists of two compact boxes designed to fit into a communications rack (http://www.toshiba-europe.com/research/crl/qig/quantumkeyserver.html)

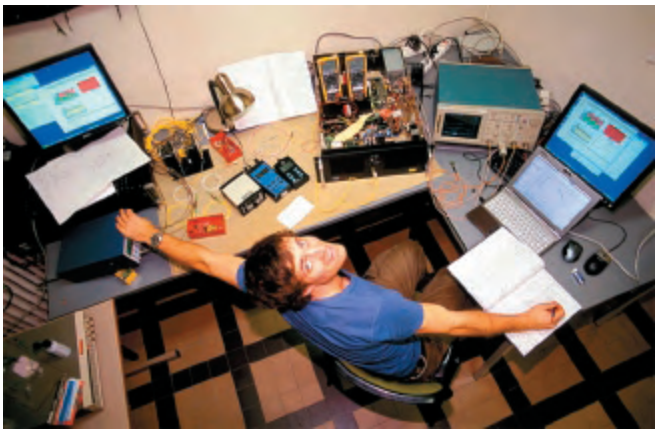
Nowa technologia pozwoli na rutynowe używanie jedynego znanego szyfru, o którym wiadomo na pewno, że jest teoretycznie niemożliwy do złamania – tzw. szyfru jednokrotnego (*one-time pad*). Używanie tego sposobu szyfrowania w przeszłości było ograniczone, gdyż wymaga on transmisji bardzo długich kluczy tajnych (tak samo długich jak szyfrowane dane). Z tego powodu technologię szyfru jednokrotnego stosowano wyłącznie do krótkich komunikatów przy wymaganiu bardzo wysokiego poziomu bezpieczeństwa, na przykład w wojsku i służbach. Szybkość transmisji uzyskana w CRL stwarza perspektywę użycia metody *one-time pad* do powszechnych zastosowań. Przykładem nowych możliwości, jakie daje ten system, jest szyfrowanie w czasie rzeczywistym transmisji sygnału video.

Teoretycznie kwantowa dystrybucja klucza kryptograficznego jest bezpieczna. Nie jest to jednak prawda, bowiem istniejące implementacje techniczne mają wiele niedoskonałości. Wynajdywanie tych słabych miejsc jest niezwykle atrakcyjne i popularne w światku kwantowych hakerów. Młodzi naukowcy z Centre for Quantum Technologies prof. Ekerta chwalą się, że mogą złamać każdy kwantowy system kryptograficzny [10] i jest to prawda.

Między innymi naukowcom Norweskiego Uniwersytetu Nauki i Technologii w Trondheim udało się dokonać ingerencji w transmisję kwantową dzięki niedoskonałości detektorów pojedynczych fotonów, zwykle fotodiod lawinowych. Wykazano, że detektory

Rys. 4. Tworzenie obrazów w CRL sterowane gestem (http://www.engadget.com)

Fig. 4.Toshiba's Cambridge Research Lab shows off gesture-controlled TVs, image recognition (http://www.engadget.com/photos/toshibas-cambridge-research-lab-shows-off-gesture-controlled-tvs-image-recognition/1006462/)



Rys. 5. Lars Lydersen z Norweskiego Uniwersytetu Nauki i Technologii „podsłuchuje" kwantową transmisję klucza kryptograficznego

Fig. 5. Lars Lydersen hacking QPN 5505 QKD system. The blue monitors belong to Alice and Bob, and display internal diagnostics at the two sides of the secure link (http://www.iet.ntnu.no/groups/optics/qcr/hacking-commercial-quantum-cryptography-2010/)

można „oślepić" silnym światłem, co w konsekwencji umożliwiło podsłuch [11]. Już w listopadzie 2010 roku CRL ogłosiło, że odkryło prostą metodę zapobiegania atakom na transmisję kryptograficzną metodą oślepiania detektora [12] sugerując, że atak jest skuteczny tylko wtedy, jeśli rezystor redundancyjny jest połączony szeregowo z pojedynczym detektorem fotonów, lub jeśli nieprawidłowo ustawione są poziomy dyskryminacji. Ponadto podano, że jest możliwe wykrycie tego rodzaju ataków poprzez monitorowanie prądu generowanego przez detektor. Jednak w tym samym numerze Nature Photonics ukazała się notka norweskich naukowców o ograniczonej skuteczności proponowanych środków zaradczych [13].

W pracy [14] fizycy z Uniwersytetu w Toronto (Dept. of Physics and Dept. of Electrical and Computer Engineering) wykazali eksperymentalnie techniczną możliwość wykonania ataku na transmisję klucza kryptograficznego metodą „przechwyć i wyślij", która wykorzystuje lukę w zabezpieczeniach komercyjnej wersji kwantowego protokołu dystrybucji klucza BB84. W uproszczeniu atak

taki polega na obniżeniu stopy błędów podsłuchanej transmisji do ok. 19%, podczas gdy w protokole BB84 uznaje się, że stopa błędów transmisji poniżej 20% świadczy o braku podsłuchu.

Nie możemy na prawa fizyki kwantowej zrzucać odpowiedzialności za dotrzymanie tajemnicy – podkreśla prof. Kurtsiefer z Centre for Quantum Technologies przy National University of Singapore. Musimy dokładnie przetestować konkretne urządzenia, których używamy. Kryptografia kwantowa jest obecnie w fazie, w której bezpieczeństwo poszczególnych wdrożeń jest dokładnie analizowane i testowane. Ważne jest odkrywanie luk w implementacjach i opracowywanie odpowiednich środków zaradczych. Ataki kwantowych hakerów ujawniają miejsca, w którym należy zabezpieczać tę technologię. Świat realny daleki jest od matematycznej perfekcji. Łatanie najnowszej technologii, która teoretycznie powinna być nie do złamania, nie powinno nikogo dziwić.

Literatura

[1] Bennett C. H., Brassard G.: Quantum Cryptography: Public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore 1984.

[2] Nowakowski W.: O kryptografii kwantowej. Elektronika, nr 2, Warszawa 2010.

[3] Ekert A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., 1991.

[4] Czajkowski R., Nowakowski W.: O protokóle Ekerta w kryptografii kwantowej. Elektronika, nr 3, Warszawa 2010.

[5] Horodecki R., Horodecki M., Horodecki P.: Correlation and information-theoretic aspects of quantum nonseparability of mixed states. Rozprawa habilitacyjna, Uniwersytet Mikołaja Kopernika, Toruń 1997.

[6] http://www.fuw.edu.pl/informacja-prasowa/items/news1180.html

[7] Dobek K. i in.: Experimental Extraction of Secure Correlations from a Noisy Private State. Physical Review Letters 106, American Physical Society, 2011.

[8] http://ebookbrowse.com/010-prezentacja-konrad-banaszek-pptx-d125213358

[9] Dixon A.R. et al.: Continuous operation of high bit rate quantum key distribution. Toshiba Research Europe Ltd, Cambridge Research Laboratory, Cambridge 2010, http://www.toshiba-europe.com/research/crl/qig/pdfs/ContinuousOperationHighBitRateQKD.pdf.

[10] http://www.polityka.pl/nauka/komputeryiinternet/1506974,1,kryptografia-nie-z-tego-swiata.read

[11] Lydersen L., Skaar J., Makarov V.: Tailored bright illumination attack on distributed-phase-reference protocols. Journal of Modern Optics, Vol. 58, Issue 8, UK 2011.

[12] Yuan Z. L., Dynes J.F., Shields A.J.: Avoiding the blinding attack in QKD. Nature Photonics 4, Correspondence, Dec. 2010.

[13] Lydersen L. et al.: Avoiding the blinding attack in QKD. Nature Photonics 4, Correspondence, Dec. 2010.

[14] Feihu Xu, Bing Qi, Hoi-Kwong Lo: Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. http://arxiv.org/pdf/1005.2376v1.pdf.