O protokóle Ekerta w kryptografii kwantowej

mgr inż. ROMAN CZAJKOWSKI, dr inż. WOJCIECH NOWAKOWSKI

Instytut Maszyn Matematycznych, Warszawa

W pracy [1] przedstawiono podstawowe pojęcia i informacje dotyczące informatyki kwantowej i jej zastosowania do kryptografii. Opisano w niej zasady kryptografii kwantowej i działanie całkowicie bezpiecznego kanału dystrybucji klucza wykorzystującego protokół BB84 [2], co w kryptografii jest zagadnieniem zasadniczym. Do kwantowej dystrybucji klucza zapewniającej pełne bezpieczeństwo transmisji można wykorzystać też zjawisko splątania fotonów, co pokazał w swojej rozprawie doktorskiej [3] A.K. Ekert, polski fizyk, absolwent Uniwersytetu Jagiellońskiego, obecnie profesor fizyki kwantowej na Uniwersytecie w Cambridge.

Splątanie

Mechanika kwantowa zakłada, że przed pomiarem wielkości kwantowej mierzona zmienna nie ma ustalonej wartości, a jedynie można mówić o rozkładach jej prawdopodobieństwa. Istnieją jednak tzw. stany splątane par obiektów kwantowych, które mają taką właściwość, że gdy dokonujemy pomiaru pewnej wielkości charakteryzującej obiekt, otrzymujemy zawsze przeciwne wyniki (pełna antykorelacja). Tego rodzaju obiektem mogą być m. in. kubity w postaci spolaryzowanych fotonów.

Stan splątany polaryzacji dwóch fotonów ma taką właściwość, że jeżeli będziemy mierzyć polaryzacje obu fotonów, używając dwóch identycznie ustawionych, ale odległych od siebie polaryzatorów, to zawsze otrzymamy dwie przeciwne polaryzacje. Natomiast zmierzone polaryzacje każdego z fotonów z osobna są zupełnie przypadkowe. Zatem para fotonów splątanych ma precyzyjnie określoną własność wspólną (polaryzacje mierzone tak samo ustawionymi polaryzatorami są zawsze przeciwne), natomiast stan podukładu, czyli pojedynczego fotonu jest całkowicie nieokreślony – wynik pomiaru polaryzacji pojedynczego fotonu jest zupełnie przypadkowy. Splątanie nie zanika wraz z odległością – tak przewiduje teoria kwantów (w latach 90. XX wieku eksperymentalnie udowodniono istnienie splątania pomiędzy fotonami odległymi od siebie o kilkanaście kilometrów (grupa Gisin'a, Genewa), potem zaobserwowano to zjawisko na odległości 144 km – na wyspach La Palma i Teneryfa (Anton Zeilinger i współpracownicy).

Pojęcie splątania zostało wprowadzone przez Erwina Schroedingera w 1935 roku. Leży ono u podstaw paradoksu EPR (Einsteina, Podolskiego i Rosena) polegającego na tym, że istnieje oddziaływanie rozchodzące się natychmiastowo na dowolną odległość, mimo że szczególna teoria względności wyklucza przekazywanie informacji i oddziaływań z prędkością większą od prędkości światła. Rozumując dalej wywnioskowali, że zmienne kwantowe muszą mieć ustaloną wartość przed pomiarem, co z kolei musiało prowadzić do wniosku, że mechanika kwantowa jest teorią niepełną, bo nie określa tych ustalonych wartości, a jedynie ich prawdopodobieństwa. Wszystko to doprowadziło do twierdzenia Bella o niemożliwości pogodzenia opisu kwantowego mikroświata z opisem o charakterze klasycznym zgodnym z teorią względności. Stany splątane jednak istnieją i mają szerokie zastosowanie w informatyce kwantowej (zwłaszcza w kryptografii i teleportacji kwantowej).

Przypomnijmy za [1, 4, 5], że rozróżnia się dwa główne typy kryptosystemów kwantowych:

– **kryptosystemy z kodowaniem opartym na pomiarze jednej z dwóch możliwych wielkości** reprezentowanych przez niekomutujące (nieprzemienne) operatory hermitowskie, tzw. protokół BB84 [2]), który można pokrótce przedstawić następująco (**N** – nadawca, **O** – odbiorca):

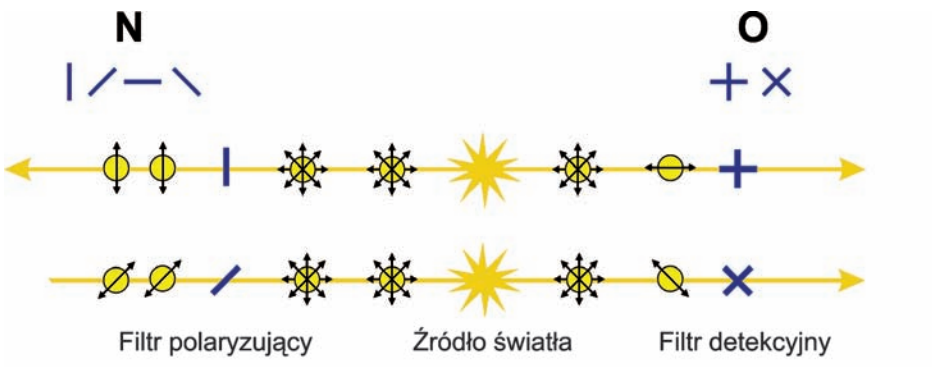
1. **N** losuje klucz i przesyła go **O** przy losowo ustawionych bazach polaryzatorów: prostej 0/90 lub ukośnej +45/–45 stopni.
2. **O** za pomoca losowo ustawionych baz swoich polaryzatorów i detektorów odbiera transmisję.
3. **O** jawnym kanałem przekazuje w jaki sposób ustawił swoje detektory.
4. **N** informuje **O** kanałem jawnym, w których przypadkach się pomylił.
5. **N** i **O** odrzucają niezgodne części klucza.
6. **N** i **O** jawnym kanałem porównują kilka bitów z uzyskanego klucza. Jeżeli sprawdzane fragmenty są zgodne odrzucają je i rozpoczynają transmisję z użyciem pozostałej części klucza.

– **kryptosystemy z kodowaniem opartym na zjawisku stanów splątanych**, tzw. protokół EPR. Protokół ten zaproponowany w 1991 roku przez Ekerta [3], opiera się na zjawisku EPR. Najogólniej mówiąc polega on na tym, że w generowanej sekwencji par splątanych (czyli związanych nierównością Bella par EPR) N i O badają polaryzację tych par:

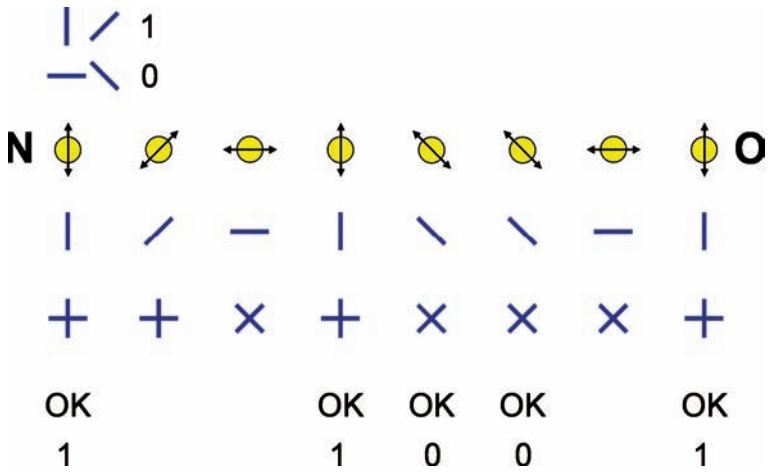
1. Splątane fotony są wytwarzane przez źródło niezależne od **N** i **O.**
2. **N** i **O** otrzymują po jednym fotonie ze splątanej pary.
3. **N** poprzez pomiar polaryzacji swojego fotonu wpływa na stan kwantowy fotonu **O.**
4. **O** dokonuje pomiaru stanu kwantowego swojego fotonu.
5. Po zakończeniu procedury przesyłania fotonów, **O** posiada pierwotny kod (raw key) zawierający około 25% błędów i kontaktuje się z **N** w celu porównania bramek użytych do polaryzacji fotonów i jej pomiaru.
6. Klucz przesiany (shifted key) składa się z ciągu bitów, dla których bramki wybrane przez **N** i **O** były zgodne (około 50%)

Opisany algorytm można zilustrować następującymi schematami [4]:

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. Każdy pomiar jest natomiast integralną częścią badanego układu.



Rys 1. Zasada transmisji według protokołu Ekerta. Fig. 1. Example of the Ekert protocol



Rys. 2. Uzyskany kod. Fig. 2. Received code

Literatura

[1] Nowakowski W.: O kryptografii kwantowej. Elektronika, nr 2, Warszawa 2010.
[2] 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.
[3] Ekert A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., 1991.
[4] Borkowska A.(UMCS Lublin): Kryptografia kwantowa, czyli praktyczne zastosowanie nieintuicyjnych cech realnego świata. Referat wygłoszony na V OSKNF, Wrocław 17-19.09.2006.
[5] Tanaś R.: http://zon8.physd.amu.edu.pl/~tanas/