Bezpieczeństwo powszechnie dzisiaj stosowanych systemów kryptograficznych opiera się na przekonaniu, że wykonanie niektórych operacji matematycznych jest bardzo trudne (MT 01/2010). Taką operacją jest np. rozkładanie liczb na czynniki pierwsze. Z punktu widzenia fundamentalnego nie są to zatem szyfry, których nie można sforsować. Prawa mechaniki kwantowej rządzące zachowaniem się obiektów w mikroświecie dostarczają nam nowych możliwości, które bezpieczeństwo kryptograficzne zakotwiczają w samych prawach przyrody. Takich szyfrów sama przyroda nie pozwala złamać.

Tomasz Sowiński jest fizykiem na Wydziale Biologii i Nauk o Środowisku UKSW i w Centrum Fizyki Teoretycznej PAN. W 2005 roku skończył studia na Wydziale Fizyki Uniwersytetu Warszawskiego w zakresie fizyki teoretycznej, a trzy lata później uzyskał tam stopień naukowy doktora. Od lat zajmuje się popularyzacją nauk przyrodniczych. W roku 2008 otrzymał tytuł Mistrza Popularyzacji Nauki „Złoty Umysł" w konkursie Prezesa Polskiej Akademii Nauk.

Tomasz Sowiński

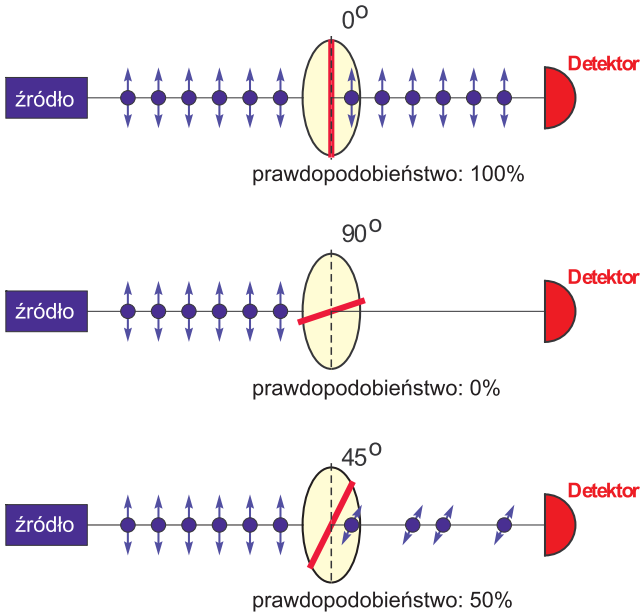
Kryptografia klasyczna i kwantowa cz. II

TEKST ŚREDNIO TRUDNY

POLARYZACJA FALI ELEKTROMAGNETYCZNEJ

Efekt kwantowy, który daje nam możliwość bezpiecznej komunikacji na odległość, związany jest bezpośrednio z polaryzacją fali elektromagnetycznej. Dokładniej mówiąc, jest związany z polaryzacją fotonów, które są nośnikiem tej fali. Polaryzacji poświęciliśmy bardzo wiele czasu (MT 10–12/2009) i chyba każdy już dobrze wie, jakie tajemnice kryje to pojęcie zarówno w obrazie klasycznym (falowym), jak i kwantowym (fotonowym). Przypomnę zatem tylko podstawowe elementy, które będą mi potrzebne do przedstawienia sposobu na wygenerowanie absolutnie bezpiecznego klucza kryptograficznego. Najlepiej zrobić to w punktach:

1. Każda fala elektromagnetyczna może być uważana za strumień cząstek zwanych fotonami. Obraz taki jest szczególnie użyteczny, gdy mamy do czynienia ze zjawiskami zachodzącymi w mikroświecie.
2. Każdy foton ma w sobie w pewien sposób zapisaną informację o fali, której jest nośnikiem. Ma w sobie zakodowaną zarówno jej częstość, jak i polaryzację.
3. Polaryzację fali elektromagnetycznej można zmieniać za pomocą polaryzatora.
   a. Światło spolaryzowane w kierunku zgodnym z kierunkiem osi ustawionego na jego drodze polaryzatora przechodzi na drugą stronę niezmienione.
   b. Światło spolaryzowane prostopadle do kierunku osi ustawionego na jego drodze polaryzatora jest całkowicie przez niego pochłaniane.
   c. Światło spolaryzowane pod kątem 45° względem kierunku osi ustawionego na jego drodze polaryzatora jest w połowie przez ten polaryzator pochłaniane, a w połowie przepuszczane; przy czym przepuszczone światło ma obróconą polaryzację do kierunku zgodnego z kierunkiem polaryzatora.
4. W obrazie fotonowym działanie polaryzatora można zrozumieć jedynie, zakładając, że to, czy foton zostanie przepuszczony na drugą stronę, czy zostanie pochłonięty, jest całkowicie losowe. Jedynie znane są prawdopodobieństwa tych zdarzeń.
   d. Jeśli polaryzacja fotonu jest zgodna z osią polaryzatora, to prawdopodobieństwo przejścia fotonu na drugą stronę jest równe 100%.
   e. Jeśli polaryzacja fotonu jest prostopadła do osi polaryzatora, to prawdopodobieństwo przejścia fotonu na drugą stronę jest równe 0.
   f. Jeśli polaryzacja fotonu jest ustawiona pod kątem 45° do osi polaryzatora, to prawdopodobieństwo przejścia fotonu na druga stronę jest równe prawdopodobieństwu jego pochłonięcia i wynosi 50%; przy czym jeśli foton zostanie przepuszczony, to jego polaryzacja zostanie obrócona do kierunku zgodnego z kierunkiem osi polaryzatora.



PROSTA OBSERWACJA

Przedstawione powyżej zasady, na jakich odbywa się oddziaływania światła z polaryzatorami, są bardzo proste, ale mają dramatyczne konsekwencje. Jedną z nich jest niemożność dokładnego poznania polaryzacji nieznanego fotonu. Aby to zrozumieć, zastanówmy się, w jaki sposób możemy zmierzyć polaryzację danego fotonu. Jeśli na przykład wiemy, że foton ma polaryzację albo pionową, albo poziomą, to nie ma z tym żadnego problemu. Wystarczy ustawić na jego drodze polaryzator ustawiony w jednym z tych kierunków, a za nim detektor. Jeśli detektor zarejestruje foton, to znaczy, że padający foton miał polaryzację zgodną z kierunkiem ustawienia polaryzatora. Jak wynika bowiem z naszych prostych zasad, wtedy prawdopodobieństwo przepuszczenia fotonu wynosi 100%. Jeśli natomiast detektor fotonu nie zarejestruje, to też mamy informację o fotonie padającym. Wtedy wiemy, że miał on polaryzację prostopadłą do kierunku osi polaryzatora, bo właśnie w takiej sytuacji foton jest zawsze pochłaniany.

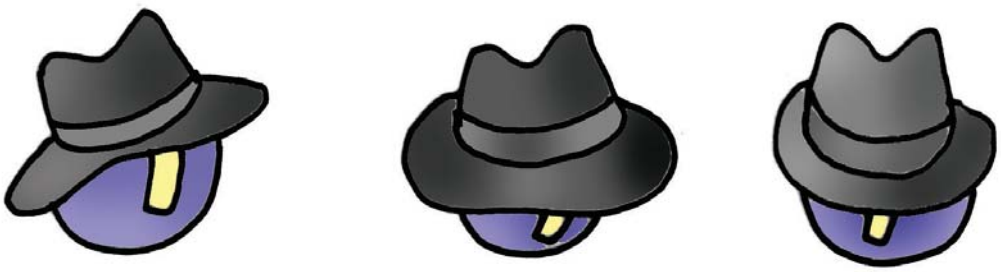
Problem pojawia się jednak, gdy zupełnie nie wiemy, w jakich kierunkach foton może być spolaryzowany. Jeśli bowiem na drodze zupełnie nam nieznanego fotonu ustawimy polaryzator np. w kierunku pionowym, to rejestracja fotonu przez detektor za nim ustawionym nie powie nam za wiele. Foton padający mógł być spolaryzowany pionowo i przeszedł przez polaryzator bez problemu. Ale równie dobrze mógł to być foton spolaryzowany pod kątem 45° i akurat tak się zdarzyło, że został on przepuszczony. Prawdopodobieństwo, że tak właśnie się stanie, wynosi przeciętnie 50%. Sam zatem fakt, że detektor coś zarejestrował, nie mówi nam nic o tym, którym z tych dwóch rodzajów mógł być padający foton. Jeśli detektor zarejestruje foton, to możemy być jedynie pewni na 100%, że foton padający nie był spolaryzowany poziomo. Wtedy bowiem nie miałby szans na przedarcie się przez polaryzator.

Sytuacja jest całkowicie analogiczna, gdy foton zostanie przez taki polaryzator pochłonięty. Wiemy wtedy na 100%, że foton padający nie był spolaryzowany pionowo. Wtedy bowiem nie mógłby być pochłonięty, bo taki foton przechodzi zawsze przez pionowo ustawiony polaryzator. Ale czy był to foton spolaryzowany poziomo, który jest na 100% pochłaniany, czy może foton spolaryzowany pod kątem 45°, który jest pochłaniany średnio jedynie w co drugiej próbie, nikt nie wie i nigdy się nie dowie. Co gorsza, w takiej sytuacji foton został zniszczony. Nic więcej zatem o nim się już nie dowiemy. Zresztą, jakby przeszedł przez polaryzator, to też już nic o nim dowiedzieć byśmy się nie mogli, bo po przejściu przez polaryzator ma on już polaryzację zupełnie obróconą i informacja o polaryzacji fotonu padającego została zniszczona.

PROTOKÓŁ BB-84

Ta prosta obserwacja i płynąca z niej lekcja wydaje się bardzo smutna. Wynika z niej jasno, że nigdy nie możemy się dowiedzieć wszystkiego o fotonie, który się do nas zbliża. Nie możemy zdobyć pełnej informacji o polaryzacji, jaka jest w nim zakodowana.

Protokół BB-84



Nie wiadomo w jakim kierunku jest spolaryzowany foton

Co gorsza, gdy próbujemy to zrobić, całkowicie tracimy możliwość powtórzenia eksperymentu, bo foton albo jest niszczony, albo całkowicie zmieniony.

Fizyk to jednak osoba, która nigdy nie obraża się na przyrodę. Nie możemy mieć pretensji do natury

o to, że działa w ten, a nie w inny sposób. Lepiej zastanowić się, czy takie dziwne zachowanie fotonów można jakoś wykorzystać. Takie właśnie optymistyczne podejście doprowadziło do opracowania sposobu na wygenerowanie całkowicie bezpiecznego klucza kryptograficznego. Ten sposób nazywamy dziś protokołem BB-84. Wymyślili go bowiem dwaj fizycy, Charles Bennett i Gilles Brassard, w roku 1984.

USTALANIE ZASAD

Załóżmy, że mamy dwie oddalone od siebie osoby A i B, które chcą ustalić między sobą tajny klucz kryptograficzny. W tym celu odbywają one na początku prostą rozmowę telefoniczną, która nie wymaga żadnych zabezpieczeń. Może być podsłuchiwana, nagrywana czy kopiowana dowolną liczbę razy, gdyż na bezpieczeństwo całej procedury nie ma to żadnego wpływu. Podczas tej rozmowy rozmówcy umawiają się, że jeden z nich (np. A) będzie wysyłał do B fotony o określonych polaryzacjach, przy czym polaryzacja każdego fotonu będzie jedną z czterech: pionową (↕), poziomą (↔), skośną (⤢) lub antyskośną (⤡). Polaryzacje te rozmówcy umownie dzielą na dwie grupy: grupę ⊕, do której należą polaryzacja pionowa

Ustalanie zasad

i pozioma, oraz grupę ⊗, do której należą pozostałe dwie. Każdy kolejny foton będzie miał jedną z tych czterech polaryzacji, ale nie wiadomo, który jaką, bowiem osoba A będzie to losowała. Przed zakończeniem rozmowy osoby A i B umawiają się jeszcze, że poszczególnym polaryzacjom przypisują wartości logiczne 0 i 1 w taki sposób, aby polaryzacje do siebie dokładnie prostopadłe (lub inaczej mówiąc: należące do tej samej grupy) miały różne wartości. Może to być np. zrobione tak: pionowa = skośna = 1, pozioma = antyskośna = 0. Mamy wtedy następującą tabelę kodową, która jest całkowicie jawna.

	1	0
⊕	↕	↔
⊗	⤢	⤡

Warto zauważyć, że ta tabela ma bardzo ciekawą własność. Otóż podając samą grupę albo samą wartość logiczną, nie można jednoznacznie określić fotonu. Do każdej grupy należą bowiem dwa fotony. Podobnie jest z każdą wartością logiczną. Aby jednoznacznie określić foton, trzeba mieć stuprocentową pewność, zarówno co do grupy, jak i wartości logicznej.

PRZESYŁANIE FOTONÓW

Po tej rozmowie osoba A zaczyna wysyłać do osoby B fotony. Robi to dokładnie tak, jak zapowiadała. Losuje jedną z czterech dostępnych polaryzacji i wysyła do B. Jednocześnie zapisuje sobie, jaki foton wysłała. Ciąg wysyłanych fotonów jest zupełnie przypadkowy i znany jedynie osobie A. Załóżmy, że wysłała ona dziesięć fotonów i miały one następującą losową kolejność:

wylosowana polaryzacja	↕	⤡	↕	↔	⤢	⤢	↔	⤡	↕	⤢
wartość	1	0	1	0	1	1	0	0	1	1
grupa	⊕	⊗	⊕	⊕	⊗	⊗	⊕	⊗	⊕	⊗

W wyniku tego procesu do osoby B dolatują fotony zupełnie przypadkowe o nieznanej jej polaryzacji. Polaryzacja fotonu nadlatującego jest zupełnie niepoznawalna. Jest tak ze względu na wcześniej poczynioną przez nas obserwację. Osoba B nie wie, do jakiej grupy należy nadlatujący foton. Nie może zatem przygotować swojego polaryzatora tak, aby mógł on jednoznacznie rozstrzygnąć, jaka jest polaryzacja nadlatującego fotonu. Gdyby np. ustawił polaryzator pionowo, to ze stuprocentową pewnością mógłby rozróżnić jedynie fotony o polaryzacji pionowej i poziomej. Jeden z nich zawsze przechodzi na drugą stronę, a drugi zawsze jest pochłaniany. Tak ustawiony polaryzator praktycznie nie rozróżnia natomiast fotonów z grupy skośnej. One przez polaryzator przechodzą dokładnie z takim samym prawdopodobieństwem, a po ewentualnym przejściu mają polaryzację pionową.

Z kolei ustawienie polaryzatora pod kątem 45° rozróżnia fotony ⤡ i ⤢, ale nic nie może powiedzieć o fotonach ↕ i ↔. Ponieważ osoba A wysyła fotony z dwóch grup zupełnie losowo z równym prawdopodobieństwem osoba B nie może na taką sytuację nic poradzić. I to wbrew pozorom jest właśnie siłą protokołu BB-84.

Przesyłanie fotonów

ODBIERANIE FOTONÓW

Osoba B odbiera fotony. Ponieważ nie może przewidzieć do jakiej grupy należy nadlatujący foton, wybiera tę grupę całkowicie losowo dla każdego z fotonów i notuje, co zaobserwowała. Jeśli foton przeleciał przez polaryzator, to przypisuje takiemu zdarzeniu wartość logiczną 1, jeśli foton zostanie pochłonięty, to 0. Krótko mówiąc, osoba B zakłada, że za każdym razem dobrze wybrała ustawienie osi swojego

J-42 przesyła garść fotonów

polaryzatora, to znaczy wybrała tak, że nadlatujący foton ma polaryzację albo do niej prostopadłą, albo równoległą. Oczywiście w rzeczywistości sytuacja jest zupełnie inna. Gdy nadlatujący foton „nie pasuje" do przygotowanego polaryzatora, to szansa na to, że przejdzie lub nie na drugą stronę polaryzatora, jest taka sama. Co gorsza, domniemana polaryzacja fotonu jest zupełnie inna niż polaryzacja fotonu, który naprawdę przyleciał.

Aby to zrozumieć, posłużmy się przykładem. Poniższa tabelka prezentuje wynik tego, co zapisze osoba B po przeprowadzeniu swojej procedury rejestrującej. Pierwszy wiersz prezentuje prawdziwe polaryzacje fotonów, które wysłała osoba A. Oczywiście osoba B tych danych nie ma. Drugi wiersz prezentuje kolejne grupy, jakie osoba B wylosowała. To losowanie prowadzi do odpowiedniego ustawienia polaryzatora. Kolejny wiersz to wyniki pomiarów, jakie dokona osoba B za pomocą swoich polaryzatorów na fotonach, które nadlatują. Jeśli osoba B dobrze trafi i wylosuje ustawienie polaryzatora dokładnie tak, aby pasował on do polaryzacji nadlatującego fotonu, to wynik pomiaru jest jednoznaczny i wywnioskowana na tej podstawie polaryzacja fotonu jest dokładnie taka, jak polaryzacja fotonu wysłanego przez A. Jeśli natomiast polaryzator niestety nie pasuje, to są możliwe dwie sytuacje. Każda z nich prowadzi do błędnego przewidywania prawdziwej polaryzacji fotonu.

prawdziwa polaryzacja	↕	↘	↕	↔	↗	↗	↔	↘	↕	↗
wylosowana grupa	⊕	⊗	⊗	⊗	⊗	⊕	⊕	⊗	⊕	⊕
wynik pomiaru	1	0	0|1	0|1	1	0|1	0	0	1	0|1
domniemana polaryzacja	↕	↘	↘|↙	↘|↙	↗	↔|↕	↔	↘	↕	↔|↕

UZGADNIANIE GRUP

W wyniku przeprowadzenia procedury, którą tu nakreśliłem, łatwo się przekonać, że osoby A i B dysponują następującymi danymi:

A	wartość	1	0	1	0	1	1	0	0	1	1
	grupa	⊕	⊗	⊕	⊕	⊗	⊗	⊕	⊗	⊕	⊗
B	grupa	⊕	⊗	⊗	⊗	⊗	⊕	⊕	⊗	⊕	⊕
	wynik pomiaru	1	0	0|1	0|1	1	0|1	0	0	1	0|1

Zauważmy, że wartości logiczne zgadzają się wszędzie tam, gdzie grupa wylosowana podczas detekcji przez osobę B zgadza się z grupą wylosowaną przez osobę A podczas wysyłania. Gdy natomiast osoba B źle wylosowała swoją grupę, wtedy w wyniku pomiaru mogła dostać z równym prawdopodobieństwem wartość 0 lub 1 i tym samym w co drugim przypadku (nie wiadomo, którym) różni się od wartości, jakie ma osoba A. Przychodzi zatem czas na ostatni, bardo zaskakujący krok całej procedury.

Osoba A znów przeprowadza rozmowę z osobą B przez zwykły telefon, który może być podsłuchiwany. Podczas tej rozmowy przekazuje jej grupy, do których należały kolejno wysyłane fotony. Osoba B robi dokładnie to samo w stosunku do osoby A. Opisuje jej swoje grupy, które wylosowała dla kolejno przylatujących fotonów. Krótko mówiąc, osoby A i B porównują swoje grupy i usuwają te kolumny ze swoich tabel, których grupy do siebie nie pasują. W wyniku tej procedury pozostają im następujące dane:

A	wartość	1	0	1	0	1	1	0	0	1	1
	grupa	⊕	⊗	⊕	⊕	⊗	⊗	⊕	⊗	⊕	⊗
B	grupa	⊕	⊗	⊗	⊗	⊗	⊕	⊕	⊗	⊕	⊕
	wynik pomiaru	1	0	0|1	0|1	1	0|1	0	0	1	0|1

Jak widać, osoby A i B dysponują tym samym ciągiem liczb 1 0 1 0 0 1. Ciąg ten jest całkowicie tajny i tym samym może być użyty jako klucz kryptograficzny. Jest on naprawdę tajny. Nigdy bowiem osoby A i B ani słowa nie powiedziały o tych liczbach. Nigdy też osoba A nie zdradziła, jakie fotony wysyłała. Jedyne, co zostało zdradzone, to grupy, do jakich należały wysyłane fotony. To natomiast, jak już powiedzieliśmy wcześniej, nie wystarcza, aby powiedzieć, jaką wartość logiczną one reprezentowały.

No dobrze. Rzeczywiście w wyniku nakreślonej tu procedury osoby A i B dysponują tym samym ciągiem liczb, którego nigdy nie wypowiedziały. Ale jest mały problem. Przecież jest całkiem możliwe, że jakaś osoba C, oprócz tego, że podsłuchiwała rozmowę, to jeszcze majstrowała coś przy światłowodzie, którym leciały fotony. Mogła np. sprawdzić, jaki to foton leci, albo, co gorsza, skopiować go jakoś i przesłać do swojego laboratorium. Być może wtedy, wykorzystując tak skradzione fotony oraz informacje z podsłuchanych rozmów, mogłaby również odtworzyć tajny klucz. Mam dobrą wiadomość! Zabraniają tego prawa mechaniki kwantowej. Ale o tym już następnym razem... ●

Osoba C majstruje przy światłowodzie