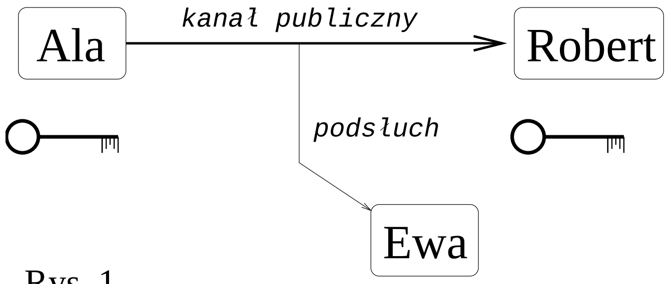
Kryptografia kwantowa

Wojciech Broniowski
Instytut Fizyki Jądrowej im. H. Niewodniczańskiego

Czy można komunikować sie na odległość w sposób całkowicie bezpieczny, niemożliwy do podsłuchania? Okazuje się, że tak, dzięki podstawowym prawom fizyki mikroświata!

Kryptografia (gr. kryptos - ukryty) to sztuka zapisywania informacji w taki sposob, aby była ona zrozumiała tylko dla wtajemniczonego odbiorcy, posiadającego umówiony *klucz*. Sztuka ta jest zapewnie równie stara jak samo pismo i na przestrzeni dziejów zajmowała poczesne miejsce. Używali szyfrów starożytni dowódcy i władcy, królowie i papieże, Rosenbergowie i Ché Guevara. Kodowane są rozmowy płynące "czerwoną" linią między Białym Domem i Kremlem, przekazy pieniężne między bankami, czy numery kart kredytowych podczas elektronicznych zakupów w Internecie.



Rys. 1

Rys. 1 ukazuje podstawowe zagadnienie kryptologii: Ala przekazuje informację do Roberta, posługując sie tzw. kanałem publicznym (telefon, radio, list nadany pocztą). Informacja Ali jest zaszyfrowana z pomocą klucza. Ten sam klucz służy Robertowi do jej odszyfrowania. Kanał publiczny jest z definicji narażony na podsłuch przez kryptoanalityka Ewę, która nie znając klucza stara się złamać szyfr. Ramki I i II przedstawiają dwa przykłady kodowania: prościutki *szyfr Cezara*, oraz szyfr *bloczka jednorazowego*, dla którego dowiedziono, że jest nie do złamania!

Kwantowość z tytułu tego artykułu nie ma nic wspólnego z kryptologią samą w sobie. Jak zobaczymy za chwilę, jest ona przydatna zanim Ala i Robert mogą zacząć się komunikować. Otóż we wszystkich schematach kryptologicznych niezbędne jest, by początkowo Ala i Robert posiedli wspólną tajemnicę. Dawniej tajemnicą okrywano samą metodę kodowania. Dziś używanych jest kilka powszechnie znanych metod, a tajemnicę stanowi klucz. W naszych przykładach jest to liczba N dla szyfru Cezara, lub bloczek jednorazowy z wypełnionymi środkowymi wierszami.

Szyfr Cezara **I**

Jest to najprostszy szyfr transpozycyjny, w którym każda litera tekstu jest zastępowana przez następującą po niej N miejsc dalej w alfabecie. Juliusz Cezar używał $N = 3$: $A \to D$, $B \to E$, $C \to F$, ..., $Z \to C$ (FOTON → IRXRQ). W starożytnosci taka metoda mogła uchodzić za bezpieczną, ale też niewielu ludzi w ogóle umiało czytać! Uzbrojeni w komputery kryptoanalitycy mogą złamać szyfry transpozycyjo-permutacyjne (z przesunieciami, jak w szyfrze Cezara, i dodatkowo z przestawieniami) w mgnieniu oka.

Aby przekazać sobie klucz w sposób bezpieczny, Ala i Robert nie mogą użyć konwencjonalnego kanału publicznego, jak np. radio, bo narażają się wtedy na podsłuch. Zdobywszy klucz, Ewa może następnie bez trudu rozszyfrować ich dalszą korespondencję. A zatem pojawia się problem praktyczny bezpiecznego przekazania klucza. Ewa i Robert mogą się w tym celu spotkać w ustronnym miejscu, lub użyć zaufanych posłańców. Ale co będzie jeśli posłaniec dostanie się w ręce wroga? Szczególnie dla metody bloczka jednorazowego przekazanie klucza, a także jego przechowywanie, jest uciążliwe, gdyż klucz jest równie długi jak szyfrowana nim później informacja.

Bloczek jednorazowy — II

Szyfr, dla którego udowodnino, że jest nie do złamania, to tzw. *bloczek jednorazowy* (ang. one-time pad). Nazwa pochodzi od bloczka z kartkami, na których sporządza sie kryptogram. Każdą kartkę można użyć tylko jeden raz i po wykorzystaniu oddziera się ją i wyrzuca. Ala i Robert najpierw przygotowują swoje bloczki, dzieląc kartki na trzyliniowe wiersze, i wpisując losowo wygenerowany ciąg liczb w środkowe linie. To jest ich wspólny klucz. Posługujemy się tu dla prostoty zapisem binarnym. Przygowując kryptogram Ala wpisuje swą informację w górną linię, dodaje modulo 2 liczby z górnej i środkowej linii (0+0 mod 2 = 0, 1+0 mod 2 = 1, 1+1 mod 2 = 0) i zapisuje wynik w linii dolnej. Zawartość dolnej linii (kryptogram) przekazywana jest kanałem publicznym do Roberta, który wpisuje ją do górnej linii swojego bloczka, odejmuje modulo 2 środkową linię i w wyniku dostaje informację Ali w linii dolnej.

Ala

informacja	011100010101011001010
klucz	100101000100100101001
kryptogram	111001010001111100011
informacja	010010101001101001101
klucz	100100110011100101000
kryptogram	110110011010001100101
	itd.

Robert

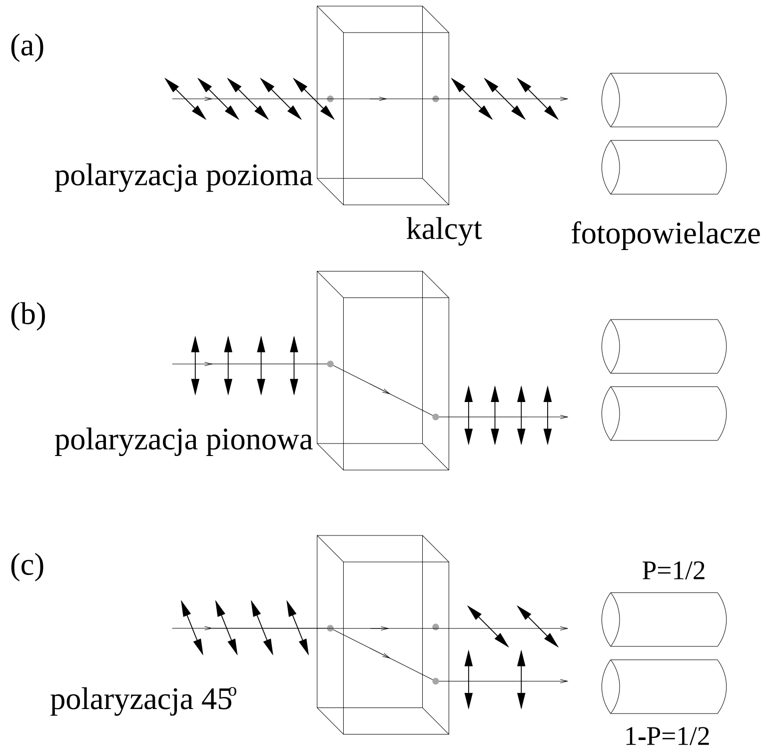
kryptogram	111001010001111100011
klucz	100101000100100101001
informacja	011100010101011001010
kryptogram	110110011010001100101
klucz	100100110011100101000
informacja	010010101001101001101
	itd.

Metodę bloczka jednorazowego wymyslili ok. 1917 r. Gilbert S. Vernam oraz Joseph O. Mauborgne. W latach czterdziestych twórca teorii informacji, matematyk amerykański Claude E. Shannon dowiódł, że szyfr ten jest nie do złamania jeśli klucz jest równie długi jak informacja, jest całkowicie przypadkowy, oraz użyty tylko raz.

Jak zrozumieć, że szyfr ten jest nie do złamania bez lektury prac Shannona? Wyobraźmy sobie najpierw, że Ewa usiłuje złamać szyfr Cezara, w którym przesunięto litery o N miejsc. N pełni tu rolę klucza, i oczywiście Ewa go nie zna. Przechwyciwszy kryptogram, próbuje kolejno różnych N, których może być tyle, ile liter alfabetu minus 1 (dla alfabetu łacińskiego 25). Ewa wygeneruje w ten sposób 25 różnych tekstów. Jeśli informacja jest dostatecznie długa, bez trudu stwierdzi, który tekst ma sens i w ten sposób złamie szyfr. W przypadku bloczka jednorazowego Ewa, zgadując wszystkie możliwe klucze (których jest aż 2^n, gdzie n jest liczba cyfr w kryptogramie) wygeneruje wszystkie możliwe informacje długości n bitów! Rzecz jasna, nie sposób rozstrzygnąć, który przypadek jest informacją wysłaną przez Alę, zatem szyfr jest nie do złamania. Zauważmy, że jego bezpieczeństwo wynika z długości klucza.

W jaki sposób Ala i Robert mogą się bezpiecznie "wymienić" kluczem na odległość? Umożliwia to właśnie *kryptografia kwantowa*, która właściwie powinna się nazywać *kwantowym generowaniem klucza*. Ideę tę rozwinęli, począwszy od lat siedemdziesiątych, Stephen J. Wiesner, Charles H. Benett, Gilles Brasard i Artur Ekert (który ukończył fizykę na Uniwersytecie Jagiellońskim). Do zrozumienia tego mechanizmu potrzebne nam będzie najpierw zrozumienie natury pomiaru w mechanice kwantowej (oczywiście bez znajomości samej mechaniki kwantowej!)

Z punktu widzenia fizyki, każde podsłuchiwanie jest pomiarem. "Pajęczarz" mierzy napięcie w sieci telefonicznej, posiadacz skanera mierzy częstotliwość fal radiowych w danym paśmie, itd. W świecie makroskopowym, z którym spotykamy się na co dzień, pomiar jest pasywny, tzn. nie zmienia stanu mierzonego układu. Pomiar długości stołu linijką nie zmienia jego długości, czytanie korespondencji pod światło nie zmienia zawartości listu. Te oczywiste, zdawałoby się, stwierdzenia, nie są prawdziwe w świecie mikroskopowym, czyli kwantowym. W świecie mikroczastek pomiar jest *aktywny*, tzn. zmienia stan badanego układu. Właśnie w tej aktywności pomiaru leży szansa pokonania Ewy!



Rys. 2

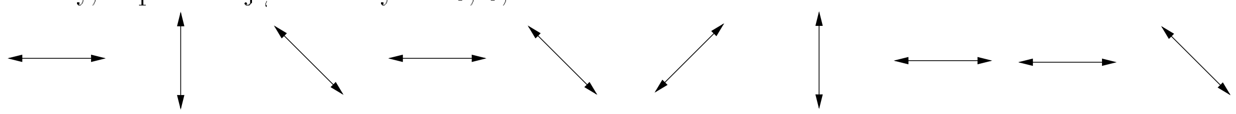
Ala i Robert będą poslugiwać się *fotonami*. Są to najmniejsze możliwe porcje, czyli *kwanty* światła. Foton jest falą elektromagnetyczną, w której pole elektryczne i magnetyczne drgają prostopadłe do siebie i do kierunku rozchodzenia się fali. Kierunek drgania pola elektrycznego nazywamy *polaryzacją*. Zwykłe światło składa się z wielu fotonów o różnych polaryzacjach. Fizycy, np. przy pomocy laserów, potrafią emitować pojedyncze fotony, a także polaryzować je przepuszczając przez odpowiednie filtry.

Tak właśnie postępuje Ala, posyłając do Roberta pojedyncze spolaryzowane fotony. Obracając swoim polaryzatorem może dowolnie zmieniać kierunek polaryzacji każdego fotonu. Robert posiada *analizator*, którym bada polaryzację przychodzących fotonów. Może w tym celu użyć kryształu kalcytu, który ma właściwość *dwójłomności*, tzn. współczynnik załamania w tym krysztale zależy od kierunku polaryzacji światła. Przy odpowiednim ustawieniu analizatora, foton spolaryzowany poziomo nie ulega odchyleniu (rys. 2 (a)) i jest rejestrowany przez górny fotopowielacz (urządzenie zamieniające światło na impuls elektryczny). Natomiast foton spolaryzowany pionowo odchyla się jak na rys. (b) i wpada do dolnego fotopowielacza. Ustawienie analizatora z rys. 2 (a) i (b) możemy nazwać “zgodnym”. W obu tych przypadkach pomiar jest całkowicie przewidywalny — zmierzona polaryzacja odpowiada polaryzacji fotonu przed pomiarem.

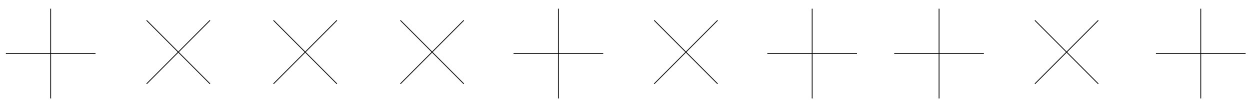
A co się stanie, jeśli foton jest spolaryzowany ukośnie, jak na rys. 2 (c)? Foton nie może się rozdzielić i wpaść do obu fotopowielaczy, gdyż jest on najmniejszą możliwą, niepodzielną porcją światła. Przy pomiarze “zdecyduje się”, czy wybrać górną, czy dolną drogę, i zostanie zarejestrowany przez jeden z fotopowielaczy. Innej możliwości nie ma! Mechanika kwantowa mówi nam, że trafi do górnego fotopowielacza z prawdopodobieństwem $P = cos^2\alpha$, gdzie α jest kątem polaryzacji względem kierunku poziomego, a do dolnego z prawdopodobieństwem $1 - P = sin^2\alpha$. Np. dla kąta 45^o obydwa prawdopodobieństwa wynoszą 1/2, jak na rys. 2 (c). Mierząc w opisany sposób polaryzację fotonu, możemy “na 100 %” stwierdzić, jaka była jego polaryzacja tylko w przypadku “zgodnego” ustawienia analizatora, jak na rys. 2 (a) i (b). Jeśli

Kwantowa generacja klucza III

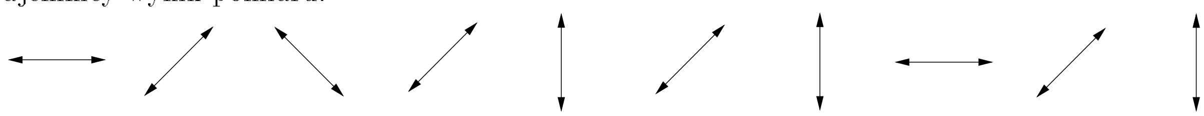
Korzystając z kanału kwantowego (np. światłowodu) Ala posyłą Robertowi pojedyncze fotony, których polaryzacja jest wybrana losowo spośród czterech możliwości: 0, 45, 90 i 135^o. Według umowy, odpowiadające im bity to: 0, 0, 1 i 1.



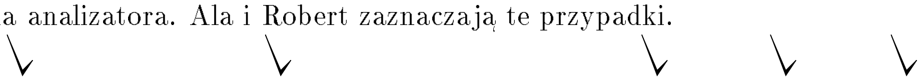
Robert mierzy kolejno polaryzację każdego fotonu, ustawiając losowo swój analizator albo pionowo, jak na rys. 2, albo przekręcając go o 45^o.



Oto przykładowy wynik pomiaru Roberta. Polaryzacja pierwszego fotonu musiała być zarejestrowana jako pozioma — jest to sytuacja z rys. 2 (a). Dla drugiego fotonu polaryzacja mogła zostać zarejestrowana jako 45^o, jak narysowano poniżej, lub 135^o, oba przypadki z prawdopodobieństwem 1/2 (porównaj rys. 2 (c)). Dla trzeciego fotonu wynik musi być 135^o, itd. Robert zachowuje w tajemnicy wynik pomiaru.



Po zakończeniu rejestracji wszystkich fotonów Robert, używając kanału publicznego, mówi Ali jaka była sekwencja ustawień analizatora. Ala, również kanałem publicznym, odpowiada, w którym przypadku polaryzacja fotonu była “zgodna”, tzn. równoległa lub prostopadła do kierunku ustawienia analizatora. Ala i Robert zaznaczają te przypadki.



Zgodnie z umową, Ala i Robert przyporządkowują polaryzacji poziomej bit 0, pionowej bit 1, pod kątem 45^o bit 0 i pod kątem 135^o bit 1. Uzyskana sekwencja stanowi ich klucz.

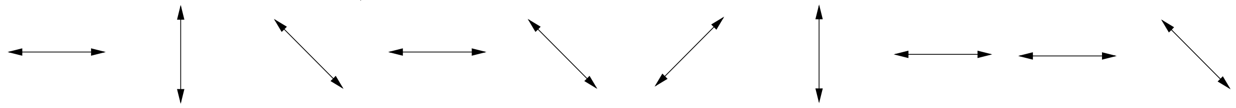
0 1 0 1 0

nie wiemy, czy ustawienie jest zgodne, to możemy jedynie mieć pewność, że jeśli foton został zarejestrowany przez np. górny fotopowielacz, to nie był on spolaryzowany pionowo. Mógł on natomiast być spolaryzowany poziomo, jak też ukośnie pod dowolnym kątem. Widzimy zatem, że pomiar kwantowomechaniczny dostarcza jedynie *ograniczonej* informacji o stanie układu. Przypadek z rys. 2 (c) uwidacznia również wspomnianą *aktywność* pomiaru kwantowego. W trakcie pomiaru polaryzacji ukośnej, otrzymujemy z prawdopodobieństwem 1/2 polaryzację poziomą, i z tym samym prawdopodobieństwem polaryzację pionową. Widzimy, że pomiar "obraca" polaryzację ukośną.

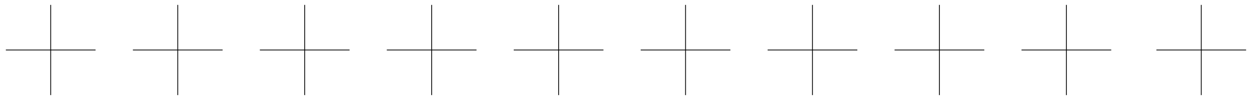
Możemy teraz przystąpić do przedstawienia tzw. kwantowego protokołu generowania klucza kryptograficznego. Metoda opisana w ramkach III pochodzi od Benetta i Brasarda. Ala i Robert, oprócz zwykłego kanału publicznego, muszą posiadać *kanał kwantowy*, np. światłowód.

Podsłuchująca Ewa — IV

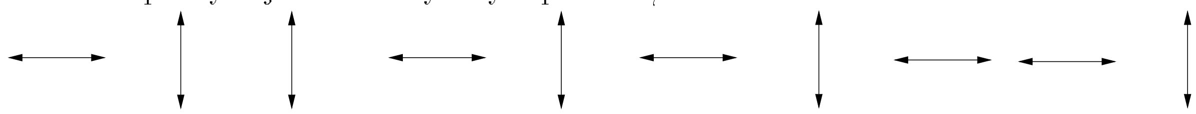
Jak w ramce III, Ala wysyłą fotony do Roberta.



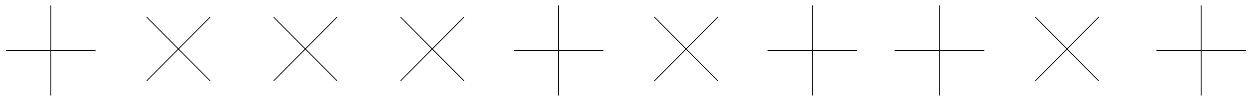
Ewa przecięła światłowód, jedną nitkę dopięła do swojego analizatora, a drugą będzie posyłać dalej fotony tak, aby Ala i Robert nie zorientowali się, że łączność została zerwana. Dla prostoty, zakładamy, że Ewa nie zmienia ustawienia swojego analizatora, i jest on ustawiony pionowo.



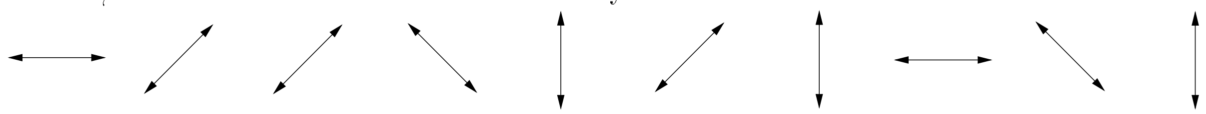
Oto przykład pomiaru Ewy. Zmierzywszy dany foton, Ewa generuje foton z taką jak zmierzona polaryzacją i posyła go Robertowi. Niektóre polaryzacje (np. trzeci foton) mogą być obrócone w stosunku do polaryzacji fotonów wysłanych przez Alę.



Robert mierzy polaryzację.



Oto możliwy wynik jego pomiarów. Dla trzeciego fotonu polaryzacja jest prostopadła do wysłanej przez Alę! To właśnie rezultat "działalności" Ewy.



Jak uprzednio, Robert uzgadnia z Alą, które ustawienie osi było "zgodne".

Ala przyporządkowuje tym przypadkom następujący ciąg bitow:

0 1 0 1 0

Ciąg bitów Roberta różni się w drugiej cyfrze od ciągu Ali. To przekłamanie jest wynikiem podsłuchiwania. Statystycznie, zdaży się to w co czwartym bicie.

0 0 0 1 0

Tym kanałem, który jest również narażony na podsłuch Ewy, Ala posyła Robertowi pojedyncze fotony. Procedura wymaga kilku kroków, co opisane jest szczegółowo w ramkach III. W efekcie Ala i Robert stają się szczęśliwymi posiadaczami klucza.

Ci, którzy przebrną przez tekst w ramkach III zapewne zadadzą pytanie: Po co ta skomplikowana procedura? Otóż okazuje się (ramki IV), że taki kwantowy protokół pozwala Ali i Robertowi stwierdzić, czy podczas generowania klucza Ewa podsłuchiwała, czy nie. Podsłuchiwanie jest bowiem pomiarem kwantowym, jest "aktywne", i w rezultacie transmisja Ali do Roberta zawiera przekłamania (patrz ramki IV). Aby stwierdzić, czy Ewa podsłuchiwała, czy nie, Ala i Robert poświęcają kawałek (np. 10%) świeżo wygenerowanego klucza. Przekazują go sobie zwykłym kanałem publicznym, i porównują. Jeśli przekłamania są na poziomie 1/4 przypadków, więdzą, że Ewa podsłuchiwała. Wyrzucają wówczas klucz, i rozpoczynają cały protokół od nowa. Jeśli nie ma przekłamań, to znaczy że Ewa nie podsłuchiwała, i klucz jest bezpieczny. Przytoczony w ramkach IV przykład analizy kryptologicznej można uogólnić. Okazuje się, że cokolwiek by Ewa nie robiła, nie jest w stanie podsłuchać pasywnie transmisji kwantowej. Wymagałoby to bowiem złamania praw mechaniki kwantowej!

W roku 1989 naukowcy z IBM skonstruowali prototypowe urządzenie, realizujące protokół Benetta i Brasarda. Obecnie, stosując światłowody i spolaryzowane fotony, można komunikować się kwantowo na odległość 1 km. Przy użyciu nieco innej niż opisana tutaj metody można zwiększyć zasięg do 10 km, przy częstości generacji klucza 20000 bitów na sekundę. Ograniczenia odległości i częstości wynikają z technicznych własności stosowanych urządzeń (szumy, tłumienie sygnału, wydajność detektorów). Przy obecnej technologii możliwe jest zwiększenie zasięgu do ok. 50 km. Niestety, niemożliwe jest zastosowanie przekaźników, by móc zwiększyć tę odległość. Wzmacnianie to pomiar i reemisja, co musi prowadzić do przekłamań (ramki IV).

Gdzie może być przydatna kryptografia kwantowa? Wyobrażalne zastosowania to komunikacja między agencjami rządowymi czy bankami w obrębie jednego miasta. Oczywiście całą sprawą interesuje się wojsko, agencje wywiadowcze i firmy telekomunikacyjne, które finansują wspomniane eksperymenty. Czas pokaże, czy rzeczywiście kryptografia kwantowa będzie stosowana w praktyce, czy też odejdzie do lamusa ciekawostek i do zbiorów zadań dla studentów fizyki. Na razie pozostaje intrygującą możliwością całkowicie odpornej na podsłuch komunikacji, zapewnionej przez jedno z podstawowych praw Przyrody.

Na koniec wymieńmy jeszcze jednym tchem inne niekonwencjonalne zastosowania zasad mechaniki kwantowej: komputery kwantowe, teleportacja kwantowa, niepodrabialne kwantowe pieniądze. W odróżnieniu od kryptografii kwantowej, nie ma jeszcze prototypów realizujących fizycznie te pomysły, ale badania, zwłaszcza nad niezwykle potężnymi komputerami kwantowymi, są bardzo intensywne.

Literatura:

1. C. H. Benett, G. Brasard, A. Ekert, *Kryptografia kwantowa*, Świat Nauki nr 12, grudzień 1992, str. 28, oraz cytowana tam literatura.

2. Zobacz też stronę domową kryptogafii kwantowej w Oxfordzie, http://eve.physics.ox.ac.uk/QChome.html