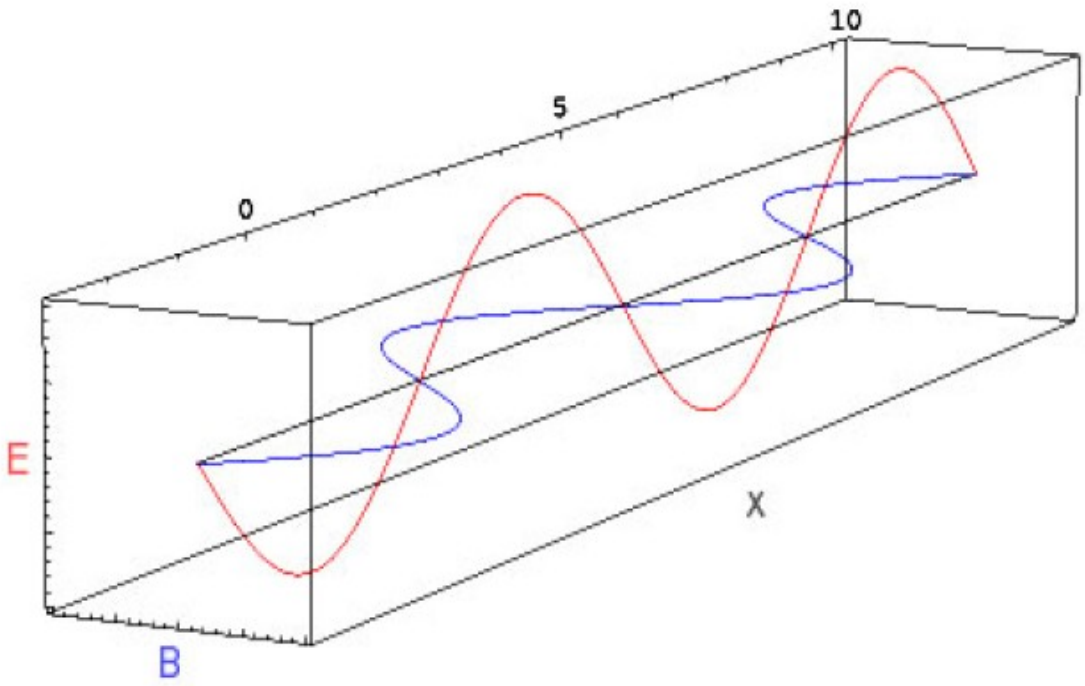
PORADNIKI

Kryptografia Kwantowa

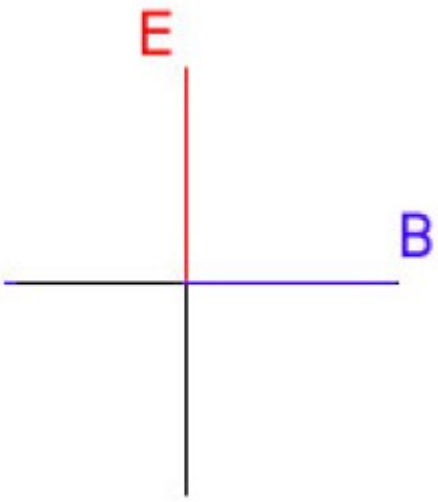
Witam, zacznijmy od podstaw teorii kwantowej. Najpierw, wyjaśnię termin "kwant". Bardziej uważny obserwator może zauważyć ,że relatywnie blisko słowa kwant (quantum) jest słowo ilość (quantity). Na początku XX wieku fizycy zauważyli ,że coś nie tak jest z klasyczną teorią, precyzyjniej, zauważyli ,że ich punkt widzenia na podstawowe cząsteczki nie bardzo pasuje do wyników eksperymentów jakie uzyskali.Logicznym wnioskiem było to ,że coś nie tak jest z kalsycznym podejściem do atomu. W związku z tym, Ma Planck wprowadził nowe podejście do tej sprawy. W klasycznej fizyce, elektron orbituje (orbitowanie wokół również jest pojęciem względnym) wokół jądra lub atom mógł mieć możliwą energię, i co z tym związane, mógł orbitować wokół jądra na dowolnie możliwym dystansie. Problem z tą wizją był taki ponieważ elektron jest naładowany ujemnie a jądro, ponieważ składa się z dodatnich protonów i neutralnych neutronów, było naładowane dodatnio, oczekiwano ,że elektron będzie zbliżał się do jądra około 0.0000000001 sec(z powodu różnej biegunowości, jądro przyciąga elektron). Odpowiedź była taka ,że elektron nie ma żadnej energii podczas orbitowania wokół jądra, energia elektronu jest kwantowana. Oznacza to ,że elektron ma wyraźnie zdefiniowane poziomy energii, i może orbitować tylko w pewnych odległościach od atomu. Bardziej precyzyjnie, nie jest dokładnie prawdą, że elktron nie orbituje dokładnie wokół orbit, orbity są tylko definicją miejsca gdzie jest najlepsza możliwość znalezienia elektronu. Zmieszany? Możesz być przynajmniej.... lekko zszokowany jeśli nigdy nie szłyszałeś o tym. Prowadzi nas to do mylącegi i paradoksalnego świata mechaniki kwantowej (mechanika kwantowa – jedna z części fizyki zajmująca się zjawiskam małego świata, szczególnie badania ruchu cząsteczek, równolegle do mechaniki klasycznej, ale dużo szerzej) W świecie mechaniki kwantowej nie mówimy o dokładnych wartościach, ale o wartościach możliwych. Aby wyrazić to jaśniej, powiedzmy ,że chcemy znaleźć miejsce gdzie jest cząstka jaką jesteś szczególnie zainteresowany, nie będziesz mógł znaleźć dokładnego miejsca i powiedzieć jest tu, będziesz się czuł jak bóbr który miał wypadek samochodowy ... jedna stosunkowowo szeroka plama na środku. Ten środek to miejsce gdzie jest największa możliwość znalezienia cząstki, ale nie koniecznie jest to miejsce gdzie cząsteczka jest rzeczywiście. Jest to konsekwencja naszej niemożności dokonania dokładnych pomiarów. W naszym świecie "dużych" obiektów, pomiary są wyjątkowo dokładne aby powiedzieć ,że "bóbr miał 1,5 m długości (hmmmm ...duży bóbr), ale jeśli spojrzeć dokładniej 1,5 to może być 1,485755432m albo 1,49532221 m albo 1,5000000 m. Zawsze mamy błąd pomiarowy. W świecie małych obiektów, pomiary są tak wrażliwe ,że nie można na przykład zmierzyć pozycji i impulsu (impuls jest iloczynem masy i prędkości, określa ruch) cząstki, co jest jedną z podstaw mechaniki kwantowej. Duże znaczenie ma zrozumienie ,że fizyka oparta jest na pomiarach, nie na teorii. Więc przejdźmy do konkluzji... Mechanika kwantowa zajmuje się "małym" światem atomów i cząstek podstawowych, podczas gdy fizyka klasyczna, od Isaaca Newtona zajmuje się "dużym" światem bobrów... W świecie kwantów wszystko co da się zaobserwować (rzeczy jakie możemy zmierzyć) mają wartości dyskretne (co oznacza ,że nie mamy żadnej dającej się zaobserwować wartości, na przykład, elektron nie może mieć energii podczas orbitowania wokół jądra), i możemy mówić tylko o prawdopodobieństwie rzeczywistych zdarzeń... jest dużo więcej zasad, ale te są jednymi z podstawowych.

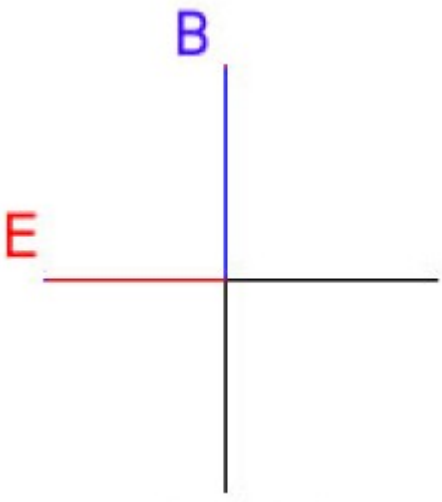
Teraz, kiedy przeszedłeś podstawy mechanik kwantowej, nie poddawaj się.Muszęwyjaśnić ci pewne fakty o również o świetle zanim przejdziemy dalej. Sednem sprawy jest to ,że jest zbudowane z mniejszych części. Najmniejsze z nich jakie znamy a które budują wszystkie większe konstrukcje natury, jak atomy i molekuły nazywamy *cząstkami*. To co odkryli fizycy to fakt, że cząstki nie są cząstkami ale są również falami. Mam dla ciebie jeszcze jedną iluzję. Cząsteczki nie wyglądają jak piłeczki, wrzeczywistości nie można powiedzieć ,że cząsteczki mają jakikolwiek kształt. Jeśli ktoś pokazał ci zdjęcie czarnej zamazanej piłeczki i powiedział ci "to jest zdjęcie elektronu", prawdopodobnie pokazał ci zdjęcie rozkładu energii elektronu.Co chcę wskazać? W 'kryptografii kwantowej' główną rolę odgrywa światło, więc muszę powiedzieć coś o świetle i terminach takich jak *polaryzacja* i *przesunięcie fazowe*. Wyjaśnię konstrukcję falowo – cząsteczkową. Prawdopodobnie słyszałeś o fotonów i o falach elektromagnetycznych. Zobacz zwykły obraz fali elektromagnetycznej (E - pole elektryczne, B - pole magnetyczne, x - kierunek

podróży światła)



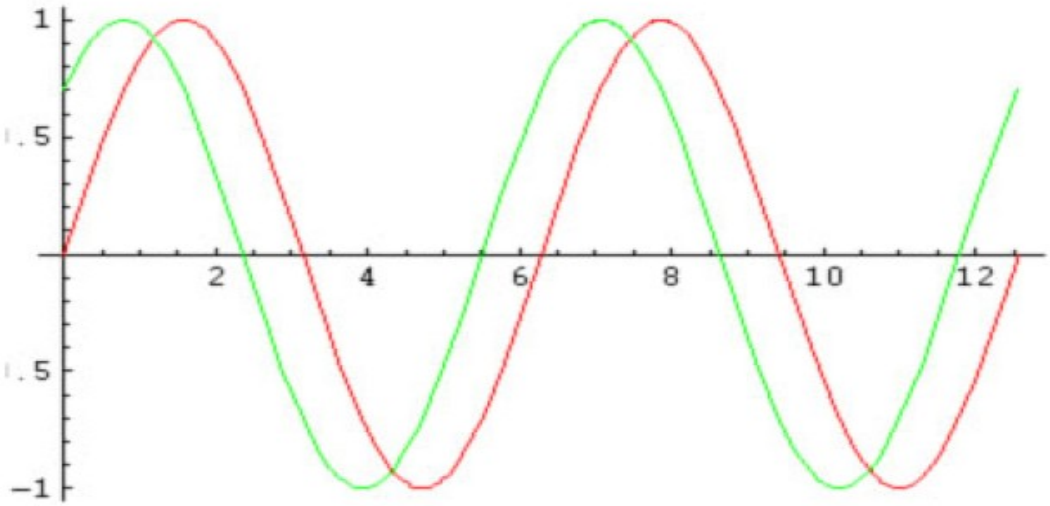
Cóż, są dwa spojrzenia na tą samą sprawę tycząca światła. Światło ma bardzo złe maniery, mogę powiedzieć ,że światło działa trochę schizofrenicznie. Określa miarę jaką bierzemy, może zobaczyć ,że światło zachowuje się jak fala elektromagnetyczna, lub ,że światło jest złożone z cząstek ,które nazywamy fotonami. Nie jest to tak jak z wodą, gdzie mamy dużą ilość cząsteczek , które oddziaływują na siebie i tworzy fale jakie widzimy. Wynika to z charakteru organizacji natury którą nazywamy dualnością. Zatrzymam się tu, aby nie wgłębiać się w ten temat.
Teraz wyjaśnię terminy polaryzacja i przesunięcie fazowe. Widzisz oś x? Przedstawiona jest jako długa czarna linia w środku grafiki. Cóż, dlaczego nie można obrócić pozostałych dwóch osi wokół niej? Nie ma żadnego powodu aby nie można było obrócić całego obrazka wokół tej osi. Przypuśćmy ,że mamy dwie fale o tej samej długości (och, jest to jeden ze smaków światła, w rzeczywistości jest to wartość, która określa energię fali, a wartość ta określa czy jest to fala radiowa, zwykłe światło widzialne, promień x, gamma itp) i niech podążają tą samą ścieżką x. Ale co z pozostałymi dwoma osiami E i B? Jedna fala musi mieć osie E i B pod stałym kątem 90 stopni. (później zobaczysz wyrażenia takie jak Pi, Pi/2, które są innym sposobem do oznaczania kątów, Pi = 180 stopni, tak ,że samo Pi = 3.14.. Ok, teraz wiesz,że mozesz obrócić te dwie osie E i B wokół osi x a co możesz zrobić z nią? Jeśli na przykład weźmiemy dowolne pozycje wektorów E i B, to niech to będzie pozycja osi jaką możesz zobaczyć na poniższym rysunku:





Rysunek 1 Rysunek 2

Jeśli mamy pozycję wektorów E i B taką jak na Rysunku 1, jako arbitralne (polaryzacja nie jest definitywny terminem, nie jest to istniejąca absolutna pozycja wektorów E i B ale musisz najpierw zdefiniować arbitralne pozycje wektorów E i B a potem rozważyć termin polaryzacja), możesz zobaczyć czy wygląda choć trochę podobnie do Rysunku 2, któych wektory są obrócone o 90 stopni przeciwnie do ruchu wskazówek zegara (lub możesz powiedzieć ,że są obrócone o Pi/2) Teraz w końcu możemy zdefiniować termin polaryzacja. Możesz powiedzieć ,że fala elektromagnetyczna na rysunku 2 jest spolaryzowana o 90 stopni (oczywiście, w porównaniu z naszą arbitralną polaryzacją na Rysunku 1). Nawet jeden foron, jeśli rozpatrujemy go jakostronę cząsteczki światła, może być spolaryzowany, dlaczego? Ponieważ, jak mówiłem wcześniej, światło jest i cząsteczką jak i falą ,a jeden foton może być rozważany również jako fala, i możesz również powiedzieć ,że foton jest spolaryzowany pod tym samym kątem. Jeśli używasz jakiegoś źródła światła, takiego jak żarówka, masz falę elektromagnetyczną o wszystkich możliwych kątach polaryzacji. Możesz uzyskać światło o szczególnej polaryzacji pod tym samym kątem z urządzenia zwanego polryzatorem. Teraz pozostało nam wyjaśnienie terminy przesunięcie fazowe. Możesz zobaczyć na powyższym rysunku ,że funkcja opisująca falę elektormagnetyczną rzeczywiście wygląda jak fala. Jest to funkcja sinus, i możesz zobaczy ,ze jest funkcją okresową. Teraz powiem ci ,że okres tej funkcji to 360 stopni lub 2Pi. "Okresowy" oznacza ,że funkcja powtarza swój obraz po jakiejś wartości x. Spójrz:

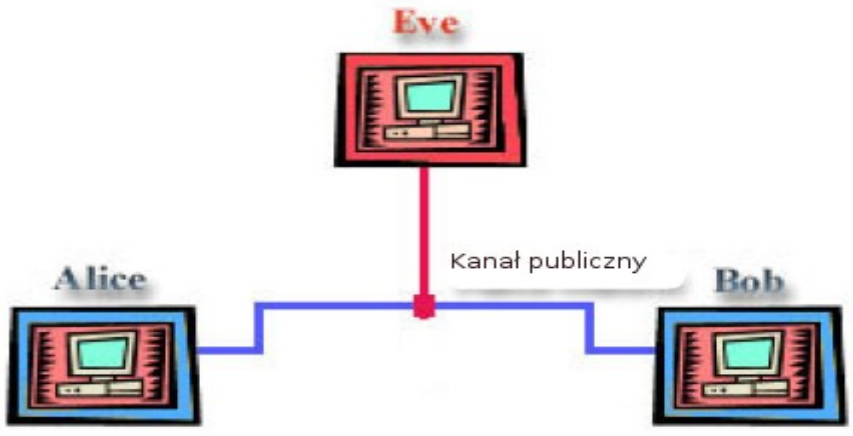


Widać ,że zielona i czerwona funkcja to takie same funkcje, ale przesuniętę na osi x.Aby być

bardziej precyzyjnym powiem ,że równanie dla funkcji czerwonej to Sin(x) a równanie dla funkcji zielonej to Sin(x+Pi/4). Mogę powiedzieć ,że funkcja zielona jest przesunięta fazowo o Pi/4 (45 stopni) wobec funckji czewrwonej. To samo się tyczy fali elektormagnetycznej ponieważ fala elektromagnetyczna jest opisywana funkcją sinus (tj. jednym ze sposobów opisu fali elektormagnetycznej)

Teraz keidy poznaliśmy fizyczne terminy do celów dlaszego wyjaśnienia, możemy przejść do podstawowego tematu czyli kryptografii kwantowej i jej zalet w porównaniu normalnej kryptografii. Nie będzie to omówienie samej kryptografii kwantowej ,ale wyjaśnienie jak jest dystrybuowana informacj. Głównym powodem dlaczego kryptografia kwantowa jest tak imponująca, jest to ,że jest tu używany jeden z fundamentów fizyki w bardzo praktyczny sposób. Zwróćmy teraz oczy na standardy systemów kryptograficznych, ponieważ są one fundamentami kryptografii kwantowej. Możemy zdefiniować kryptografię jako sztukę ukrywania informacji w łańcuchach bitów, które są niezrozumiałe dla strony nieautoryzowanej. Aby odnieśćsukces w naszym zadaniu ukrycia informacji, zazwyczaj używamy algorytmu połączenia komunikatu z jakąś dodatkową informacją, którą zazwyczaj nazwywamy kluczem tworząc razem kryptogram. Technika ta jest nazywana szyfrowaniem. Domyślam się , że wielu z was słyszało już tą historię ,ale wszystko musi być jasne, więc bądź cieprliwy a może zostaniesz nagrodzony. Recz o jakiej nie wiesz prawdopodobnie jeśli jesteś nowy w kryptografii i teorii informacji, jest to ,że osoba która szyfruje jest tradycyjnie nazywana Alice a osoba ,która odbiera wiadomość to tradycyjnie nazywany Bob (zwykle oznaczani jako A i B) Spójrz na rysunek

Tradycyjny trzeci element w tej historii jest nazywany Eve. To jest zło, Eve oznacza podsłuch (eavesdropper). Jak wskazuje nazwa jest tym który przechwytuje informacje jakie Alice wysyła do Boba. Eve jest nieuwierzytelnioną, nieżyczliwą osobą , jaką zwykle nazywamy crackerem. Spójrzmy na obrazek:



Teraz mamy kompletny obraz problemu z jakim się musimy zmierzyć. Kanał publiczny jest zwykle

kanałem używanym dla rozprowadzania informacji, takim jak linia telefoniczna, światłowód, internet itp. Dla każdego zabezpieczonego kryptosystemu, powinno być niemożliwe odblokowanie kryptogramu bez klucza Boba. W praktyce sprowadza się to do tego ,że system jest aksymalnie trudny do scrackowania. Główną ideą jest to,że komunikat powinien pozostać chroniony tak długo jak informacja zaawarta w wiadomości jest cenna (to wyjaśnia dlaczego na przykład DES jest do złamania) Kryptosystemy są dzielona na dwie główne klasy. Zależy to od tego czy klucz jest współdzielony w tajemnicy czy publicznie. Podam dwa przykłady, po jednym dla każdej grupy;"szyfr z kluczem jednorazowym" i RSA, obnażając ich jakość i ułomności.

Szyfr z kluczem jednorazowym kontra RSA w normalnej kryptografii

Szyfr z kluczem jednorazowym
Ten system został zaproponowany przez Gilberta Vernama z AT&T w 1935 roku, obejmujący podział klucza tajnego i jest jedynym kryptosystemem który dostarcza sprawdzonej, idealnej tajemnicy. W tym przypadku Alicja szyfruje komunikat używając losowo generowanego klucza a potem po prostu dodaje każdy bit tej wiadomości do odpowiedniego bitu klucza. Zakodowana wiadomość jest wysyłana do Boba, który ją deszyfruje przez odjęcie tego samego klucza.

Alicja

Wiadomość		**11001010**
Doany klucz	+	**01110010**
Zakodowany klucz	=	**00111100**

Transmisja

Bob

Zakodowany tekst		**00111100**
Odejmowany klucz	-	**01110010**
Wiadomość	=	**11001010**

Normalnie, zaszyfrowany tekst nie zawiera żadnej informacji dopóki używamy klucza. Mimo doskonałego zabezpieczenia, problem z tym systemem jest taki ,że jest niezbędne aby Alicja i Bob współdzielili wspólny tajny klucz, który musi być przynajmniej tak długi jak sama wiadomość. Może również użyć tego klucza dla pojedynczego szyfrowania (to wyjaśnia nazwa szyfr z kluczem jednorazowym), ponieważ jeśli będą używać tego klucza więcej niżraz, Eve może nagrać wszystkie zakodowane wiadomości i zacznie budować obraz tego klucza. Tu się zaczynają prawdziwe problemy. Jeśli chcą współdzielić ten sam klucz, muszą ten klucz transmitować przez jakiś zaufany kanał, taki jak kurier. Tu zaczyna się historia szpiegowska...itd. Sądzę ,że może być tu parę tysięcuy problemów począwszy od problemów uwierzytelnienia, drogich spotkań, podsłuchiwania itd. Dobre jest to ,ze Eve jeśli zechce sckrackować wiadomość, nie znając klucza, będzie musiała wyprówbować wiele kombinacji, bez żadnej pewności.

RSA (Rivest, Shamir, Adleman)
RSA należy do innej klasy kryptosystemów , tzw. kryptosystemów klucza publicznego. Pierwszy taki system stworzono w 1976 roku przez Whithfielda Diffie i Martina Hellmana na Uniwersytecie Stanforda. Użyli oni funkcji jednokierunkowej w której łatwo jest wyliczyć tą funkcję, na przykład f(x) (co zonacza, że mamy jakąś funkcję w zależności od zmiennej x) ale trudno jest wyliczyć w drugą stronę. Aby określić co oznacza "trudne do wyliczenia w drugą stronę" możemy wziąćczas jako współczynnik, dobry kryptosystem może być tym w którym upływający czas rośnie

wykładniczo wraz z liczbą bitów użytych do szyfrowania. Na przykład, możemy wziąść rozkład liczby na czynniki pierwsze. Pokaże ten sposób. 109*59 równa się 6431, ale zajęłoby zbyt wiele czasu odkrycie ,że czynniki pierwsze dla 6431 to 59 i 109. Jednakże, niektóre z tych funkcji jednokierunkowych mają coś takiego co nazywa się "zapadką", cooznacza ,że jest łatwy sposób obliczenia funkcji w różnych kierunkach z dodatkową informacją, w tym przypadku klucz lub hasło. Więc jeśli na przykład znasz ,ze jednym z czynników pierwszych 6431to 59, nietrudno jest obliczyć drugi czynnik pierwszy. RSA jest oparty na tej funkcji.Nie jest to silna teoria, że czas konieczny dla znalezienia czynników pierwszych liczby całkowitej i uzyskania klucza prywatnego rośnie wykładniczo z ilością bitów wejściowych. Może to być główna luka bezpieczeństwa jeśli ktoś odkryje ,że jest szybszy sposób obliczania czynników pierwszych, problemami stają się większe dzięki faktowi ,że wiekszość transakcji finansowych w zabezpieczonych systemach jest oparta o RSA. Nie sądź ,że odkryłeś sposób na faktoryzację liczb pierwszych i złamiesz serwery Wall Street w 10 minut (brzmi to jak idiotyczny opis hackerów jakie czasami zdarzają się w mediach) . Pokolenia matematyków (dużo mądrzejszych niż ty i ja) poświęciły swoją karierę temu zadaniu, a wszystko zaczeło się , jak sądzę, od Fermata do XIX wieku. Jeśli chcesz poświęcić swoje życie nauce, zapomnij o obrazie Alberta Einsteina rozwiązującego problem teorii względności w ciagu jednego długiego weekendu. OK? Hacking jest nauką i sztuką, jak matematyka lub fizyka (i programowanie oczywiście) i zajmuje wiele wiele czasu.

OK, co oznacza publiczny kryptosystem. Cóż, oznacza ,że z jednego klucza możesz stworzyć dwa klucze, publiczny i prywatny. Dla mnie wygląda to na dobry interes. Możesz współdzielić klucz publiczny z całym światem, i może on szyfrować nim wiadomości, ale keidy waidomość jest zaszyfrowana, odczytać ją może tylko właściciel klucza prywatnego. Również, kiedy wysyłasz wiadmość zaszyfrowaną kluczem prywatnym (trzymasz go tylko dla siebie, to ocznacza prywatny), ta wiadomość będzie odkodowana kluczem publicznym, ale klucz publiczny nie deszyfruje żadnej widomości , która nie jest zaszyfrowana kluczem prywatnym. To wyjaśnia termin podpis cyfrowy. Nie, nie możesz wyliczyc klucza prywatnego mając klucz publiczny, przynajmniej nie w jakimś rozsądnym czasie, zakładając ,że druga strona wybierze trudne hasło. Jesteśmy coraz bliżej tematu. Jest to jeden z wielu powodów (jest to najczęstszy powodó dla posiadania kryptografii kwantowej jako rozwiązania) dlaczego RSA może wydać się niepraktycznym w przyszłości. Są urządzenia,które tylko w teorii zwą się komputerami kwantowymi, które mogą faktoryzować liczby nie wykładniczo, a lineranie z liczbami bitów. Wyjaśnieniem jest przetwarzanie równoległe , które jest nawet bardziej równoległe niż istniejące obecnie.

Cóż jak możemy zobaczyć, publiczne kryptosystemy takie jak RSA staną się w przyszłości bezużyteczne, z pojawieniem się pierwszych użytecznych komputerów kwantowych. Masz jedne możliwy sposób, do tego najprostszy dla sekretnego wysyłania wiadomości.Zawsze możesz wrócić do systemów tajnego klucza, takie jak system Vernona, jeśli masz sposób doskonałego ukrycia tajnego klucza przed Eve. To jest dokładnie ten moment gdzie fizyka kwantowa wchodzi na scenę... Bob i Alicja muszą współdzielić tajny klucz (w przeciwieństwie do systemów klucza publicznego), a kryptografia kwantowa pozwala na dwie oddzielene fizycznie części do tworzenia losowego tajnego klucza bez uciekania się do usług kurierskich. Co lepsze ,pozwala im również na zweryfikowanie czy klucz nie został przejęty. Kryptografia kwantowa nie jest całkowicie nowym kryptosystemem, ale procedura dystrybucji klucza w doskonałej tajemnicy przed innym osobnikami, takimi jak Eve.. Krytpografia kwantowa nie jest algorytmem kryptograficznym, ale pozwala na bezpieczną dystrybucję klucza, a zatem jest naturalnym uzupełnieniem szyfru Vernona

Aby zrozumieć jak działa kryptografia kwantowa możemy spojrzeć na protokół komunikacyjny "BB84", który został wprowadzony w 1984 roku przez Charles'a Bennetta z IBM i Giles'a Brassarda z Unwersytetu w Montrealu. Alicja i Bob są połączeni kanałem kwantowym i klasycznym kanałem publicznym. Jeśli pojedyncze fotony są użyte do przenoszenia informacji kanałem kwantowym, jest to zazwyczaj światłowód. Kanał publiczny jednak, może być łączem komunikacyjnym, takim jak linia telefoniczna lub internet. Zastanówmy się trochę nad samą informacją. Taka informacja w świecie kmputerów jest przedstawiana szeregiem 0 i 1 które są łączone razem w określonym celu dla obecności informacji. Taka informacja może być wszystkim, liczbami, słowami, zdjęciami, musimy tylko wiedzieć jak zinterpretować tą informację binarną (binarna oznacza ,że informacja jest przedstawiana szeregiem 0 i 1...ale to wykracza trochę poza zakres tego tekstu.) Cóż ,takie 0 i 1 podczas podróży linią telefoniczną są przedstawiane przez jakiś poziom napięcia. Zazwyczaj, w świecie elektroniki cyfrowej logiczne 0 i 1 sąodpowiednio napięciami 0V i 5V (czasami -5V i 5V, a 0V przedstawiało jakiś inny stan). W przypadku kanału kwantowego przenoszone są fotony i jak można zobaczyć można użyć polaryzacji i przesunięcia fazowego. Możemy zdefiniować pewne arbitralne kąty polaryzacji lub przesunięcia fazowego. W praktyce, publiczne łącze jest również światłowodem, z oboma kanałami różniącymi się tylko intensywnością impulsów świetlnych. Jak to działa?

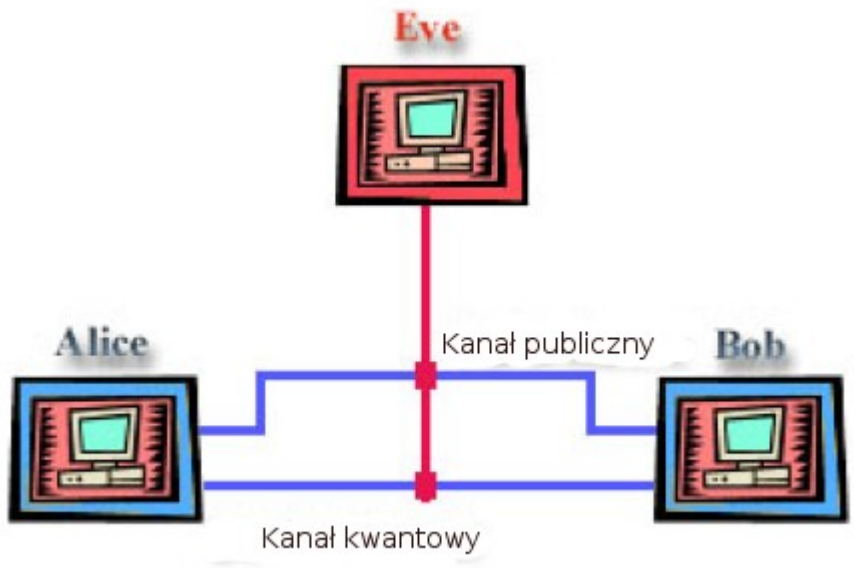
ALICJA BOB

Sekwencja bitów Alicji	1 0 1 1 0 0 1 1 0 0 1 1 1 0
Sekwencje analizatorów Boba	+ x + + x x + + x +x x + +
Pomiary Boba	1 0 0 1 0 0 1 1 0 0 0 1 0 0
Zatrzymana sekwencja bitów	1 - - 1 0 0 – 1 0 0 – 1 – 0

1) Po pierwsze Alicja ma cztery polaryzacje, które mogą transmitować spolaryzowane pojedyncze fotony poziomo, pionowo, pod kątem +45 stopni lub -45 stopni. Wysyła szerego fotonów kanałęm kwantowym, wybierając losowo jeden ze stanów polaryzacji dla każdego fotonu (który w tym przypadku przedstawia klucz, również zauważ na obrazku jaki kat polarzyacji przedstawia 0 a jaki 1, TO NIE POMYŁKA, TO JEST BARDZO WAŻNE aby

zrozumieć proces

2) Po drugie, Bob ma cztery analizatory, nie dwa (które są urządzeniami mogącymi analizować kąt polaryzacji, lub kilka kątów w danym czasie, ale zauważ ,że kiedy możesz umieścić analizator i jest pojedynczy foton, jeśli ustawisz analizator na jakiś kąt(y) będziesz mógł zobaczyć czy foton jest spolaryzowany pod tym kątem czy nie, również kiedy wykonujesz pomiar nie możesz zmierzyć polaryzacji tego samego fotonu ponwnie innym analizatorem ustawionym do pomiaru jakichś innych kątów, ponieważ kiedy mierzysz, informacja jest niszczona przez pomiar z powodu interakcji systemu pomiarowego i systemu jaki mierzysz, przedstawiany w fizyce jako teoria projekcji. Mówiłem już o mechanice kwantowej,innymi słowy , oznacza to ,że nie możesz zmierzyć WSZYSTKICH kątów od razu. Jeden analizator pozwala Bobowi rozróżniać między fotonami spolaryzowanym pod kątem +45 stopni i -45 stopni, a inne pozwalają mu rozróżniać między fotonami spolaryzowanymi poziomo i pionowo. Zwróć uwagę ,że Alicja ma cztery polaryzacje a Bob ma tylko dwa analizatory!! Zauważ też jak 0 i 1 są ustawiane przez Alicję. To jest kluczowe! Co Bob robi potem? Cóż, wybiera losowo jeden analizator i używa go do zapisu każdego fotonu. Teraz zapisuje jakiego analizatora używał i co zapisał (jeśli wybrał zły analizator, nie uzyska żadnej informacji o stanie fotonu, w przypadku zapomnienia, polaryzacja jest jednym ze stanów fotonu). Na przykład, jeśli Alicja wyśle foton spolaryzowany pionowo a Bob wybierze detekcję fotonów +/- 45 stopni. Zasadniczo jeśli Bob wybrał analizator +/-45 stopni jest 50% szans ,że coś zapisze. Nawet jeśli Bob odkryje później ,że wybrał zły analizator, ne będzie sposobu odkrycia jaki stan polaryzacji wysłała Alicja.
3) Po trzecie , po wymianie wystarczającej liczby fotonów, Bob rozpowie na kanale publicznym jakiej sekwencji analizatorów użył , ale nie wyniki jakie uzyskał.
4) Po czwarte, Alicja porówna tą sekwencję z wysłaną listą swoich oryginalnych bitów, i powie Bobowi na kanale publicznym przy okazji który analizator był kompatybilny z polaryzacją fotonów. Nie powie mu jakie stany polaryzacji wysłała. Jeśli Bob użył analizatora, który nie był kompatybilny z fotonem Alicji, bit jest po prostu niszczony. Dla bitów które pozostały (zobacz zatrzymaną sekwencję bitów na rysunku) Alicja i Bob wiedzą ,że mają tą samą wartość -wiedzą,że podsłuchujący nie poturbował ich transmisji.Bity które pozostały, Ala i Bob mogą wykorzystać do wygenerowania klucza, którego użyją do zaszyfrowania wiadomości wysyłanej kanałem publicznym.



Zobaczmy przypadek kiedy mamy Eve. Przypuśćmy ,że Eve ma dojścia do kanału kwantowego i publicznego, i oczywiście,wysyła informacje do Boba, wiec jej podłuch będzie niezauważony. Co jest nie tak na tym rysunku w tym przypadku? Oczywiście, ujawnione bity nie mogą być użyte do

szyfrowania czegokolwiek. Jeśli Eve przechwyci ich klucz, korelacja między wartościami ich bitów zostanie zredukowana. Na przykład, jeśli Eve ma te same urządzenia co Bob i przecięła kabel i mierzy sygnał, zawsze otrzyma bit losowy ilekroć wybierze zły analizator (statystycznie to 50% przypadków) .Ale mając przechwycony sygnał Eve musi jeszcze wysłać foton do Boba aby pokryć jego ścieżki. Dlatego w 50% przypadków analizatory Ali i Boba pasują, ale co w przypadku kiedy Eve nie używa poprawnego analizatora i tak jest w 50% przypadków? Jednak w połowie tych przypadków foton incydentalnie będzie przechodził przez poprawny analizator po stronie Boba. Widzimy teraz ,że korelacja między pomiarami Alicji i Boba spadnie tylko 25% w obecności Eve. W tym przypadku, Alice i Bob wiedzą ,że ta informacja została przechwycona, kiedy porównywali klucze publicznym łączem widzieli wielkie rozbieżności (precyzyjniej, dwukrotne rozbieżności) i porzucili transmisję. Proste, nieprawdaż?

Jednak jak osiągnąć kryptografię kwantową w praktyce? Fotony są dobrymi kandydatami do przenoszenia informacji, są łatwe do stworzenia i pomiaru. Historia jaką przedstawiłem odnośnie polaryzacji może być zastosowana i do przesunięcia fazowego. Faktycznie, jest dużo częściej używana niż polarzyacja. Co lepsze, mogą być transmitowane przez światłowód , a przez ostatnie 25 lat tłumienia światła (pomiar ile fotonów gubi się podczas transmisji przy długości fali 1300 nm zostało zredukowane z kilku decybeli na metr do 0,35 decybela na kilometr. Oznacza to ,że fotony mogą sobie podróżować do 10km nim 50% z nich się zgubi ,co jest wystarczającym powodem dla zastosowania krytpografii kwantowej w sieciach lokalnych. Niektórzy z was mogą zwrócić uwagę ,że można użyć wzmacczniacza do transmisji fotonów, ale wzmacniacze nie mogą być użyte ponieważ stany kwantów nie mogą być kopiowane (w pewnych przypadkach tak, w przypadku teleportacji kwantowej, ale to nie ten przypadek). Są też projekty wykorzystania komunikacji kwantowej z satelity na ziemię lub innego satelity, ale jeszcze to nie jest praktykowane. Oczywiście to nie jedyny problem. Jest zawsze problem z jakością połączenia. Nieskorelowane bity mogą doprowadzić do eksperymentalnej niedoskonałości. Po pierwsze, Alicja musi mieć pewność ,że stworzyła fotony ,które są dokładnie w takim stanie jaki wybrała. Jeśli na przykład, foton pionowy jest niepoprawnie spolaryzowany pod kątem 84 stopni, jest tylko 1% możliwości ,że Bob znajdzie w kanale fotony spolaryzowane poziomo. Podobny problem jest po stronie Boba; czy mierzy dokładnie 90 stopni. Inną trudnością jest upewnienie się ,że kodowane bity utrzymają się podczas transmisji. Jest również jeden duży problem, ze względu na dwójłomność włókna, odbierane stany polaryzacji przez Boba, będą , generalni, różnić się od tych wysyłanych przez Alicję, i przez kalibrację ich apratów itd itp. Dla uniknięcia tych problemów, Ala i Bob muszą zastosować klasyczny algorytm korekcji błędów do swoich danych abyb mogli zredukować błędy poniżej poziomu błędów 10^(-9) - standard przemysłowy dla telekomunikacji cyfrowej. A ponieważ nie mogą być pewni czy obecność nieskorelowanych bitów wystąpiła ze względu na słabą konfigurację sprzętu czy podsłuchującego, muszą zakładać najczarniejszy scenariusz – że wszystkie błedy zostały spowodowane przez Eve. Istnieje pewna procedura znana Alicji i Bobowi jako "wzmocnienie ochrony prywatności", w której kilka bitów jest łączonych w jeden .Procedura ta zapewnia ,korelację bitów tylko jeśli bity inicjalizujące Alicji i Boba są takie same. Problem ze wzmocnieniem ochrony prywatności jest taki ,że skaraca długość klucza i możliwe jest tylko do pewnych błędów. Oznacza to ,że Alinka i Bob muszą być czujni aby nie wprowadzić kilku błędów kiedy zapoczątkowują wysyłanie swoich kwantowych bitów.