IX.
KRYPTOGRAFIA KWANTOWA

Janusz Adamowski

1 Wstęp

Wykład ten stanowi wprowadzenie do kryptografii kwantowej. Kryptografia kwantowa jest bardzo obszerną i szybko rozwijającą się dziedziną obliczeń kwantowych, która doczekała się już pierwszych zastosowań.

Wykład ten nie będzie zawierał systematycznego omówienia problemów kryptografii kwantowej. Przedstawię jedynie wybrane problemy kryptografii kwantowej oraz przykłady kwantowych kodów szyfrujących.

Zjawiska kwantowe mają zastosowanie w następujących operacjach kryptograficznych:

(1) łamanie kodów szyfrujących opartych na kluczu publicznym,

(2) generacja niemożliwego do złamania klucza prywatnego,

(3) bezpieczne przesyłanie klucza publicznego.

Ad (1): Peter Shor w pracach opublikowanych w latach 1994-1997 zastosował algorytm kwantowej transformaty Fouriera do faktoryzacji liczb całkowitych.

Uwaga: na Wykładzie 7 omówiona została szczególna wersja algorytmu Shora, której celem jest znajdowanie okresu funkcji.

Klucze publiczne (klasyczne i kwantowe) oparte są na faktoryzacji dużych liczb całkowitych. Zgodnie z algorytmem opracowanym przez Shora faktoryzacja liczby całkowitej N może zostać dokonana w czasie rzędu $\mathcal{O}(\log N)$.

Na tym wykładzie przedstawię wybrane zagadnienia związane z **kwantową dystrybucją klucza publicznego**.

Najpierw jednak podam wprowadzenie do **kryptografii opartej na kluczu prywatnym**.

2 Kryptografia oparta na kluczu prywatnym

Kryptografia oparta na kluczu publicznym została wprowadzona w latach 1970.

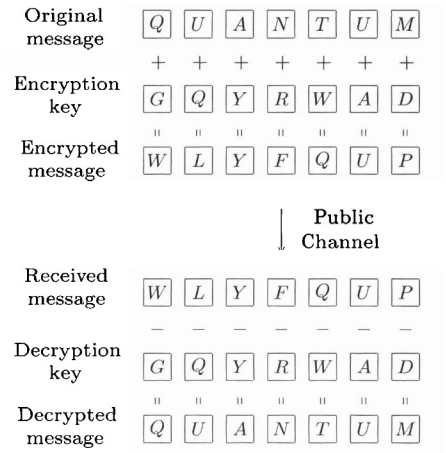
Do tego czasu wszystkie systemy kryptograficzne były oparte na **kluczu prywatnym**.

W systemie opartym na kluczu prywatnym **przed wysłaniem** przez nadawcę (Alicja, A) zaszyfrowanej wiadomości do odbiorcy (Bartek, B) Alicja i Bartek musieli **w bezpieczny sposób** wymienić się prywatnym kluczem szyfrującym. Nadawca A używał tego klucza do **zakodowania** przesyłanej informacji, którą wysyłał do odbiorcy B. Po odebraniu zakodowanej informacji odbiorca B używał tego klucza do **odkodowania** informacji.

Prostym, lecz efektywnym, przykładem klucza prywatnego jest **kod Vernama**.

Zasada działania tego kodu jest prosta:

Nadawca A i odbiorca B posiadają N-bitowe sekretne ciągi znaków, które są identyczne. Ten ciąg jest uzgodnionym wcześniej **kluczem prywatnym**. Nadawca A szyfruje wiadomość dodając do siebie ciągi znaków wiadomości i



Rysunek 1: Ilustracja działania kodu Vernama. Nadawca dokonuje szyfrowania wiadomości dodając przypadkowe bity klucza (w tym przypadku litery alfabetu) do oryginalnej wiadomości. Odbiorca odszyfrowuje odebraną wiadomość odejmując bity klucza i odzyskuje wiadomość oryginalną.

klucza. A wysyła powstałą w ten sposób zaszyfrowana wiadomość do B. Odbiorca rozszyfrowywuje tę wiadomość odejmując od otrzymanego ciągu znaków znaki klucza.

Zasada kodu Vernama zilustrowana jest na rysunku (1).

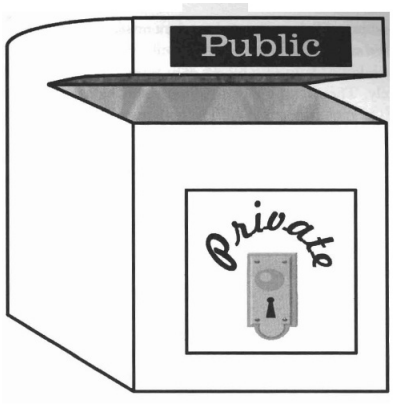
Zaletą tego systemu jest jego prostota. Jeżeli ponadto ciąg znaków klucza jest odpowiednio długi i nieznany postronnym osobom, to kod ten jest bezpieczny. Szpieg (Ewa, E) może wprawdzie zakłócić (przerwać) przekaz informacji pomiędzy A i B, jednak to zakłócenie może zostać wykryte i przesyłanie informacji zostaje wstrzymane.

Stosując odpowiednio długi ciąg znaków kodu szyfrującego A i B mogą spowodować, że część informacji ewentualnie rozszyfrowanej przez E jest dowolnie mała.

Jednakże pozostaje problem bezpiecznego przekazania klucza prywatnego pomiędzy A i B.

W przypadku kodu Vernama bezpieczeństwo kodowania jest zapewnione, jeżeli długość ciągu bitów klucza jest co najmniej równa długości ciągu bitów przesyłanej informacji. Ponadto użyte bity klucza nie mogą zostać użyte powtórnie.

Prowadzi to do ograniczeń w bezpiecznym stosowaniu systemów kryptograficznych opartych na kluczu prywatnym.



Rysunek 2: Ilustracja idei kryptografii opartej na kluczu publicznym: schemat działania skrzynki pocztowej.

3 Kryptografia oparta na kluczu publicznym

Podstawowa idea kryptografii opartej na kluczu publicznym jest analogiczna do działania skrzynki na listy, używanej przez pocztę wielu krajów (w tym Polski). Pokazuje to rysunek (2).

Powiedzmy, że odbiorca B chce otrzymywać wiadomości z użyciem klucza publicznego. Zgodnie z przedstawioną na rys. 9.2 ideą B musi wygenerować **dwa klucze: publiczny (powszechnie dostępny, P) i prywatny (sekretny, S)**. Dokładny rodzaj tych kluczy zależy od zastosowanego systemu szyfrującego.

Po wygenerowaniu kluczy odbiorca B podaje do publicznej wiadomości klucz publiczny P.

Załóżmy teraz, że nadawca A chce wysłać do odbiorcy B zaszyfrowaną wiadomość. Najpierw nadawca A musi otrzymać od odbiorcy B kopię jego klucza publicznego P. Następnie A szyfruje wiadomość używając klucza P i wysyła zaszyfrowaną wiadomość do B.

W celu zabezpieczenia się przed rozszyfrowaniem wiadomości przez osobę postronną (E) operacja szyfrowania powinna być trudna od odwrócenia (nawet przy użyciu znanego powszechnie klucza publicznego).

Najczęściej stosowaną, trudną do odwrócenia operacją jest **faktoryzacja dużych liczb całkowitych**. W skrócie: szyfrowanie wykorzystuje łatwą do wykonania operację mnożenia, natomiast odszyfrowanie wymaga zastosowania dużo trudniejszej operacji dzielenia.

Szpieg E mógłby ewentualnie odszyfrować przechwyconą zaszyfrowaną wiadomość, ponieważ dysponuje on kluczem publicznym P. Jednak taka operacja wymagałaby bardzo długiego czasu, a pod względem trudności wykonania byłaby porównywalna z wydobywaniem listu ze skrzynki pocztowej z wykorzystaniem otworu do wrzucania listów.

Odbiorca B dysponuje szybszym i prostszym sposobem odszyfrowania ode-

branej wiadomości, a mianowicie stosuje on w celu sekretny klucz prywatny S. Zastosowanie klucza S pozwala na szybkie i niezawodne odzyskanie oryginalnej wiadomości.

Obecnie w klasycznej kryptografii powszechnie stosowany jest **kod RSA**, nazwany zgodnie z inicjałami nazwisk jego twórców (Rivest, Shamir, Adleman).

4 Kwantowa dystrybucja klucza

Kwantowa dystrybucja klucza jest protokołem kwantowym, za pomocą którego ciąg bitów klucza prywatnego może być przesyłany (tworzony) w sposób **bezpieczny** pomiędzy dwoma stronami za pośrednictwem **kanału publicznego**.

Przesłane bity klucza mogą zostać następnie użyte do implementacji klasycznego systemu szyfrującego, który umożliwi bezpieczne komunikowanie się stron.

Jedynym ograniczeniem protokołu kwantowej dystrybucji klucza jest konieczność przesyłania kubitów za pośrednictwem kanału publicznego, którego poziom błędów jest niższy od pewnego progu. W trakcie tego procesu nadawca przekształca swój ciąg bitów w kubity, które są przesyłane poprzez kanał publiczny, a odbiorca z powrotem przekształca odebrane kubity w bity klasyczne.

Bezpieczeństwo wytworzonego w ten sposób klucza jest gwarantowane przez własności informacji kwantowej, które wynikają z fundamentalnych prawa mechaniki kwantowej.

Podstawowa idea bezpieczeństwa kwantowej dystrybucji klucza opiera się na następującej własności informacji kwantowej:

Osoba podsłuchująca (E) nie może odczytać żadnej informacji, przechwytując kubity przekazywane pomiędzy A i B, **bez zaburzenia stanów kwantowych kubitów**.

(1) Zgodnie z twierdzeniem o nieklonowaniu kubitów (Twierdzenie I) E nie może skopiować przechwyconych kubitów.

(2) **Każdy zysk informacji kwantowej oznacza zaburzenie stanów kwantowych.** $\Longrightarrow$ Twierdzenie II

Twierdzenie II

Uzyskanie informacji w wyniku dowolnej próby rozróżnienia dwóch nieortogonalnych stanów kwantowych jest możliwe wyłącznie wtedy, gdy zostanie wprowadzone zaburzenie do odczytywanego sygnału.

Dowód

Powiedzmy, że $|\varphi\rangle$ i $|\psi\rangle$ są dwoma nieortogonalnymi stanami kwantowymi, z których E próbuje odczytać informację.

$$\langle\varphi|\psi\rangle = C \neq 0\,. \tag{1}$$

Ponadto oczywiście $C \neq 1$.

Proces uzyskiwania informacji kwantowej można zaimplementować przy użyciu układu pomocniczego, który zostaje spreparowany w pewnym standardowym stanie $|u\rangle$. Odebrane kubity $|\varphi\rangle$ lub $|\psi\rangle$ oddziaływują w sposób unitarny z układem pomocniczym. Oddziaływanie to opisane jest za pomocą operatora unitarnego U, który nie zaburza stanów $|\varphi\rangle$ i $|\psi\rangle$.

Dla obu stanów otrzymujemy zatem

$$\begin{aligned} |\varphi\rangle|u\rangle &\xrightarrow{U} |\varphi\rangle|v\rangle \\ |\psi\rangle|u\rangle &\xrightarrow{U} |\psi\rangle|v'\rangle \ . \end{aligned} \tag{2}$$

Gdyby stany $|v\rangle$ i $v'\rangle$ były różne, to osoba podsłuchująca (E) mogłaby je zidentyfikować uzyskują w ten sposób informację o kubitach $|\varphi\rangle$ i $|\psi\rangle$.

Jednakże transformacje unitarne nie zmieniają iloczynów skalarnych, otrzymujemy więc

$$\langle v|v'\rangle\langle\varphi|\psi\rangle = \langle u|u\rangle\langle\varphi|\psi\rangle \ . \tag{3}$$

Wynika stąd, że

$$\langle v|v'\rangle = \langle u|u\rangle = 1 \ . \tag{4}$$

A zatem stany $|v\rangle$ i $|v'\rangle$ muszą być identyczne.

Stany te mogłyby się różnić wyłącznie wtedy, gdyby w wyniku operacji (2) co najmniej jeden z przechwyconych kubitów ($|\varphi\rangle$ lub $|\psi\rangle$) uległ zmianie, ale to oznaczałoby zaburzenie przynajmniej jednego z kubitów.

$\Longrightarrow$ Rozróżnienie kubitów $|\varphi\rangle$ i $|\psi\rangle$ w sposób nieuchronny prowadzi do zaburzenia co najmniej jednego z nich.

c.b.d.o.

Twierdzenie II można wykorzystać do zabezpieczenia się przed podsłuchem przy przesyłaniu informacji pomiędzy Alicją i Bartkiem. W tym celu A i B przesyłają między sobą kubity nieortogolne i sprawdzają, czy przekaz informacji został zaburzony. Jeżeli stwierdzą zaburzenie, to albo przerywają transmisję danych albo ustalają górny próg szumów lub podsłuchu w kanale informacyjnym. Po jego przekroczeniu transmisja zostaje przerwana.

Mogą tego dokonać za pomocą kubitów "próbnych", które są w przypadkowy sposób wplecione w ciąg przesyłanych kubitów. W ten sposób górne ograniczenie na szumy stosuje się również do kubitów niosących wymienianą informację. Każde ich zaburzenie powyżej ustalonego poziomu szumów jest wykrywane.

Procedury postępowania w celu uzyskania bezpiecznej transmisji danych zawarte są w opracowanych protokołach kwantowej dystrybucji klucza.

Omówię dwa spośród tych protokołów.

5 Protokół BB84

C.H. Bennet and G. Brassard,Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, December **1984**, pp. 175-179 (IEEE, New York).

Etap I.

Nadawca (Alicja, A) rozpoczyna procedurę wytwarzając dwa przypadkowe ciągi (a i b) bitów klasycznych każdy o długości $(4+\Delta)n$.

Alicja koduje ciąg bitów a w postaci $(4+\Delta)n$ kubitów używając w tym celu czterech następujących stanów:

$$|\psi_{00}\rangle = |0\rangle \ , \tag{5}$$

$$|\psi_{10}\rangle = |1\rangle \ , \tag{6}$$

$$|\psi_{01}\rangle \equiv |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \ , \tag{7}$$

$$|\psi_{11}\rangle \equiv |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \ . \tag{8}$$

Stany (5) i (6) są stanami własnymi operatora Pauliego $Z \equiv \sigma_z$ odpowiednio do wartości własnych $+1$ i -1. Można łatwo sprawdzić, że stany (7) i (8) są stanami własnymi operatora Pauliego $X \equiv \sigma_x$ odpowiednio do wartości własnych $+1$ i -1.

Alicja koduje każdy z bitów ciągu a w postaci kubitu zapisanego w bazie $\{|0\rangle, |1\rangle\}$, jeżeli wartość bitu $b_k = 0$, lub kubitu zapisanego w bazie $\{|+\rangle, |-\rangle\}$, jeżeli wartość bitu $b_k = 1$.

Alicja otrzymuje w wyniku kodowania stan

$$|\Psi_A\rangle = \bigotimes_{k=1}^{(4+\Delta)n} |\psi_{a_k b_k}\rangle \ . \tag{9}$$

We wzorze (9) wskaźnik a_k odpowiada k-temu bitowi ciągu a, podobnie wskaźnik b_k odpowiada k-temu bitowi ciągu b.

Wynikiem pierwszego kroku, wykonanego przez Alicję, jest zakodowanie ciągu bitów a w bazach stanów własnych operatorów X lub Z, przy czym wybór bazy ($\{|\psi_{00}\rangle, |\psi_{10}\rangle\}$ lub $\{|\psi_{01}\rangle, |\psi_{11}\rangle\}$) jest określony przez wartości bitów ciągu b.

Można zauważyć, że stany (5), (6), (7) i (8) nie są wzajemnie ortogonalne, czyli żaden pomiar nie może rozróżnić wszystkich tych stanów.

Etap II.

Po wykonaniu pierwszego kroku Alicja wysyła stan $|\Psi_A\rangle$ do odbiorcy (Bartka, B) za pośrednictwem publicznego kanału komunikacji.

Bartek otrzymuje zaburzony kubit $|\Psi_B\rangle \equiv \mathcal{E}(|\Psi_A\rangle\langle\Psi|)$, gdzie $\mathcal{E}$ opisuje operację kwantową będącą wynikiem połączonego działania zakłóceń kanału komunikacyjnego i podsłuchu dokonanego przez Ewę (E).

Kubit otrzymany przez Bartka można zapisać w jawnej postaci jako

$$|\Psi_B\rangle = \sum_c \langle\psi_c|\Psi_A\rangle|\psi_c\rangle + \sum_i \langle\eta_i|\Psi_A\rangle|\eta_i\rangle \ , \tag{10}$$

gdzie $|\psi_c\rangle$ jest stanem kanału komunikacyjnego, a $|\eta_i\rangle$ jest stanem użytym przez Ewę do podsłuchu.

Uwaga (1): Oczywiście Bartek nie zna współczynników rozwinięcia we wzorze (10). Zna jedynie stan wynikowy $|\Psi_B\rangle$.

Uwaga (2): W przypadku braku podsłuchu wszystkie amplitudy $\langle\eta_i|\Psi_A\rangle = 0$. Ponadto przy braku zakłóceń w kanale komunikacyjnym $\langle\psi_c|\Psi_A\rangle = 0$ dla $c \neq A$, natomiast dla $c = A$ zachodzi $\psi_c = \Psi_A$ oraz $\langle\psi_c|\Psi_A\rangle = 1$, skąd otrzymujemy $|\Psi_B\rangle = |\Psi_A\rangle$.

Następnie Bartek ogłasza publicznie odebrany stan $|\Psi_B\rangle$.

Na tym etapie A, B i E posiadają swoje własne różniące się od siebie stany (odpowiednio $|\Psi_A\rangle$, $|\Psi_B\rangle$ i $|\eta_i\rangle$).

Należy zauważyć, że Alicja nie opublikowała dotąd ciągu b, a zatem Ewa nie wie, jakiej bazy ma użyć do pomiaru. Ewa może co najwyżej zgadywać. Jeżeli jednak jej odgadnięcie będzie błędne, to zaburzy ona stan otrzymany przez Bartka.

Ponadto Ewa nie może oddzielić efektu działania środowiska (zakłóceń kanału komunikacyjnego) od efektu swojego podsłuchu.

Na tym samym etapie odebrany przez Bartka stan $|\Psi_B\rangle$ nie zawiera użytecznej dla niego informacji, ponieważ Bartek nie zna ciągu b potrzebnego do odczytu.

Etap III.

Bartek przechodzi do kolejnej operacji, a mianowicie generuje on ciąg b', złożony z przypadkowych $(4 + \Delta)n$ bitów, a następnie dokonuje pomiaru odebranych kubitów używając w tym celu bazy stanów własnych operatorów X lub Z. Wybór bazy (X lub Z) przez Bartka jest określony przez wartości bitów przypadkowego ciągu b'.

Po wykonaniu pomiarów Bartek otrzymuje pewien ciąg bitów a' (po zamianie otrzymanych z pomiarów kubitów na bity).

Dopiero teraz Alicja publicznie ogłasza zawartość ciągu bitów b.

Etap IV.

W kolejnym etapie Alicja i Bartek prowadzą dyskusję za pośrednictwem publicznego kanału komunikacyjnego.

W trakcie tej wymiany informacji A i B odrzucają ze zbiorów a i a' wszystkie bity za wyjątkiem tych, dla których odpowiadające sobie bity w ciągach b i b' są sobie równe.

Bity pozostawione w ciągach a i a' spełniają warunek

$$a' = a \,, \tag{11}$$

ponieważ tylko w tym przypadku Bartek wykonał pomiary przy użyciu tych samych stanów bazy co Alicja.

Należy zauważyć, że znajomość ciągu b (ogłoszonego publicznie) nie odkrywa żadnej informacji o ciągu a.

W praktycznej realizacji można przyjąć, że A i B posiadają ciągi zawierające $2n$ bitów, wynikających z ich własnych pomiarów, natomiast liczbę $n\Delta$ dodatkowych bitów bitów należy przyjąć odpowiednio dużą.

Etap V.

Teraz Alicja i Bartek przeprowadzają testy w celu określenia, ile szumu lub zakłóceń wynikających z podsłuchu wystąpiło podczas ich komunikowaniu się z sobą. W tym celu wybierają progową maksymalną liczbę bitów n_t, dla której dopuszczają wystąpienie niezgodności pomiędzy wartościami ich bitów. Alicja wybiera w sposób przypadkowy n bitów spośród jej $2n$ bitów i publicznie ogłasza ten wybór. Wtedy Alicja i Bartek porównują wartości bitów testowych komunikując się poprzez kanał publiczny.

Jeżeli nie zgadzają się wartości więcej niż n_t bitów, przerywają komunikowanie się z sobą i uruchamiają protokół od początku. Jeżeli wynik testu jest pozytywny, tzn. Alicja i Bartek nie stwierdzą podsłuchu, Alicja i Bartek tworzą klucz publiczny używając do tego m bitów wybranych spośród n pozostałych bitów.

6 Protokół EPR

Zgodnie z protokołem EPR bity klucza są generowane jako ciąg rzeczywiście przypadkowy w procesie, wykorzystującym splątanie kwantowe.

Zasada działania protokołu EPR

Krok I.

Alicja i Bartek wytwarzaja wspólnie zbiór n splątanych par kubitów każdy w stanie Bella (stanie EPR)

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \,. \tag{12}$$

Sposoby produkcji zbioru splątanych kubitów:

- Alicja może spreparować n stanów splątanych, a następnie wysłać połowę z nich do Bartka lub *vice versa*,
- trzecia osoba (Cezary) może spreparować zbiór splątanych kubitów, a następnie przesłać połowę z nich Alicja, a drugą połowę Bartkowi,
- Alicja i Bartek mogli się spotkać dawno temu, wytwarzając wspólnie n par splątanych kubitów, którymi się podzielili po połowie i przechowali aż do aktualnego użycia.

Krok II.

Alicja i Bartek wybierają z tego zbioru – w sposób przypadkowy – podzbiór par EPR i sprawdzają, czy spełnia on nierówność Bella, czyli

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle \leq 2 \,. \tag{13}$$

Przypominam, że w nierówności (13) wielkości Q i R (mierzone przez Alicję) oraz S i T (mierzone przez Bartka) mogą przyjmować wartości ± 1, a symbol $\langle W\rangle$ oznacza wartość oczekiwaną wielkości W.

Kubity, które przejdą pomyślnie ten test, stanowią odpowiednio czyste splątane stany kwantowe. Mogą być one użyte do sprawdzenia wiarygodności pozostałych par EPR, a zatem do stwierdzenia, czy wystąpi szum spowodowany, np. podsłuchem.

Krok III.

Alicja i Bartek dokonują pomiarów wielkości Q, R, S, T we wspólnie określonej przypadkowej bazie. Wynikami tych pomiarów są przypadkowe ciągi liczb ± 1, które Alicja i Bartek zapisują w postaci ciągu bitów klasycznych.

W ten sposób Alicja i Bartek otrzymują ciąg skorelowanych z sobą bitów. Z tego ciągu mogą wytworzyć sekretny klucz prywatny do zastosowania, np. w protokole BB84.

Dyskusja

Protokół EPR jest w pełni **symetryczny**, ponieważ Alicja i Bartek wykonują identyczne operacje na swoich kubitach.

Nie można zatem stwierdzić, że czy klucz został wygenerowany przez Alicję czy przez Bartka.

Tak wygenerowany klucz jest **ciągiem liczb naprawdę przypadkowych**.

Ponadto klucz jest **nieokreślony** zanim Alicja i Bartek przeprowadzą pomiary na swoich parach EPR.

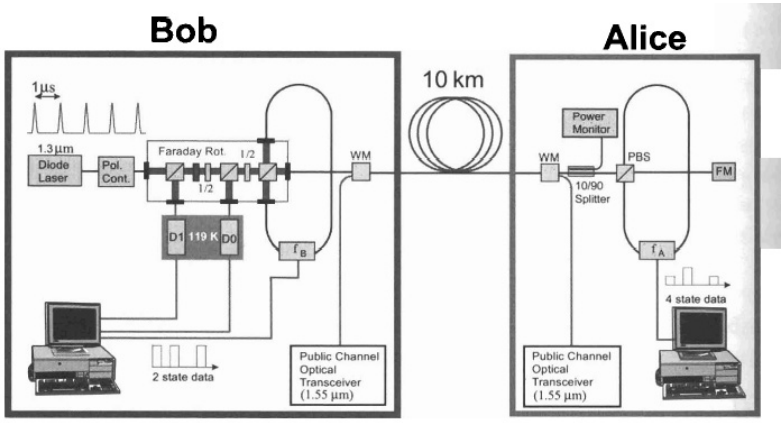
Końcowym wynikiem protokołu EPR jest **generacja sekretnego klucza prywatnego**.

7 Eksperymentalna realizacja kwantowej dystrybucji klucza

Rysunek (3) pokazuje schemat układu komercyjnego, służącego do kwantowej dystrybucji klucza, zbudowanego w IBM na bazie światłowodów.

Opis realizacji protokołu BB84:

- Najpierw Bartek generuje koheretne stany światła za pomocą lasera emitującego światło o długości fali 1.3 μm.
- Następnie Bartek wysyła wiązkę fotonów do Alicji, która poddaje ją takiemu osłabieniu, aby otrzymać (w przybliżeniu) pojedynczy foton.
- Alicja polaryzuje ten foton zgodnie z czterema stanami (5), (7), (6), (8) używanymi w protokole BB84. Stosowane w tej realizacji stany pierwszej bazy $|0\rangle$ i $|1\rangle$ odpowiadają liniowej polaryzacji poziomej (w kierunku x) i pionowej (w kierunku y). Natomiast stany drugiej bazy $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ i $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ opisują odpowiednio fotony spolaryzowane pod kątem $\pi/4$ i $3\pi/4$ względem osi x.
- Alicja wysyła spolaryzowany foton do Bartka.



Rysunek 3: Schemat układu, za pomocą którego zrealizowano kwantową dystrybucję klucza.

- Bartek mierzy polaryzację fotonu za pomocą analizatora ustawionego używając w tym celu wybranych w sposób przypadkowy stanów bazy (5), (7), (6), (8).
- Alicja i Bartek stosują do przesyłania fotonu specjalnej konfiguracji, w której foton przebywa dwukrotnie tę samą trajektorię. Dzięki temu następuje autokompensacja błędów, wynikających np. z powolnych fluktuacji długości trajektorii czy przesunięć kierunków polaryzacji.
- Alicja i Bartek selekcjonują podzbiór wyników, otrzymanych przy użyciu tej samej bazy, oraz uzgadniają swoje informacje.
- Alicja i Bartek dokonują wzmocnienia sygnałów, przesyłając wiązkę fotonów o długości fali 1.55 μm za pośrednictwem tego samego światłowodu. W trakcie tej operacji wymieniane są bity klucza z szybkością[†] ok. kilkuset bitów na sekundę.

[†] Poprawa jakości źródła światła i detektora może zwiększyć tę szybkość o kilka rzędów wielkości.

Pierwszy eksperyment demonstrujący kwantową dystrybucję klucza wykonany został w IBM w 1998 roku.

D.S. Bethune and W.P. Risk, *IQEC'98 Digest of Postdeadline Papers*, pages QPD12-2, Optical Society of America, Washington, DC, 1998.