W Y D A W N I C T W O P O L I T E C H N I K I Ś L Ą S K I E J W G L I W I C A C H

ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2018
Seria: ORGANIZACJA I ZARZĄDZANIE z. 130

ZAWODNOŚĆ KOMERCYJNYCH IMPLEMENTACJI INFORMATYKI KWANTOWEJ

Ireneusz J. JÓŹWIAK[1], Piotr JÓŹWIAK[2]

[1]Politechnika Wrocławska, Wydział Informatyki i Zarządzania, Wrocław; ireneusz.jozwiak@pwr.edu.pl
[2]Politechnika Wrocławska, Wydział Informatyki i Zarządzania, Wrocław; piotr.jozwiak@pwr.edu.pl

Streszczenie: W artykule został przedstawiony sposób przechwycenia transmisji danych poprzez kanał kwantowy. Najpierw omówiona została ogólna budowa sieci kwantowej oraz protokół komunikacyjny. Następnie przedstawiony został sposób obejścia zabezpieczeń sieci kwantowej na przykładzie jednego z komercyjnych systemów kwantowych.

Słowa kluczowe: kryptografia kwantowa, kanał kwantowy, bezpieczeństwo transmisji, szyfrowanie, atak.

COMMERCIAL QUANTUM COMPUTING IMPLEMENTATIONS FAILURE

Abstract: In this article was shown the way to intercept data transmission over the quantum channel. First was discussed the general structure of quantum network and communication protocol. Then was illustrated the way to bypass the protection of quantum network with the example of one of commercial quantum systems.

Keywords: quantum cryptography, quantum channel, transmission security, encryption, attack.

1. Wprowadzanie

Kryptografia kwantowa jest uważana za teoretycznie niezawodną. Głównym nośnikiem informacji w systemach kwantowych jest foton, a wartości binarne są zapisywane poprzez jego polaryzacje. W teorii system ten powinien być całkowicie odporny na próbę podsłuchania przez osobę niepożądaną, ponieważ, z zasad mechaniki kwantowej wynika, że nie można odczytać informacji przenoszonej przez foton, nie zmieniając jej. Okazało się

jednak, że niektóre komercyjne implementacje systemów kwantowych istniejące obecnie na rynku posiadają wady konstrukcyjne, które umożliwiają obejście zabezpieczeń opartych na fundamentalnych zasadach mechaniki kwantowej - które czynią te systemy teoretycznie niezawodnymi. Zostało udowodnione, że dzięki lukom konstrukcyjnym, osoba podsłuchująca transmisje kwantową może przechwycić informację, nie zdradzając swojej obecności.

W artykule przedstawiono najważniejsze elementy systemu kwantowego oraz protokół wymiany klucza kryptograficznego poprzez kanał kwantowy, szczególnie elementy, które powinny chronić transmisję przed przechwyceniem. Następnie omówiony został atak na komercyjny system dystrybucji klucza kwantowego ID-500 opracowany przez szwajcarską firmę id Quantique.

2. Budowa kanału kwantowego

W kryptografii kwantowej, podstawowym nośnikiem informacji jest foton, czyli fala elektromagnetyczne, w której pole elektryczne i magnetyczne drgają prostopadle do siebie i do kierunku rozchodzenia się fali. Kierunek drgań pola elektrycznego nazywany jest polaryzacją. Osoba emitująca foton ma możliwość nadania mu dowolnej polaryzacji obracając polaryzatorem – filtrem przepuszczającym jedynie te fotony, których kierunek drgań pola elektromagnetycznego jest zgodny z konfiguracją polaryzatora. Przy użyciu analizatora fotonów można również odczytać kierunek polaryzacji pojedynczego fotonu. Role analizatora może pełnić na przykład kryształ kalcytu, którego współczynnik załamania światła zależy od kierunku polaryzacji fotonów. Gdy foton jest spolaryzowany ukośnie, trafia do górnego fotopowielacza z prawdopodobieństwem równym $\cos^2\alpha$, gdzie α jest kontem polaryzacji fotonu wyglądem kierunku poziomego, a do dolnego z prawdopodobieństwem $1\text{-}P = \sin^2\alpha$. Dla polaryzacji ukośnej (kąt 45°) prawdopodobieństwo trafienia do górnego, jak i dolnego fotopowielacza jest jednakowe i wynosi ½. Pomiar kierunku polaryzacji fotonu kryształem jest aktywny, czyli zmienia stan badanego układy w trakcie pomiaru. Jeżeli więc foton jest spolaryzowany ukośnie w stosunku do kryształy (analizatora), to kierunek jego polaryzacji ulegnie zmianie. Jedynie dla polaryzacji pionowej i poziomej, kierunek na wejściu i wyjściu analizatora jest taki sam.

By przenieść informację binarną za pomocą fotonu należy go spolaryzować zgodnie z ustalonym alfabetem. Zazwyczaj przyjmowany jest alfabet prosty A_p, gdzie polaryzacja pionowa oznacza jedynkę logiczną, a pozioma – zero logiczne. Dla bezpieczeństwa transmisji ustala się również drugi alfabet. Jest to alfabet ukośny A_u, gdzie logiczne zero są oznaczone przez fotony spolaryzowane pod kątem 45°, a logiczną jedynkę oznacza polaryzacja pod kątem 135° (-45°). Inne kierunki polaryzacji nie są wykorzystywane w procesie komunikacji. Tabele 1 i 2 stanowią zestawienie sposobów kodowania fotonów (Maćkowiak, 20.11.2017).

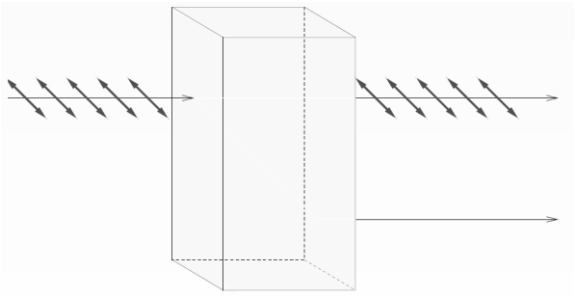
Tabela 1.
Alfabet prosty A_p (Maćkowiak, 20.11.2017)

Kierunek polaryzacji	Wartość logiczna
↔ (poziomy)	0
↕ (pionowy)	1

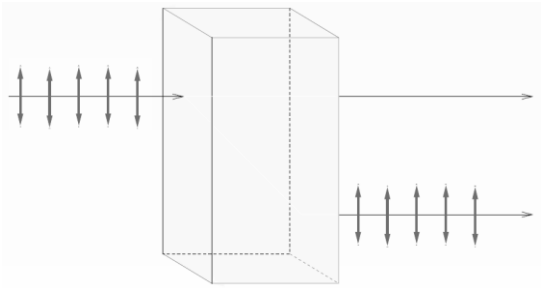
Tabela 2.
Alfabet prosty A_u (Maćkowiak, 20.11.2017)

Kierunek polaryzacji	Wartość logiczna
↗ (ukośny 45°)	0
↖ (ukośny 135°)	1

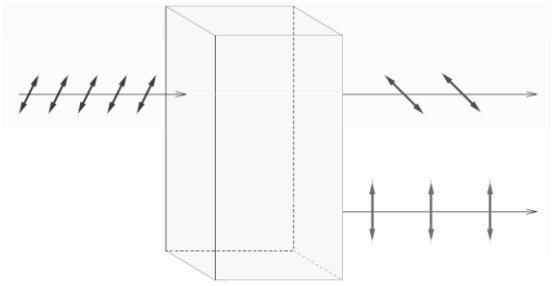
Podobnie jak fotony mogą być spolaryzowane ukośnie lub prosto, kryształ analizujący również można obracać o pewien ustalony kąt w celu manipulowania wynikami pomiarów. Gdy kryształ nie jest obrócony, stanowi bazę prosta pomiarów. W tym układzie fotony spolaryzowane poziomo i pionowo przechodzą przez kryształ bez zmiany kierunku polaryzacji odpowiednio do górnego i dolnego fotopowielacza z prawdopodobieństwem równym 1. Foton spolaryzowany ukośnie natomiast trafi do górnego lub dolnego fotopowielacza w prawdopodobieństwem równym ½, oraz kierunek jego polaryzacji ulegnie zmianie, ponieważ jest zorientowany ukośnie względem kryształu. Wszystkie trzy sytuacje zostały zilustrowane na rysunkach 1, 2 i 3.



Rysunek 1. Przykład transmisji fotonu odczytany na krysztale ustawionym w pozycji bazy prostej oraz pozioma polaryzacja fotonów. W tym przypadku foton zawsze opuszcza kryształ do górnego fotopowielacza. Maćkowiak, 20.11.2017.

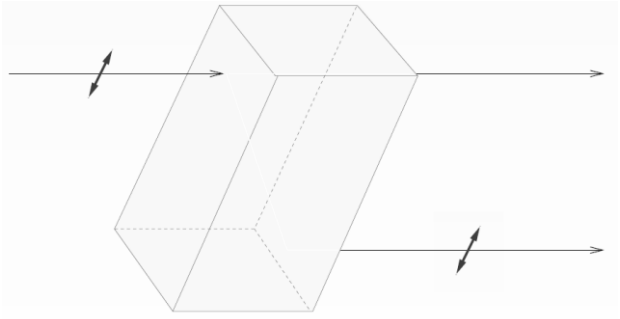


Rysunek 2. Przykład transmisji fotonu odczytany na krysztale ustawionym w pozycji bazy prostej oraz pionowa polaryzacja fotonów. W tym przypadku foton zawsze opuszcza kryształ do dolnego fotopowielacza. Maćkowiak, 20.11.2017.

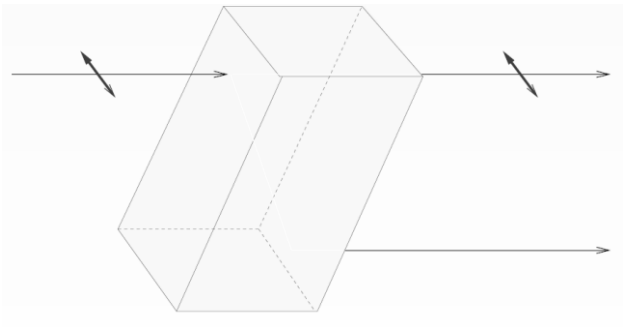


Rysunek 3. Przykład transmisji fotonu odczytany na krysztale ustawionym w pozycji bazy prostej oraz ukośna polaryzacja fotonów. W tym przypadku foton opuszcza kryształ do dolnego lub górnego fotopowielacza z prawdopodobieństwem równym w obu przypadkach ½. Maćkowiak, 20.11.2017.

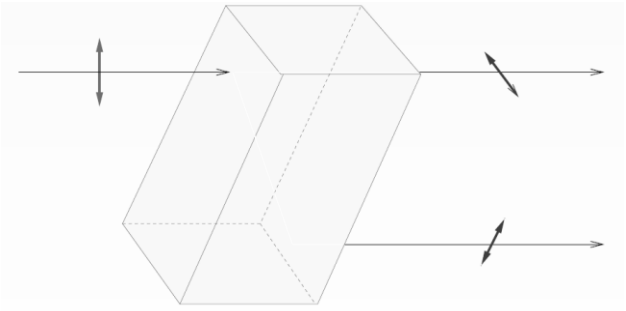
Po obróceniu kryształ o kąt 45° w stosunku do bazy prostej, powstaje baza ukośna. Teraz fotony spolaryzowane ukośnie są przepuszczane przez kryształ bez zmiany kierunku polaryzacji, ponieważ ich polaryzacja jest równoległa lub prostopadła do orientacji kryształu. Teraz również wiadomo, że fotony spolaryzowane pod kątem 45° trafią do dolnego fotopowielacz z prawdopodobieństwem równym 1, a te spolaryzowane pod kątem 135° – do górnego z tym samym prawdopodobieństwem. Fotony spolaryzowane pionowo, bądź poziomo są teraz nastawione ukośnie względem kryształu, więc ich polaryzacja ulegnie zmianie w trakcie pomiaru i prawdopodobieństwo trafienia go górnego lub dolnego fotopowielacza wynosi ½. Wszystkie trzy sytuacje zostały zilustrowane na rysunkach 4, 5 i 6.



Rysunek 4. Przykład transmisji fotonu odczytany na krysztale ustawionym w pozycji bazy ukośnej oraz ukośna polaryzacja fotonów (45°). W tym przypadku foton zawsze opuszcza kryształ do dolnego fotopowielacza. Maćkowiak, 20.11.2017.



Rysunek 5. Przykład transmisji fotonu odczytany na krysztale ustawionym w pozycji bazy ukośnej oraz ukośna polaryzacja fotonów (135°). W tym przypadku foton zawsze opuszcza kryształ do górnego fotopowielacza. Maćkowiak, 20.11.2017.



Rysunek 6. Przykład transmisji fotonu odczytany na krysztale ustawionym w pozycji bazy ukośnej oraz pionowa polaryzacja fotonów. W tym przypadku foton opuszcza kryształ do dolnego lub górnego fotopowielacza z prawdopodobieństwem równym w obu przypadkach ½. Maćkowiak, 20.11.2017.

Jeżeli foton trafił do dolnego fotopowielacza, to odbiorca założy że nadawca chciał przesłać „jedynkę", jeżeli trafi do górnego – „zero". Tabele 3 i 4 przedstawiają zestawienie informacji na temat analizy polaryzacji fotonów kryształami o bazie prostej i ukośnej. Opracowano je na podstawie monografii (Jacak et al., 2013).

Tabela 3.
Zachowanie fotonu na krysztale w ustawieniu bazy prostej.

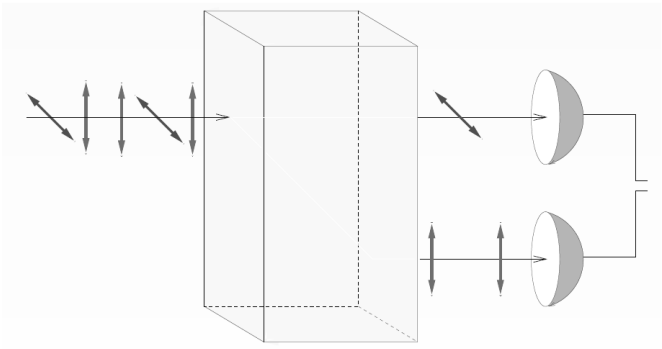
Wejście	**Polaryzacja wyjściowa**	**Fotopowielacz**	**Prawdopodobieństwo**
Polaryzacja pozioma	Pozioma	Górny	1
Polaryzacja pionowa	Pionowa	Dolny	1
Polaryzacja ukośna	Pozioma	Górny	½
	Pionowa	Dolny	½

Tabela 4.
Zachowanie fotonu na krysztale w ustawieniu bazy ukośnej.

Wejście	Polaryzacja wyjściowa	Fotopowielacz	Prawdopodobieństwo
Polaryzacja pozioma	Ukośna 135°	Górny	½
	Ukośna 45°	Dolny	½
Polaryzacja pionowa	Ukośna 135°	Górny	½
	Ukośna 45°	Dolny	½
Polaryzacja ukośna 45°	Ukośna 45°	Dolny	1
Polaryzacja ukośna 135°	Ukośna 135°	Górny	1

Z powyższej analizy bezpośrednio widać że, pomiary w bazie prostej nie dają żadnych informacji o polaryzacji ukośnej, tzn. o polaryzacji fotonów padających na kryształ pod kątem 45° lub 135°, tym samym baza prosta nie nadaje się do wykonywania pomiarów fotonów spolaryzowanych ukośnie. Analogiczne stwierdzenie odnajdujemy dla bazy ukośnej oraz fotonów spolaryzowanych pionowo i poziomo.

Urządzenia przeznaczone do odbioru kwantowych transmisji zaopatrzone są również w detektory fotonów. Rolę detektora fotonów pełni fotodioda lawinowa – element oparty o złącze P-N. W momencie oświetlenia fotodiody, powstaje w niej siła elektromotoryczna, która powoduje przepływ prądu w obwodzie. Ponieważ foton może zostać skierowany do jednego z dwóch fotopowielaczy, wymagane jest użycie dwóch detektorów fotonów. Jeden rejestruje trafienia samych „jedynek", czyli fotonów pochodzących z dolnego fotopowielacza, drugi rejestruje trafienia samych „zer", czyli fotonów pochodzących z górnego fotopowielacza. Uzupełniony układ, który mógłby posłużyć do odbioru transmisji kwantowej przedstawiony został na rysunku 7 (Gisin, Ribordy, Tittel, Zbinden, 2002).



Rysunek 7. Układ do odbioru kwantowej transmisji – kryształ i dwie fotodiody lawinowe. Gisin, Ribordy, Tittel, Zbinden, 2002.

3. Bezpieczeństwo komunikacji w kanale kwantowym

Wspomaganie Bezpieczeństwo komunikacji w transmisji kwantowej można zapewnić w oparciu o klasyczną kryptografię z wykorzystaniem szyfrowania transmisji w oparciu o klucz kryptograficzny. Jednym z pierwszych przykładów szyfrowania transmisji kwantowej był protokół BB84 opracowany w 1984 roku przez Gillesa Brassarda z Uniwersytetu Cornell oraz Charlesa Bennetta z Uniwersytetu Harvard (Lomonaco, 1998).

Tym samym podstawowym wyzwaniem jest możliwość wymiany klucza kryptograficznego pomiędzy dwoma stronami komunikacji w sposób zapewniający bezpieczeństwo braku jego podsłuchania. Problem ten znany jest pod nazwą Kwantowej Dystrybucji Klucza QKD (ang. *Quantum Key Distribution*).

Podstawową różnicą pomiędzy kryptografią kwantową (QC) a kryptografią klasyczną (CC) jest możliwość wykorzystania podstawowych praw mechaniki kwantowej do zabezpieczenia transmisji w przeciwieństwie do metod opartych o trudnościach obliczeniowych używanych w systemach CC. Prawa fizyki kwantowej sprawiają, że QC jest bezpieczna ze względu na poniższe zasady (Houston, 2007):

– jakakolwiek próba zmierzenia fotonu przez osobę podsłuchującą jest nie możliwa bez wykrycia tego faktu przez nadawcę i odbiorcę,
– pojedynczy foton nie da się podzielić, aby móc wykonać pomiar w tajemnicy,
– pojedynczy foton nie da się sklonować ani skopiować, aby pomiar dokonać na jego kopii w sposób tajemny.

Protokół BB84, w idealnych warunkach – bez zakłóceń, przebiega w dwóch fazach. Uczestnikami komunikacji będą nadawca, odbiorca i osoba podsłuchująca. Nadawca jest wyposażony w emiter fotonów i polaryzator, dzięki któremu może nadawać fotonom dowolny kierunek polaryzacji. Odbiorca posiada analizator i dwa detektory fotonów omówione w poprzednim rozdziale. Nadawca i odbiorca ustalają pomiędzy sobą dwa różne alfabety do kodowania i dekodowania informacji binarnej na podstawie kierunku polaryzacji fotonów: prosty(A_p) oraz ukośny(A_u).

W pierwszej fazie nadawca przesyła sygnał kwantowy do odbiorcy. W tym celu musi wybrać w sposób losowy, z prawdopodobieństwem równym ½, jeden z dwóch alfabetów do zakodowania informacji binarnej w fotonie. Wybór alfabetu przez nadawcę oznacza wybranie kierunku polaryzacji fotonu. Kierunek polaryzacji może być prosty – pionowy bądź poziomy, lub ukośny – pod kątem 45° lub 135°. Odbiorca w celu zdekodowania informacji przenoszonej przez foton również musi wybrać w sposób losowy jeden z dwóch ustalonych alfabetów, czyli wybrać bazę pomiarową poprzez obracanie analizatora o odpowiedni kont. Ponieważ odbiorca nie wie w jaki sposób nadawca spolaryzował foton, jedynie w około 50% przypadków wybierze alfabet kompatybilny z alfabetem wybranym przez nadawcę. W pozostałych 50% przypadków dokona złego wyboru, ale nawet wtedy ma 50% szans na to,

że analizator odczyta foton zgodnie z intencją nadawcy. Reasumując, odbiorca wybiera bazę pomiarową w sposób losowy, z równym prawdopodobieństwem wynoszącym ½. Jeżeli wybór jest prawidłowy, prawdopodobieństwo poprawnego rozkodowania informacji wynosi 1. Jeżeli wybór był nieprawidłowy, to prawdopodobieństwo wynosi ½. Czyli całkowite prawdopodobieństwo prawidłowego rozkodowania informacji przez odbiorcę w oparciu o wzór (1) wynosi ¾.

$$P_C = P(b_K) \cdot P_t(t \mid K) + P(b_N) \cdot P_t(t \mid N) \tag{1}$$

$$P_C = \frac{1}{2} \cdot 1 + \frac{1}{2} * \frac{1}{2} = \frac{3}{4}$$

gdzie:

b_K – baza kompatybilna z wyborem nadawcy,

b_N – baza niekompatybilna z wyborem nadawcy,

P_c – prawdopodobieństwo całkowite poprawnego rozkodowania fotonu przez odbiorcę,

$P(b_K)$ – prawdopodobieństwo wyboru bazy kompatybilnej z wyborem nadawcy,

$P_t(t \mid K)$ – prawdopodobieństwo trafienia pod warunkiem, że baza była kompatybilna z wyborem nadawcy,

$P(b_N)$ – prawdopodobieństwo wyboru bazy niekompatybilnej z wyborem nadawcy,

$P_t(t \mid N)$ – prawdopodobieństwo trafienia pod warunkiem, że baza była niekompatybilna z wyborem nadawcy.

Użycie dwóch różnych alfabetów, których pomiarów nie można ze sobą łączyć sprawia, że zarówno odbiorca, jak i osoba podsłuchująca może odebrać transmisję nadawcy, co najwyżej z 75% pewnością.

W fazie drugiej, nadawca i odbiorca komunikują się ze sobą poprzez kanał publiczny w celu ustalenia, które wybory alfabetów były ze sobą kompatybilne. Pozycje bitów, gdzie wybory alfabetów były niekompatybilne są usuwane z ciągu. Powstają w ten sposób dwa

Tabela 5.
Przykład komunikacji przez kanał kwantowy. (Yi et al, 2007)

Losowy ciąg (nadawca)	0	1	1	0	1	0
Polaryzacja fotonów (nadawca)	↔	↘	↕	↔	↘	↗
Wybór bazy (odbiorca)	ukośna	ukośna	prosta	prosta	ukośna	prosta
Otrzymana polaryzacja (odbiorca)	↘	↘	↕	↔	↘	↔
Zgodność	nie	tak	tak	tak	tak	Nie
Klucz wynikowy	X	1	1	0	1	X

Tabela 6.
Przykład komunikacji przez kanał kwantowy z ingerencją osoby podsłuchującej. (Yi et al, 2007)

Losowy ciąg (nadawca)	0	1	1	0	1	0
Polaryzacja fotonów (nadawca)	↔	↘	↕	↔	↘	↗
Wybór bazy (osoba podsłuchująca)	prosta	prosta	prosta	prosta	prosta	Prosta
Otrzymana polaryzacja(osoba podsłuchująca)	↔	↔	↕	↔	↕	↕
Wybór bazy (odbiorca)	ukośna	ukośna	prosta	prosta	ukośna	prosta
Otrzymana polaryzacja (odbiorca)	↘	↗	↕	↔	↘	↔
Zgodność	nie	tak	tak	tak	tak	Nie
Klucz wynikowy	X	**0**	1	0	1	X

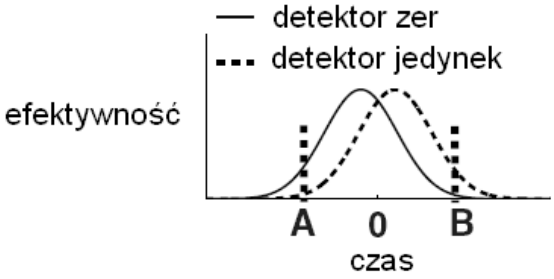
krótsze ciągi bitów, po stronie nadawcy i odbiorcy, które stanowią klucz kryptograficzny. Tabela 5 przedstawia przykładowy ciąg przesyłany poprzez kanał kwantowy.

Osoba trzecia, w celu podsłuchania transmisji na kanale kwantowym, musiałaby przechwytywać fotony od nadawcy, dekodować je losowo wybraną bazą pomiarową i odsyłać do odbiorcy. Jak zostało powiedziane w poprzednim rozdziale, wybór złej bazy pomiarowej zmienia polaryzację fotonu, więc może dojść do sytuacji, w której odbiorca pomimo wyboru alfabetu kompatybilnego z wyborem nadawcy, źle rozkodował informacje binarną. W takim przypadku, niektóre bity w kluczach nadawcy i odbiorcy nie będą się ze sobą zgadzać. Fakt niezgodności obu kluczy demaskuje osobę podsłuchującą. Jeżeli próba podsłuchu zostanie wykryta, cały proces zaczyna się od nowa. Tabela 6 prezentuje skutek ingerencji osoby trzeciej w proces komunikacji.

4. Przebieg ataku Time Shift Attack (TSA)

Komercyjne urządzenia służące do komunikacji kwantowej dostępne obecnie na rynku są oparte na tej samej zasadzie detekcji fotonów jaką przedstawiono w poprzednich rozdziałach. Również dysponują analizatorem oraz dwiema fotodiodami pełniącymi rolę detektorów fotonów. Transmisja kwantowa była uważana za niemożliwą do przechwycenia przez osobę podsłuchującą, bez jednoczesnego ujawnienia jej. Przyczyną tego był fakt, że nie można zmierzyć polaryzacji fotonu, bez zmiany jej kierunku. Rzeczywiste urządzenia kwantowe posiadają jednak wady konstrukcyjne dzięki którym możliwe jest obejście tego problemu i wykradzenie części klucza kryptograficznego, bez zdradzania swojej obecności.

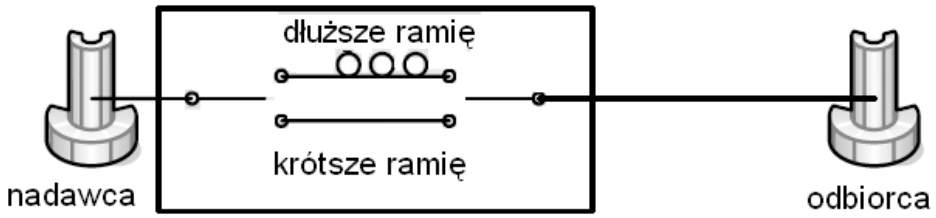
W 2008 został zademonstrowany, w warunkach laboratoryjnych, pierwszy udany atak na komercyjny system kwantowej dystrybucji klucza kryptograficznego ID-500, wyprodukowany przez szwajcarską firmę id Quantique. Atak ten wykorzystuje wadę w budowie dekodera fotonów, polegającą na różnicy w wydajności diody wykrywającej zera i diody wykrywającej jedynki na przestrzeni odcinka czasu. Rozbieżności te wynikają z różnic w długości kabla jakim zostały połączone. W momencie, gdy nadawca chce przesłać sygnał kwantowy, odbiorca włącza detektory zer i jedynek na kilkaset pikosekund, by odebrać transmisję. Jednak jeden z detektorów posiada dłuższy czas aktywacji niż drugi i przez pewien czas będzie wykazywał mniejszą efektywność w wykrywaniu fotonów.



Rysunek 8. Niezgodność wydajności dekoderów w czasie.

Rysunek 8 przedstawia rozbieżności w efektywności wykrywania fotonów pomiędzy dwoma detektorami na przestrzeni odcinka czasu. Jak widać, efektywność detektora zer w czasie A jest znacznie wyższa niż detektora jedynek, którego czas aktywacji jest dłuższy. Analogiczna zależność występuje w czasie B i jest związana z różnymi czasami wygaśnięcia obu diod. W czasie A jak i B, odbiorca na możliwość odbierania tylko jednego rodzaju fotonów – zer lub jedynek.

Koncepcja ataku z wykorzystaniem przesunięcia w czasie aktywacji obu detektorów jest bardzo prosta. Osoba chcąca podsłuchać transmisje, nie dokonuje pomiaru fotonów tylko włącza się do procesu ich przesyłania pomiędzy nadawca i odbiorcą, zmieniając w ten sposób długość drogi jaką musi przemierzyć elektron od nadawcy do odbiorcy. W czasie gdy tylko jeden detektor fotonów w systemie jest aktywny, odbiorca może rejestrować jedynie nadejścia zer lub jedynek. Nadawca, zmieniając długość połączenia, może przesuwać czas dotarcia sygnału kwantowego do dekodera w stronę czasu A lub B. Jeżeli przesunie czas dotarcia sygnału kwantowego w stronę A, to ma pewność, że każdy zarejestrowany w tym czasie foton był zerem. Tego, kiedy odbiorca zarejestrował trafienie, osoba podsłuchująca może dowiedzieć się, na przykład przez przechwycenie transmisji poprzez kanał publiczny. Rysunek 9 przedstawia jedno z ustawień możliwych do przeprowadzenia ataku z przesunięciem w czasie aktywacji detektorów (Yi et al, 2007).



Rysunek 9. Układ do przesuwania czasu dotarcia fotonu do odbiorcy.

Tak więc kluczowym elementem ataku jest czas aktywacji detektorów fotonów, który w ID-500 jest ustawiany niezależnie dla każdego detektora przez wbudowany w dekoder program kalibrujący. W czasie testów laboratoryjnych, najwyższa zaobserwowana rozbieżność w czasach aktywacji wynosiła w przybliżeniu 100 pikosekund. Po uruchomieniu programu kalibrującego 2844 razy, maksymalna wartość 100 pikosekund została osiągnięta 106 razy, co stanowi w przybliżeniu 4% wszystkich prób. Na podstawie tych wyników przeprowadzono następnie symulacje prawdziwego ataku z sygnałem kwantowym długości 100 pikosekund. W 4% przypadków udało się przechwycić całość klucza kryptograficznego (Yi, Chi-Hang, Bing, Christine, Hoi-Kwong, 2007). Nie jest to najlepszy wynik jednak pokazuje, że teoretycznie niezawodne systemy kryptografii kwantowej mogą zostać w rzeczywistości złamane.

5. Podsumowanie

Podstawowym nośnikiem informacji w systemach kwantowych jest foton. Informacja binarna jest w nim kodowana i rozkodowywana za pomocą kierunku jego polaryzacji zgodnie z ustalonym alfabetem. By zapewnić bezpieczeństwo komunikacji, w jednej transmisji używane są dwa różne alfabety. Nadawca, chcąc przesłać wiadomość, koduję ją zgodnie z jednym z alfabetów, odbiorca musi następnie wybrać alfabet kompatybilny z wyborem nadawcy by poprawnie odczytać wiadomość. Wybór alfabetu przez odbiorcę jest równoznaczny z wyborem bazy pomiarowej jaką będzie badany kierunek polaryzacji fotonu. Interpretacja informacji zakodowanej przy użyciu fotonów zależy od wyboru alfabetu przez odbiorcę. Ponieważ odbiorca nie wie jakiego alfabetu użyto do zakodowania informacji w fotonie, a pomiar dokonany w jednej bazie nie daje żadnej informacji o pomiarze w drugiej, odbiorca nie może ze 100% pewnością stwierdzić czy prawidłowo zdekodował bit. Użycie dwóch różnych alfabetów stanowi jedno z zabezpieczeń komunikacji kwantowej. Drugim zabezpieczeniem jest właściwość fizyczna samego fotonu, która sprawia, że nie można dokonać na nim pomiaru, nie zmieniając jednocześnie kierunku jego polaryzacji. Te dwa elementy sprawiają, że systemy kwantowe są teoretycznie niezawodne (Jacak et al, 2012).

Niektóre urządzenia rzeczywiste oparte na technologii kwantowej posiadają wady konstrukcyjne, które pozwalają na obejście wyżej wymienionych zabezpieczeń. Jedną z takich wad odkryto w systemie ID-500. Polega ona na różnicy w czasie aktywacji detektorów fotonów odpowiedzialnych za rejestrowanie fotonów oznaczających logiczne zera i jedynki. W praktyce oznacza to że przez pewien określony czas, detektor nie jest w stanie rejestrować jednej z wartości logicznych. Osoba chcąca podsłuchać transmisję nie musi badać stanu fotonu narażając się na zdemaskowanie. Musi ona jedynie przesunąć sygnał w czasie, w którym jeden z dekoderów jest nieaktywny. Jeżeli jej się to uda, zyskuje pewność, że wszystkie fotony odebrane przez odbiorcę w tym odcinku czasu reprezentują jedną wartość logiczną – zero lub jeden – zależnie kierunku przesunięcia sygnału.

Atak ten został skutecznie przeprowadzony w 2008 roku. Odbył się w warunkach laboratoryjnych, a jego skuteczność wynosiła zaledwie 4%, jednak fakt ten dowodzi zawodności komercyjnych implementacji systemów kwantowych.

Bibliografia

1. Houston, L. (20.11.2017). *Secure Ballots Using Quantum Cryptography*. Retrived from https://www.cse.wustl.edu/~jain/cse571-07/ftp/ballots/index.html
2. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., (2002). *Quantum cryptography*. Geneva: University of Geneva.
3. Jacak, J.E., Gonczarek, R., Jacak, L., Jóźwiak, I.J. (2012). *Application of braid groups in 2D Hall system physics: composite fermion structure.* World Scientific, Singapore.
4. Jacak, M., Jóźwiak, I.J., Jacak, J.E., Gruber, J., Jacak, W. (2013). *Wprowadzenie do kryptografii kwantowej: implementacja protokołów kryptografii kwantowej na systemach niesplątanych fotonów (system Clavis II) I splatanych fotonów (system EPR S405 Quelle).* Wrocław: Oficyna Wydawnicza Politechniki Wrocławskiej.
5. Lomonaco, S.J. (1998). *A Quick Glance at Quantum Cryptography*. Baltimore: Dept. of Comp. Sci. & Elect. Engr. University of Maryland.
6. Maćkowiak, K. (20.11.2017) Kryptografia kwantowa. Retrived from: http://www.centrum.bezpieczenstwa.pl/artykuly/krypt_kwant.pdf
7. Yi, Z., Chi-Hang, F.F., Bing, Q., Christine, C., Hoi-Kwong, L. (2007). *Quantum hacking: Experimental demonstration of time-shift attac against practical quantum-key-distribution systems*. Toronto: Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical and Computer Engineering, University of Toronto.