KRYPTOGRAFIA KWANTOWA

Wstęp

Wykład ten stanowi wprowadzenie do kryptografii kwantowej.

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 stanowi wprowadzenie do kryptografii kwantowej. Kryptografia kwantowa jest bardzo obszerną i szybko rozwijającą się dziedziną obliczeń kwantowych, która doczekała się już pierwszych zastosowań.
Na wykładzie tym przedstawię wybrane problemy kryptografii klasycznej i kwantowej oraz podam przykłady kwantowych kodów szyfrujących i deszyfrujących.

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.
Na wykładzie tym przedstawię wybrane problemy kryptografii klasycznej i kwantowej oraz podam przykłady kwantowych kodów szyfrujących i deszyfrujących.
Kwantowy charakter kryptografii związany jest głównie z **kwantową dystrybucją klucza publicznego**.

Zjawiska kwantowe mają zastosowanie w następujących operacjach kryptograficznych:

Zjawiska kwantowe mają zastosowanie w następujących operacjach kryptograficznych:

(1) łamanie kodów szyfrujących opartych na kluczu publicznym,

Zjawiska kwantowe mają zastosowanie w następujących operacjach kryptograficznych:

(1) łamanie kodów szyfrujących opartych na kluczu publicznym,

(2) generacja niemożliwego do złamania klucza prywatnego,

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.

Ad (1): Peter Shor w pracach opublikowanych w latach 1994-1997 zastosował algorytm kwantowej transformaty Fouriera do faktoryzacji liczb całkowitych.
Algorytm Shora, omówiony na wykładzie 7., stosuje kwantową transformatę Fouriera do znajdowania okresu funkcji.

Ad (1): Peter Shor w pracach opublikowanych w latach 1994-1997 zastosował algorytm kwantowej transformaty Fouriera do faktoryzacji liczb całkowitych.
Algorytm Shora, omówiony na wykładzie 7., stosuje kwantową transformatę Fouriera do znajdowania okresu funkcji. Wynik ten może być zastosowany do faktoryzacji liczby całkowitej, co z kolei umożliwia złamanie klasycznego kodu RSA (patrz niżej).

Ad (1): Peter Shor w pracach opublikowanych w latach 1994-1997 zastosował algorytm kwantowej transformaty Fouriera do faktoryzacji liczb całkowitych.
Algorytm Shora, omówiony na wykładzie 7., stosuje kwantową transformatę Fouriera do znajdowania okresu funkcji. Wynik ten może być zastosowany do faktoryzacji liczby całkowitej, co z kolei umożliwia złamanie klasycznego kodu RSA (patrz niżej). Zgodnie z algorytmem Shora faktoryzacja liczby całkowitej N może zostać dokonana w czasie rzędu $\mathcal{O}(N^3)$.

Ad (1): Peter Shor w pracach opublikowanych w latach 1994-1997 zastosował algorytm kwantowej transformaty Fouriera do faktoryzacji liczb całkowitych.
Algorytm Shora, omówiony na wykładzie 7., stosuje kwantową transformatę Fouriera do znajdowania okresu funkcji. Wynik ten może być zastosowany do faktoryzacji liczby całkowitej, co z kolei umożliwia złamanie klasycznego kodu RSA (patrz niżej).
Zgodnie z algorytmem Shora faktoryzacja liczby całkowitej N może zostać dokonana w czasie rzędu $\mathcal{O}(N^3)$.
W stosowanych obecnie systemach szyfrujących (klasycznych i kwantowych) opartych na kluczach publicznych większość tych kluczy oparta jest na faktoryzacji dużych liczb całkowitych.

Kryptografia oparta na kluczu prywatnym

Kryptografia oparta na kluczu publicznym została wprowadzona w latach 1970.

Kryptografia oparta na kluczu publicznym została wprowadzona w latach 1970.
Do tego czasu wszystkie systemy kryptograficzne były oparte 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.

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.

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**.

Prostym, lecz efektywnym, przykładem klucza prywatnego jest **kod Vernama**.
Zasada działania tego kodu jest prosta:

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.

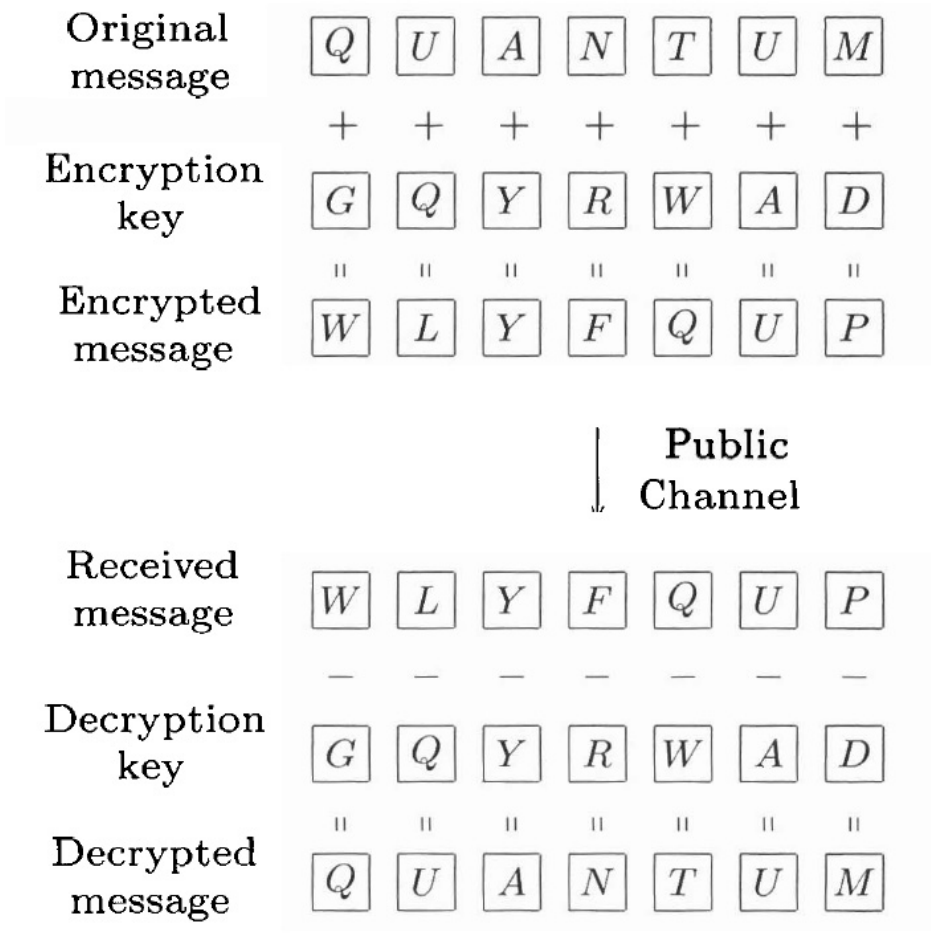
Prostym, lecz efektywnym, przykładem klucza prywatnego jest **kod Vernama**.
Zasada działania tego kodu jest prosta:
Nadawca A i odbiorca B posiadają N-bitowe sekretne ciągi znaków, które są identyczne. Ten ciąg jest uzgodnionym wcześniej **kluczem prywatnym**.

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 klucza.

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 klucza. A wysyła powstałą w ten sposób zaszyfrowana wiadomość do B.

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

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 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 rys. 9.1.



Rysunek: 9.1. 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.

Zaletą tego systemu jest jego prostota.

Zaletą tego systemu jest jego prostota. Jeżeli ponadto ciąg znaków klucza jest odpowiednio długi i nieznany postronnym osobom, to kod ten jest bezpieczny.

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.

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.

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.

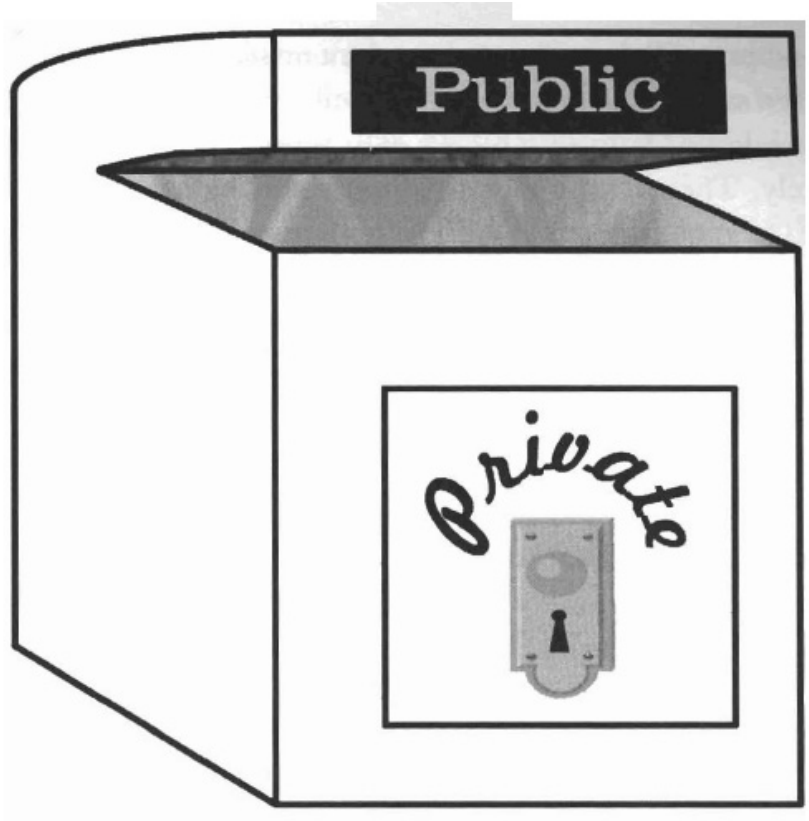
Jednakże pozostaje problem bezpiecznego przekazania klucza prywatnego pomiędzy A i B.
W przypadku kodu Vernama bezpieczeństwo kodowania jest zapewnione, jeżeli długość ciągu bitów klucza jest co najmniej równa długości ciągu bitów przesyłanej informacji. Ponadto użyte bity klucza nie mogą zostać użyte powtórnie.

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.

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).

Podstawowa idea kryptografii opartej na kluczu publicznym jest analogiczna do działania skrzynki na listy, używanej przez pocztę wielu krajów (w tym Polski). Pokazuje to rys. 9.2.



Rysunek: 9.2. Ilustracja idei kryptografii opartej na kluczu publicznym: schemat działania skrzynki pocztowej.

Powiedzmy, że odbiorca B chce otrzymywać wiadomości z użyciem klucza publicznego.

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)**.

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.

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.

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.

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.

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).

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**.

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.

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 odebranej wiadomości, a mianowicie stosuje on w celu sekretny klucz prywatny S.

Odbiorca B dysponuje szybszym i prostszym sposobem odszyfrowania odebranej wiadomości, a mianowicie stosuje on w celu sekretny klucz prywatny S. Zastosowanie klucza S pozwala na szybkie i niezawodne odzyskanie oryginalnej wiadomości.

Odbiorca B dysponuje szybszym i prostszym sposobem odszyfrowania odebranej 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).

Szyfrowanie i odszyfrowywanie informacji za pomocą kodu RSA

Elementy teorii liczb

Elementy teorii liczb

Zbiór liczb naturalnych $\mathcal{N} = 0, 1, 2, 3, 4, \ldots$.

Elementy teorii liczb

Zbiór liczb naturalnych $\mathcal{N} = 0, 1, 2, 3, 4, \ldots$.
Zbiór liczb pierwszych $\mathcal{P} = 2, 3, 5, 7, 11, 13, 17, \ldots$.

Elementy teorii liczb

Zbiór liczb naturalnych $\mathcal{N} = 0, 1, 2, 3, 4, \ldots$.
Zbiór liczb pierwszych $\mathcal{P} = 2, 3, 5, 7, 11, 13, 17, \ldots$.

Uwaga: Wszystkie, używane w tej części wykładu, zmienne przyjmują wartości należące do zbioru $\mathcal{N}$.

Fundamentalne twierdzenie arytmetyki

Fundamentalne twierdzenie arytmetyki

Dowolna liczba naturalna N większa od 1 posiada następującą własność **faktoryzacji** na iloczyn liczb pierwszych:

Fundamentalne twierdzenie arytmetyki

Dowolna liczba naturalna N większa od 1 posiada następującą własność **faktoryzacji** na iloczyn liczb pierwszych:

$$N = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} \ , \tag{1}$$

Fundamentalne twierdzenie arytmetyki

Dowolna liczba naturalna N większa od 1 posiada następującą własność **faktoryzacji** na iloczyn liczb pierwszych:

$$N = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} \ , \tag{1}$$

gdzie $p_1, \ldots, p_n$ są różnymi liczbami pierwszymi, natomiast $m_1, \ldots, m_n$ są liczbami naturalnymi.

Fundamentalne twierdzenie arytmetyki

Dowolna liczba naturalna N większa od 1 posiada następującą własność **faktoryzacji** na iloczyn liczb pierwszych:

$$N = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} \ , \tag{1}$$

gdzie $p_1, \ldots, p_n$ są różnymi liczbami pierwszymi, natomiast $m_1, \ldots, m_n$ są liczbami naturalnymi.

Faktoryzacja (1) jest jednoznaczna.

Każda liczba naturalna x może być zapisana w postaci

Każda liczba naturalna x może być zapisana w postaci

$$x = y + nM \ , \tag{2}$$

gdzie y jest resztą z dzielenia x przez M $(x, y, n, M \in \mathcal{N})$.

Każda liczba naturalna x może być zapisana w postaci

$$x = y + nM \ , \tag{2}$$

gdzie y jest resztą z dzielenia x przez M $(x, y, n, M \in \mathcal{N})$. Ze wzoru (2) wynika, że każdą liczbę naturalną można zapisać za pomocą operacji modulo jako

Każda liczba naturalna x może być zapisana w postaci

$$x = y + nM \ , \tag{2}$$

gdzie y jest resztą z dzielenia x przez M $(x, y, n, M \in \mathcal{N})$. Ze wzoru (2) wynika, że każdą liczbę naturalną można zapisać za pomocą operacji modulo jako

$$x = y \mod M \ . \tag{3}$$

Rząd liczby naturalnej x modulo N

Rząd liczby naturalnej x modulo N

Zakładamy, że $1 \leqslant x < N$.

Rząd liczby naturalnej x modulo N

Zakładamy, że $1 \leqslant x < N$.
Rzędem r liczby naturalnej x modulo N nazywany najmniejszą liczbę naturalną r taką, że

Rząd liczby naturalnej x modulo N

Zakładamy, że $1 \leqslant x < N$.
Rzędem r liczby naturalnej x modulo N nazywany najmniejszą liczbę naturalną r taką, że

$$x^r = 1 \mod N \,. \tag{4}$$

Rząd liczby naturalnej x modulo N

Zakładamy, że $1 \leqslant x < N$.
Rzędem r liczby naturalnej x modulo N nazywany najmniejszą liczbę naturalną r taką, że

$$x^r = 1 \mod N \,. \tag{4}$$

Można pokazać, że **problem wyznaczenia rzędu r modulo N liczby naturalnej x jest równoważny rozwiązaniu problemu faktoryzacji (1) liczby N.**

Działanie kodu RSA

Działanie kodu RSA

Zakładamy, że Alicja (A) jest nadawcą, a Bartek (B) – odbiorcą.

Działanie kodu RSA

Zakładamy, że Alicja (A) jest nadawcą, a Bartek (B) – odbiorcą.

(1) Ustalenie i przesłanie kodu kanałem publicznym

Działanie kodu RSA

Zakładamy, że Alicja (A) jest nadawcą, a Bartek (B) – odbiorcą.

(1) Ustalenie i przesłanie kodu kanałem publicznym

Bartek wybiera dwie liczby pierwsze p i q i oblicza $N = pq$, a następnie wybiera liczbę c, która nie posiada wspólnego dzielnika z liczbą $L = (p-1)(q-1)$.

Działanie kodu RSA

Zakładamy, że Alicja (A) jest nadawcą, a Bartek (B) – odbiorcą.

(1) Ustalenie i przesłanie kodu kanałem publicznym

Bartek wybiera dwie liczby pierwsze p i q i oblicza $N = pq$, a następnie wybiera liczbę c, która nie posiada wspólnego dzielnika z liczbą $L = (p-1)(q-1)$.
Bartek oblicza d jako odwrotność c względem operacji $\mod L \equiv \quad \mod (p-1)(q-1)$, tzn.

Działanie kodu RSA

Zakładamy, że Alicja (A) jest nadawcą, a Bartek (B) – odbiorcą.

(1) Ustalenie i przesłanie kodu kanałem publicznym

Bartek wybiera dwie liczby pierwsze p i q i oblicza $N = pq$, a następnie wybiera liczbę c, która nie posiada wspólnego dzielnika z liczbą $L = (p-1)(q-1)$.
Bartek oblicza d jako odwrotność c względem operacji mod $L \equiv \mod (p-1)(q-1)$, tzn.

$$cd = 1 \mod L\,. \tag{5}$$

Działanie kodu RSA

Zakładamy, że Alicja (A) jest nadawcą, a Bartek (B) – odbiorcą.

(1) Ustalenie i przesłanie kodu kanałem publicznym

Bartek wybiera dwie liczby pierwsze p i q i oblicza $N = pq$, a następnie wybiera liczbę c, która nie posiada wspólnego dzielnika z liczbą $L = (p-1)(q-1)$.
Bartek oblicza d jako odwrotność c względem operacji mod $L \equiv \mod (p-1)(q-1)$, tzn.

$$cd = 1 \mod L\,. \tag{5}$$

Bartek wysyła Alicji liczby c i N (lecz nie p i q oddzielnie) za pośrednictwem niezabezpieczonego kanału publicznego.

(2) Szyfrowanie i wysyłanie informacji

(2) Szyfrowanie i wysyłanie informacji

Alicja chce wysłać Bartkowi wiadomość, reprezentowaną za pomocą liczby a, przy czym $a < N$.

(2) Szyfrowanie i wysyłanie informacji

Alicja chce wysłać Bartkowi wiadomość, reprezentowaną za pomocą liczby a, przy czym $a < N$.
Uwaga: Jeżeli $a > N$, to Alicja musi podzielić wiadomość na części.

(2) Szyfrowanie i wysyłanie informacji

Alicja chce wysłać Bartkowi wiadomość, reprezentowaną za pomocą liczby a, przy czym $a < N$.
Uwaga: Jeżeli $a > N$, to Alicja musi podzielić wiadomość na części.
W celu zaszyfrowania informacji, Alicja oblicza

(2) Szyfrowanie i wysyłanie informacji

Alicja chce wysłać Bartkowi wiadomość, reprezentowaną za pomocą liczby a, przy czym $a < N$.
Uwaga: Jeżeli $a > N$, to Alicja musi podzielić wiadomość na części.
W celu zaszyfrowania informacji, Alicja oblicza

$$b = a^c \mod N \,, \tag{6}$$

(2) Szyfrowanie i wysyłanie informacji

Alicja chce wysłać Bartkowi wiadomość, reprezentowaną za pomocą liczby a, przy czym $a < N$.
Uwaga: Jeżeli $a > N$, to Alicja musi podzielić wiadomość na części.
W celu zaszyfrowania informacji, Alicja oblicza

$$b = a^c \mod N \,, \tag{6}$$

a następnie wysyła Bartkowi b (nadal za pośrednictwem publicznego kanału przekazu informacji).

(2) Szyfrowanie i wysyłanie informacji

Alicja chce wysłać Bartkowi wiadomość, reprezentowaną za pomocą liczby a, przy czym $a < N$.
Uwaga: Jeżeli $a > N$, to Alicja musi podzielić wiadomość na części.
W celu zaszyfrowania informacji, Alicja oblicza

$$b = a^c \mod N \,, \tag{6}$$

a następnie wysyła Bartkowi b (nadal za pośrednictwem publicznego kanału przekazu informacji).
Uwaga: Szpieg, który zna jedynie wartości b, c i N nie może wyznaczyć a.

(3) Odszyfrowanie informacji

(3) Odszyfrowanie informacji

Po otrzymaniu wiadomości od Alicji Bartek oblicza

(3) Odszyfrowanie informacji

Po otrzymaniu wiadomości od Alicji Bartek oblicza

$$b^d \mod N = a \, . \tag{7}$$

(3) Odszyfrowanie informacji

Po otrzymaniu wiadomości od Alicji Bartek oblicza

$$b^d \mod N = a \, . \tag{7}$$

Równość (7) wynika w teorii liczb.

(3) Odszyfrowanie informacji

Po otrzymaniu wiadomości od Alicji Bartek oblicza

$$b^d \mod N = a \, . \tag{7}$$

Równość (7) wynika w teorii liczb.

Liczby b, c i N są przesyłane za pośrednictwem publicznego kanału przekazu informacji, jednak wiadomość będzie mogła być dokładnie odczytana w krótkim czasie jedynie przez właściwego odbiorcę.

Prosty przykład liczbowy

Prosty przykład liczbowy

Bartek wybiera $p = 3$ i $q = 7$ i oblicza $N = pq = 21$ oraz $L = (p-1)(q-1) = 12$.

Prosty przykład liczbowy

Bartek wybiera $p = 3$ i $q = 7$ i oblicza $N = pq = 21$ oraz $L = (p-1)(q-1) = 12$.
Jako wartość liczby c Bartek wybiera $c = 5$, ponieważ 5 nie posiada wspólnego dzielnika z liczbą 12.

Prosty przykład liczbowy

Bartek wybiera $p = 3$ i $q = 7$ i oblicza $N = pq = 21$ oraz $L = (p-1)(q-1) = 12$.
Jako wartość liczby c Bartek wybiera $c = 5$, ponieważ 5 nie posiada wspólnego dzielnika z liczbą 12.
Bartek oblicza odwrotność d liczby $c = 5$ względem operacji mod 12

Prosty przykład liczbowy

Bartek wybiera $p = 3$ i $q = 7$ i oblicza $N = pq = 21$ oraz $L = (p-1)(q-1) = 12$.
Jako wartość liczby c Bartek wybiera $c = 5$, ponieważ 5 nie posiada wspólnego dzielnika z liczbą 12.
Bartek oblicza odwrotność d liczby $c = 5$ względem operacji mod 12

$$cd = 1 \mod L = 1 \mod 12 \Longrightarrow d = 5 \,,$$

Prosty przykład liczbowy

Bartek wybiera $p = 3$ i $q = 7$ i oblicza $N = pq = 21$ oraz $L = (p-1)(q-1) = 12$.
Jako wartość liczby c Bartek wybiera $c = 5$, ponieważ 5 nie posiada wspólnego dzielnika z liczbą 12.
Bartek oblicza odwrotność d liczby $c = 5$ względem operacji mod 12

$$cd = 1 \mod L = 1 \mod 12 \Longrightarrow d = 5 \,,$$

ponieważ $5 \times 5 = 24 + 1 = 2 \times 12 + 1$.

Alicja wybiera jako jej wiadomość $a = 4$

Alicja wybiera jako jej wiadomość $a = 4$
i oblicza

$$a^c = 4^5 = 1024 = 48 \times 21 + 16 \; .$$

Alicja wybiera jako jej wiadomość $a = 4$
i oblicza

$$a^c = 4^5 = 1024 = 48 \times 21 + 16 \; .$$

A zatem $a^c \bmod N = 4^5 \bmod 21 = 16 \bmod 21$,

Alicja wybiera jako jej wiadomość $a = 4$
i oblicza

$$a^c = 4^5 = 1024 = 48 \times 21 + 16 \; .$$

A zatem $a^c \bmod N = 4^5 \bmod 21 = 16 \bmod 21$,
czyli $b = 16$.

Alicja wysyła Bartkowi zaszyfrowaną wiadomość $b = 16$.

Alicja wysyła Bartkowi zaszyfrowaną wiadomość $b = 16$.
Bartek oblicza

$$b^d = 16^5 = 1048576 = 49932 \times 21 + 4 \ ,$$

Alicja wysyła Bartkowi zaszyfrowaną wiadomość $b = 16$.
Bartek oblicza

$$b^d = 16^5 = 1048576 = 49932 \times 21 + 4 \ ,$$

czyli $b^d = 16^5 = 4 \bmod 21$,

Alicja wysyła Bartkowi zaszyfrowaną wiadomość $b = 16$.
Bartek oblicza

$$b^d = 16^5 = 1048576 = 49932 \times 21 + 4 \ ,$$

czyli $b^d = 16^5 = 4 \mod 21$,
a stąd Bartek otrzymuje oryginalną wiadomość $a = 4$.

Złamanie kodu RSA

Szczególna wersja algorytmu Shora znajduje rząd r liczby $x \in \mathcal{N}$ modulo N przy użyciu $\mathcal{O}(N^3)$ operacji, gdzie N jest liczbą elementów w zbiorze $\{x\}$.

Szczególna wersja algorytmu Shora znajduje rząd r liczby $x \in \mathcal{N}$ modulo N przy użyciu $\mathcal{O}(N^3)$ operacji, gdzie N jest liczbą elementów w zbiorze $\{x\}$. Stosując ten algorytm szpieg (Ewa, E) wyznacza rząd r.

Jeżeli zatem Ewa przechwyci zakodowaną wiadomość b oraz zna ogłoszone publicznie liczby c i N, to może obliczyć d' za pomocą

Jeżeli zatem Ewa przechwyci zakodowaną wiadomość b oraz zna ogłoszone publicznie liczby c i N, to może obliczyć d' za pomocą

$$cd' = 1 \mod N \,. \tag{8}$$

Następnie Ewa wykonuje obliczenia

Jeżeli zatem Ewa przechwyci zakodowaną wiadomość b oraz zna ogłoszone publicznie liczby c i N, to może obliczyć d' za pomocą

$$cd' = 1 \mod N \,. \tag{8}$$

Następnie Ewa wykonuje obliczenia

$$\begin{aligned} b^{d'} \mod N &= a^{cd'} \mod N = a^{1+mr} \mod N &(9)\\ &= a(a^r)^m \mod N = a \mod N \,. &(10)\end{aligned}$$

Jeżeli zatem Ewa przechwyci zakodowaną wiadomość b oraz zna ogłoszone publicznie liczby c i N, to może obliczyć d' za pomocą

$$cd' = 1 \mod N \,. \tag{8}$$

Następnie Ewa wykonuje obliczenia

$$\begin{aligned} b^{d'} \mod N &= a^{cd'} \mod N = a^{1+mr} \mod N &(9)\\ &= a(a^r)^m \mod N = a \mod N \,. &(10)\end{aligned}$$

Na podstawie ostatniej równości w (9) Ewa otrzymuje oryginalną wiadomość a.

Jeżeli zatem Ewa przechwyci zakodowaną wiadomość b oraz zna ogłoszone publicznie liczby c i N, to może obliczyć d' za pomocą

$$cd' = 1 \mod N \,. \tag{8}$$

Następnie Ewa wykonuje obliczenia

$$\begin{aligned} b^{d'} \mod N &= a^{cd'} \mod N = a^{1+mr} \mod N &(9)\\ &= a(a^r)^m \mod N = a \mod N \,. &(10)\end{aligned}$$

Na podstawie ostatniej równości w (9) Ewa otrzymuje oryginalną wiadomość a.

Uwaga: W obliczeniach (8, 9) wykorzystano własność rzędu modulo N liczby a

$$a^r = 1 \mod N \,.$$

Prosty przykład liczbowy (c.d.)

Prosty przykład liczbowy (c.d.)

Za pomocą algorytmu Shora Ewa znajduje, że właściwym rzędem jest $r = 21$.

Prosty przykład liczbowy (c.d.)

Za pomocą algorytmu Shora Ewa znajduje, że właściwym rzędem jest $r = 21$.
Następnie Ewa oblicza d' jako odwrotność liczby $c = 5$ względem operacji modulo 21, czyli

Prosty przykład liczbowy (c.d.)

Za pomocą algorytmu Shora Ewa znajduje, że właściwym rzędem jest $r = 21$.
Następnie Ewa oblicza d' jako odwrotność liczby $c = 5$ względem operacji modulo 21, czyli

$$cd' = 5 \times d' = 1 \mod 21 \, .$$

Prosty przykład liczbowy (c.d.)

Za pomocą algorytmu Shora Ewa znajduje, że właściwym rzędem jest $r = 21$.
Następnie Ewa oblicza d' jako odwrotność liczby $c = 5$ względem operacji modulo 21, czyli

$$cd' = 5 \times d' = 1 \mod 21 \, .$$

Stąd $d' = 17$, ponieważ $5 \times 17 = 85 = 1 + 4 \times 21$.

Prosty przykład liczbowy (c.d.)

Za pomocą algorytmu Shora Ewa znajduje, że właściwym rzędem jest $r = 21$.
Następnie Ewa oblicza d' jako odwrotność liczby $c = 5$ względem operacji modulo 21, czyli

$$cd' = 5 \times d' = 1 \mod 21 \, .$$

Stąd $d' = 17$, ponieważ $5 \times 17 = 85 = 1 + 4 \times 21$.
W kolejnym kroku Ewa oblicza

Prosty przykład liczbowy (c.d.)

Za pomocą algorytmu Shora Ewa znajduje, że właściwym rzędem jest $r = 21$.
Następnie Ewa oblicza d' jako odwrotność liczby $c = 5$ względem operacji modulo 21, czyli

$$cd' = 5 \times d' = 1 \mod 21 \, .$$

Stąd $d' = 17$, ponieważ $5 \times 17 = 85 = 1 + 4 \times 21$.
W kolejnym kroku Ewa oblicza

$$b^{d'} \mod N = 16^{17} \mod 21 = 4 \, .$$

Prosty przykład liczbowy (c.d.)

Za pomocą algorytmu Shora Ewa znajduje, że właściwym rzędem jest $r = 21$.
Następnie Ewa oblicza d' jako odwrotność liczby $c = 5$ względem operacji modulo 21, czyli

$$cd' = 5 \times d' = 1 \mod 21 \, .$$

Stąd $d' = 17$, ponieważ $5 \times 17 = 85 = 1 + 4 \times 21$.
W kolejnym kroku Ewa oblicza

$$b^{d'} \mod N = 16^{17} \mod 21 = 4 \, .$$

A zatem Ewa odczytuje oryginalną wiadomość $a = 4$.

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**.

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.

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.

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.

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:

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**.

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.

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.**

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

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

Dowód

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

Dowód

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

$$\langle\varphi|\psi\rangle = C \neq 0 \; . \tag{11}$$

Dowód

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

$$\langle\varphi|\psi\rangle = C \neq 0 \; . \tag{11}$$

Ponadto oczywiście $C \neq 1$.

Dowód

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

$$\langle\varphi|\psi\rangle = C \neq 0 \,. \tag{11}$$

Ponadto oczywiście $C \neq 1$.

Proces uzyskiwania informacji kwantowej można zaimplementować przy użyciu układu pomocniczego, który zostaje spreparowany w pewnym standardowym stanie $|u\rangle$.

Dowód

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

$$\langle\varphi|\psi\rangle = C \neq 0 \,. \tag{11}$$

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

Dla obu stanów otrzymujemy zatem

$$\begin{aligned} |\varphi\rangle|u\rangle &\xrightarrow{U} |\varphi\rangle|v\rangle \\ |\psi\rangle|u\rangle &\xrightarrow{U} |\psi\rangle|v'\rangle \ . \end{aligned} \tag{12}$$

Dla obu stanów otrzymujemy zatem

$$\begin{aligned} |\varphi\rangle|u\rangle &\xrightarrow{U} |\varphi\rangle|v\rangle \\ |\psi\rangle|u\rangle &\xrightarrow{U} |\psi\rangle|v'\rangle \ . \end{aligned} \tag{12}$$

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

Jednakże transformacje unitarne nie zmieniają iloczynów skalarnych, otrzymujemy więc

$$\langle v|v'\rangle\langle\varphi|\psi\rangle = \langle u|u\rangle\langle\varphi|\psi\rangle \ . \tag{13}$$

Jednakże transformacje unitarne nie zmieniają iloczynów skalarnych, otrzymujemy więc

$$\langle v|v'\rangle\langle\varphi|\psi\rangle = \langle u|u\rangle\langle\varphi|\psi\rangle \; . \tag{13}$$

Wynika stąd, że

$$\langle v|v'\rangle = \langle u|u\rangle = 1 \; . \tag{14}$$

Jednakże transformacje unitarne nie zmieniają iloczynów skalarnych, otrzymujemy więc

$$\langle v|v'\rangle\langle\varphi|\psi\rangle = \langle u|u\rangle\langle\varphi|\psi\rangle \ . \tag{13}$$

Wynika stąd, że

$$\langle v|v'\rangle = \langle u|u\rangle = 1 \ . \tag{14}$$

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

Jednakże transformacje unitarne nie zmieniają iloczynów skalarnych, otrzymujemy więc

$$\langle v|v'\rangle\langle\varphi|\psi\rangle = \langle u|u\rangle\langle\varphi|\psi\rangle \ . \tag{13}$$

Wynika stąd, że

$$\langle v|v'\rangle = \langle u|u\rangle = 1 \ . \tag{14}$$

A zatem stany $|v\rangle$ i $|v'\rangle$ muszą być identyczne.
Stany te mogłyby się różnić wyłącznie wtedy, gdyby w wyniku operacji (12) co najmniej jeden z przechwyconych kubitów ($|\varphi\rangle$ lub $|\psi\rangle$) uległ zmianie,

Jednakże transformacje unitarne nie zmieniają iloczynów skalarnych, otrzymujemy więc

$$\langle v|v'\rangle\langle\varphi|\psi\rangle = \langle u|u\rangle\langle\varphi|\psi\rangle \ . \tag{13}$$

Wynika stąd, że

$$\langle v|v'\rangle = \langle u|u\rangle = 1 \ . \tag{14}$$

A zatem stany $|v\rangle$ i $|v'\rangle$ muszą być identyczne.
Stany te mogłyby się różnić wyłącznie wtedy, gdyby w wyniku operacji (12) co najmniej jeden z przechwyconych kubitów ($|\varphi\rangle$ lub $|\psi\rangle$) uległ zmianie, ale to oznaczałoby zaburzenie przynajmniej jednego z kubitów.

Jednakże transformacje unitarne nie zmieniają iloczynów skalarnych, otrzymujemy więc

$$\langle v|v'\rangle\langle\varphi|\psi\rangle = \langle u|u\rangle\langle\varphi|\psi\rangle \ . \tag{13}$$

Wynika stąd, że

$$\langle v|v'\rangle = \langle u|u\rangle = 1 \ . \tag{14}$$

A zatem stany $|v\rangle$ i $|v'\rangle$ muszą być identyczne.
Stany te mogłyby się różnić wyłącznie wtedy, gdyby w wyniku operacji (12) 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.

Jednakże transformacje unitarne nie zmieniają iloczynów skalarnych, otrzymujemy więc

$$\langle v|v'\rangle\langle\varphi|\psi\rangle = \langle u|u\rangle\langle\varphi|\psi\rangle \ . \tag{13}$$

Wynika stąd, że

$$\langle v|v'\rangle = \langle u|u\rangle = 1 \ . \tag{14}$$

A zatem stany $|v\rangle$ i $|v'\rangle$ muszą być identyczne.
Stany te mogłyby się różnić wyłącznie wtedy, gdyby w wyniku operacji (12) 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.

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.

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.

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.

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.

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.

Procedury postępowania w celu uzyskania bezpiecznej transmisji danych zawarte są w opracowanych protokołach kwantowej dystrybucji klucza.
Omówię dwa spośród tych protokołów.

Protokół BB84

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.

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:

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

$$|\psi_{00}\rangle = |0\rangle \ , \tag{15}$$

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

$$|\psi_{00}\rangle = |0\rangle \ , \tag{15}$$

$$|\psi_{10}\rangle = |1\rangle \ , \tag{16}$$

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

$$|\psi_{00}\rangle = |0\rangle \ , \tag{15}$$

$$|\psi_{10}\rangle = |1\rangle \ , \tag{16}$$

$$|\psi_{01}\rangle \equiv |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \ , \tag{17}$$

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

$$|\psi_{00}\rangle = |0\rangle \,, \tag{15}$$

$$|\psi_{10}\rangle = |1\rangle \,, \tag{16}$$

$$|\psi_{01}\rangle \equiv |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \,, \tag{17}$$

$$|\psi_{11}\rangle \equiv |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \,. \tag{18}$$

Stany (15) i (16) są stanami własnymi operatora Pauliego $Z \equiv \sigma_z$ odpowiednio do wartości własnych $+1$ i -1.

Stany (15) i (16) są stanami własnymi operatora Pauliego $Z \equiv \sigma_z$ odpowiednio do wartości własnych $+1$ i -1. Można łatwo sprawdzić, że stany (17) i (18) 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 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

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

$$|\Psi_A\rangle = \bigotimes_{k=1}^{(4+\Delta)n} |\psi_{a_k b_k}\rangle \, . \tag{19}$$

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

$$|\Psi_A\rangle = \bigotimes_{k=1}^{(4+\Delta)n} |\psi_{a_k b_k}\rangle \, . \tag{19}$$

We wzorze (19) 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.

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 (15), (16), (17) i (18) nie są wzajemnie ortogonalne, czyli żaden pomiar nie może rozróżnić wszystkich tych stanów.

Etap II.

Etap II.

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

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

Kubit otrzymany przez Bartka można zapisać w jawnej postaci jako

$$|\Psi_B\rangle = \sum_c \langle\psi_c|\Psi_A\rangle|\psi_c\rangle + \sum_i \langle\eta_i|\Psi_A\rangle|\eta_i\rangle \ , \tag{20}$$

Kubit otrzymany przez Bartka można zapisać w jawnej postaci jako

$$|\Psi_B\rangle = \sum_c \langle\psi_c|\Psi_A\rangle|\psi_c\rangle + \sum_i \langle\eta_i|\Psi_A\rangle|\eta_i\rangle \ , \tag{20}$$

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

Kubit otrzymany przez Bartka można zapisać w jawnej postaci jako

$$|\Psi_B\rangle = \sum_c \langle\psi_c|\Psi_A\rangle|\psi_c\rangle + \sum_i \langle\eta_i|\Psi_A\rangle|\eta_i\rangle \ , \tag{20}$$

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 (20). Zna jedynie stan wynikowy $|\Psi_B\rangle$.

Kubit otrzymany przez Bartka można zapisać w jawnej postaci jako

$$|\Psi_B\rangle = \sum_c \langle\psi_c|\Psi_A\rangle|\psi_c\rangle + \sum_i \langle\eta_i|\Psi_A\rangle|\eta_i\rangle \ , \tag{20}$$

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 (20). 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 $|\Psi_B\rangle$.

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 $|\eta_i\rangle$).

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.

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.

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.

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.

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.

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.

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'.

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).

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.

Etap IV.

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

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.

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

$$a' = a \ , \tag{21}$$

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

$$a' = a \ , \tag{21}$$

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

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

$$a' = a \ , \tag{21}$$

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.

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

$$a' = a \ , \tag{21}$$

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.

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.

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.

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.

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.

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.

Protokół EPR

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

Zasada działania protokołu EPR

Zasada działania protokołu EPR

Krok I.

Zasada działania protokołu EPR

Krok I.

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

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \, . \tag{22}$$

Sposoby produkcji zbioru splątanych kubitów:

Sposoby produkcji zbioru splątanych kubitów:

- Alicja może spreparować n stanów splątanych, a następnie wysłać połowę z nich do Bartka

Sposoby produkcji zbioru splątanych kubitów:

- Alicja może spreparować n stanów splątanych, a następnie wysłać połowę z nich do Bartka lub *vice versa*,

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,

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.

Krok II.

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

Krok II.

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

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle \leqslant 2\ . \tag{23}$$

Krok II.

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

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle \leqslant 2\,. \tag{23}$$

Przypominam, że w nierówności (23) 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.

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.

Krok III.

Alicja i Bartek dokonują pomiarów wielkości Q, R, S, T we wspólnie określonej przypadkowej bazie.

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.

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.

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

Dyskusja

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

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.

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**.

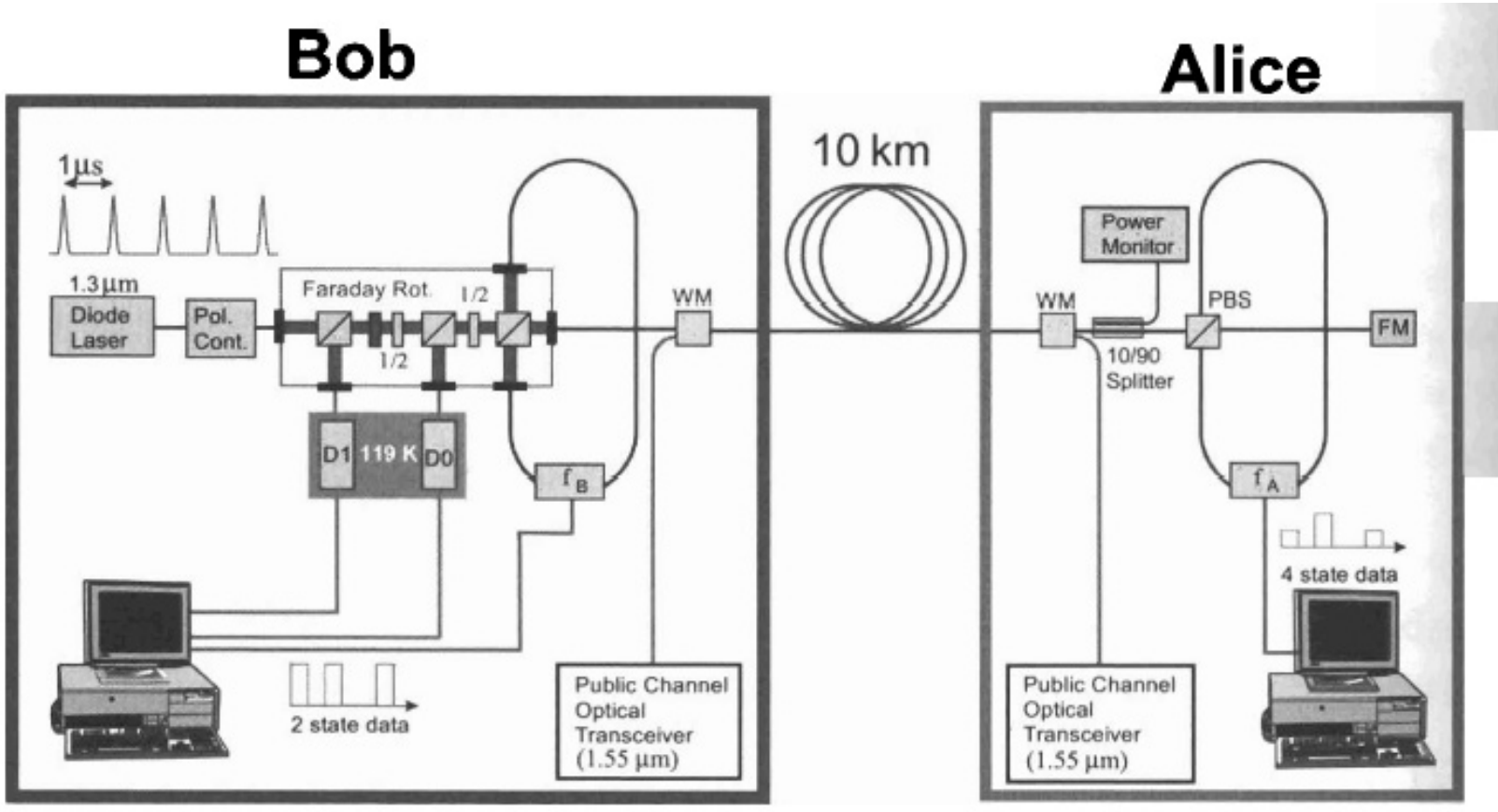
Dyskusja

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**.

Eksperymentalna realizacja kwantowej dystrybucji klucza

Rysunek 9.3 pokazuje schemat układu komercyjnego, służącego do kwantowej dystrybucji klucza, zbudowanego w IBM na bazie światłowodów.



Rysunek: 9.3. Schemat układu, za pomocą którego zrealizowano kwantową dystrybucję klucza.

Opis realizacji protokołu BB84:

Opis realizacji protokołu BB84:

- Najpierw Bartek generuje koheretne stany światła za pomocą lasera emitującego światło o długości fali 1.3 μm.

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.

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 (15), (17), (16), (18) używanymi w protokole BB84.

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 (15), (17), (16), (18) 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).

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 (15), (17), (16), (18) 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.

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 (15), (17), (16), (18) 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.

c.d.

- Bartek mierzy polaryzację fotonu za pomocą analizatora ustawionego używając w tym celu wybranych w sposób przypadkowy stanów bazy (15), (17), (16), (18).

c.d.

- Bartek mierzy polaryzację fotonu za pomocą analizatora ustawionego używając w tym celu wybranych w sposób przypadkowy stanów bazy (15), (17), (16), (18).
- Alicja i Bartek stosują do przesyłania fotonu specjalną konfigurację, w której foton przebywa dwukrotnie tę samą trajektorię.

c.d.

- Bartek mierzy polaryzację fotonu za pomocą analizatora ustawionego używając w tym celu wybranych w sposób przypadkowy stanów bazy (15), (17), (16), (18).
- Alicja i Bartek stosują do przesyłania fotonu specjalną konfigurację, w której foton przebywa dwukrotnie tę samą trajektorię. Dzięki temu następuje autokompensacja błędów, wynikających np. z powolnych fluktuacji długości trajektorii czy przesunięć kierunków polaryzacji.

c.d.

- Bartek mierzy polaryzację fotonu za pomocą analizatora ustawionego używając w tym celu wybranych w sposób przypadkowy stanów bazy (15), (17), (16), (18).
- Alicja i Bartek stosują do przesyłania fotonu specjalną konfigurację, 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.

c.d.

- Bartek mierzy polaryzację fotonu za pomocą analizatora ustawionego używając w tym celu wybranych w sposób przypadkowy stanów bazy (15), (17), (16), (18).
- Alicja i Bartek stosują do przesyłania fotonu specjalną konfigurację, 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.

c.d.

- Bartek mierzy polaryzację fotonu za pomocą analizatora ustawionego używając w tym celu wybranych w sposób przypadkowy stanów bazy (15), (17), (16), (18).
- Alicja i Bartek stosują do przesyłania fotonu specjalną konfigurację, 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.

† 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.

† 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.