Kryptografia

z elementami kryptografii kwantowej

Ryszard Tanaś

http://zon8.physd.amu.edu.pl/~tanas

Wykład 14

Spis treści

20 Kryptografia kwantowa

20.1 Protokół BB84 (Bennett, Brassard, 1984)

- Wybierzmy dwie ortonormalne bazy dla pomiaru polaryzacji fotonu:

  Baza prosta $(+)$

  Tworzą ją dwa stany o polaryzacji poziomej oraz pionowej

  $\{|\rightarrow\rangle, |\uparrow\rangle\}$

  Baza ukośna $(\times)$

  Tworzą ją dwa stany o polaryzacji 45° oraz polaryzacji 135°

  $\{|\nearrow\rangle, |\nwarrow\rangle\}$

20 Kryptografia kwantowa

20.1 Protokół BB84 (Bennett, Brassard, 1984)

- Wybierzmy dwie ortonormalne bazy dla pomiaru polaryzacji fotonu:

  Baza prosta $(+)$

  Tworzą ją dwa stany o polaryzacji poziomej oraz pionowej

  $\{|\rightarrow\rangle, |\uparrow\rangle\}$

  Baza ukośna $(\times)$

  Tworzą ją dwa stany o polaryzacji 45° oraz polaryzacji 135°

  $\{|\nearrow\rangle, |\nwarrow\rangle\}$

20 Kryptografia kwantowa

20.1 Protokół BB84 (Bennett, Brassard, 1984)

- Wybierzmy dwie ortonormalne bazy dla pomiaru polaryzacji fotonu:

  Baza prosta $(+)$

  Tworzą ją dwa stany o polaryzacji poziomej oraz pionowej

  $\{|\rightarrow\rangle, |\uparrow\rangle\}$

  Baza ukośna $(\times)$

  Tworzą ją dwa stany o polaryzacji 45° oraz polaryzacji 135°

  $\{|\nearrow\rangle, |\nwarrow\rangle\}$

20 Kryptografia kwantowa

20.1 Protokół BB84 (Bennett, Brassard, 1984)

- Wybierzmy dwie ortonormalne bazy dla pomiaru polaryzacji fotonu:

  Baza prosta $(+)$

  Tworzą ją dwa stany o polaryzacji poziomej oraz pionowej

  $\{|\rightarrow\rangle, |\uparrow\rangle\}$

  Baza ukośna $(\times)$

  Tworzą ją dwa stany o polaryzacji 45° oraz polaryzacji 135°

  $\{|\nearrow\rangle, |\nwarrow\rangle\}$

- Zachodzą następujące relacje

$$
\begin{aligned}
|\nearrow\rangle &= \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle + |\uparrow\rangle\right) \\
|\nwarrow\rangle &= -\frac{1}{\sqrt{2}}\left(|\rightarrow\rangle - |\uparrow\rangle\right) \\
|\rightarrow\rangle &= \frac{1}{\sqrt{2}}\left(|\nearrow\rangle - |\nwarrow\rangle\right) \\
|\uparrow\rangle &= \frac{1}{\sqrt{2}}\left(|\nearrow\rangle + |\nwarrow\rangle\right)
\end{aligned}
$$

- Wynika z nich, że pomiar polaryzacji fotonu "ukośnego" w bazie prostej daje z prawdopodobieństwem $1/2$ stan $|\rightarrow\rangle$ lub $|\uparrow\rangle$, co oznacza, że pomiar taki nie daje żadnych informacji o polaryzacji fotonu.

- Zachodzą następujące relacje

$$
\begin{aligned}
|\nearrow\rangle &= \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle + |\uparrow\rangle\right) \\
|\nwarrow\rangle &= -\frac{1}{\sqrt{2}}\left(|\rightarrow\rangle - |\uparrow\rangle\right) \\
|\rightarrow\rangle &= \frac{1}{\sqrt{2}}\left(|\nearrow\rangle - |\nwarrow\rangle\right) \\
|\uparrow\rangle &= \frac{1}{\sqrt{2}}\left(|\nearrow\rangle + |\nwarrow\rangle\right)
\end{aligned}
$$

- Wynika z nich, że pomiar polaryzacji fotonu "ukośnego" w bazie prostej daje z prawdopodobieństwem $1/2$ stan $|\rightarrow\rangle$ lub $|\uparrow\rangle$, co oznacza, że pomiar taki nie daje żadnych informacji o polaryzacji fotonu.

- Zachodzą następujące relacje

$$
\begin{aligned}
|\nearrow\rangle &= \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle + |\uparrow\rangle\right) \\
|\nwarrow\rangle &= -\frac{1}{\sqrt{2}}\left(|\rightarrow\rangle - |\uparrow\rangle\right) \\
|\rightarrow\rangle &= \frac{1}{\sqrt{2}}\left(|\nearrow\rangle - |\nwarrow\rangle\right) \\
|\uparrow\rangle &= \frac{1}{\sqrt{2}}\left(|\nearrow\rangle + |\nwarrow\rangle\right)
\end{aligned}
$$

- Wynika z nich, że pomiar polaryzacji fotonu "ukośnego" w bazie prostej daje z prawdopodobieństwem $1/2$ stan $|\rightarrow\rangle$ lub $|\uparrow\rangle$, co oznacza, że pomiar taki nie daje żadnych informacji o polaryzacji fotonu.

- To samo możemy powiedzieć o pomiarze fotonu “prostego” w bazie ukośnej.
- Polaryzacja prosta i polaryzacja ukośna to dwie wielkości fizyczne, które zgodnie z prawami mechaniki kwantowej nie są współmierzalne. Obowiązuje tutaj zasada nieoznaczoności Heisenberga.

- To samo możemy powiedzieć o pomiarze fotonu "prostego" w bazie ukośnej.
- Polaryzacja prosta i polaryzacja ukośna to dwie wielkości fizyczne, które zgodnie z prawami mechaniki kwantowej nie są współmierzalne. Obowiązuje tutaj zasada nieoznaczoności Heisenberga.

- Mając dwie bazy możemy stworzyć dwa kwantowe alfabety przypisując dwóm ortogonalnym stanom bazy wartości binarne 0 i 1.

Alfabet prosty

$$|\rightarrow\rangle \equiv 0$$
$$|\uparrow\rangle \equiv 1$$

Alfabet ukośny

$$|\nearrow\rangle \equiv 0$$
$$|\nwarrow\rangle \equiv 1$$

- Mając dwie bazy możemy stworzyć dwa kwantowe alfabety przypisując dwóm ortogonalnym stanom bazy wartości binarne 0 i 1.

Alfabet prosty

$$|\rightarrow\rangle \equiv 0$$
$$|\uparrow\rangle \equiv 1$$

Alfabet ukośny

$$|\nearrow\rangle \equiv 0$$
$$|\nwarrow\rangle \equiv 1$$

- Mając dwie bazy możemy stworzyć dwa kwantowe alfabety przypisując dwóm ortogonalnym stanom bazy wartości binarne 0 i 1.

Alfabet prosty

$$|\rightarrow\rangle \equiv 0$$
$$|\uparrow\rangle \equiv 1$$

Alfabet ukośny

$$|\nearrow\rangle \equiv 0$$
$$|\nwarrow\rangle \equiv 1$$

20.1.1 Etapy BB84

1. Alicja wybiera losowo jedną z dwóch baz i jedną z dwóch ortogonalnych polaryzacji w wybranej bazie, co oznacza wybór jednej z czterech możliwych polaryzacji i wysyła do Bolka foton o takiej polaryzacji. Zgodnie z przyjętymi alfabetami oznacza to odpowiadający wybranym polaryzacjom ciąg bitów.
2. Bolek losowo wybiera bazę prostą lub ukośną i wykonuje pomiar polaryzacji fotonu, który otrzymał od Alicji
3. Bolek notuje wyniki pomiarów zachowując je w tajemnicy

20.1.1 Etapy BB84

1. Alicja wybiera losowo jedną z dwóch baz i jedną z dwóch ortogonalnych polaryzacji w wybranej bazie, co oznacza wybór jednej z czterech możliwych polaryzacji i wysyła do Bolka foton o takiej polaryzacji. Zgodnie z przyjętymi alfabetami oznacza to odpowiadający wybranym polaryzacjom ciąg bitów.
2. Bolek losowo wybiera bazę prostą lub ukośną i wykonuje pomiar polaryzacji fotonu, który otrzymał od Alicji
3. Bolek notuje wyniki pomiarów zachowując je w tajemnicy

20.1.1 Etapy BB84

1. Alicja wybiera losowo jedną z dwóch baz i jedną z dwóch ortogonalnych polaryzacji w wybranej bazie, co oznacza wybór jednej z czterech możliwych polaryzacji i wysyła do Bolka foton o takiej polaryzacji. Zgodnie z przyjętymi alfabetami oznacza to odpowiadający wybranym polaryzacjom ciąg bitów.
2. Bolek losowo wybiera bazę prostą lub ukośną i wykonuje pomiar polaryzacji fotonu, który otrzymał od Alicji
3. Bolek notuje wyniki pomiarów zachowując je w tajemnicy

20.1.1 Etapy BB84

1. Alicja wybiera losowo jedną z dwóch baz i jedną z dwóch ortogonalnych polaryzacji w wybranej bazie, co oznacza wybór jednej z czterech możliwych polaryzacji i wysyła do Bolka foton o takiej polaryzacji. Zgodnie z przyjętymi alfabetami oznacza to odpowiadający wybranym polaryzacjom ciąg bitów.
2. Bolek losowo wybiera bazę prostą lub ukośną i wykonuje pomiar polaryzacji fotonu, który otrzymał od Alicji
3. Bolek notuje wyniki pomiarów zachowując je w tajemnicy

4. Bolek publicznie informuje Alicję jakiej bazy używał, zaś Alicja informuje go czy była to baza właściwa czy nie.

5. Alicja i Bolek przechowują wyniki, dla których Bolek użył właściwej bazy. Przypisując tym wynikom wartości binarne 0 i 1 zgodnie z przyjętymi alfabetami oboje otrzymują taki sam ciąg zer i jedynek (losowy), który może służyć jako klucz kryptograficzny

4. Bolek publicznie informuje Alicję jakiej bazy używał, zaś Alicja informuje go czy była to baza właściwa czy nie.

5. Alicja i Bolek przechowują wyniki, dla których Bolek użył właściwej bazy. Przypisując tym wynikom wartości binarne 0 i 1 zgodnie z przyjętymi alfabetami oboje otrzymują taki sam ciąg zer i jedynek (losowy), który może służyć jako klucz kryptograficzny

Przykład:

Alicja	+	×	+	×	×	+	×	×	×	+	+	+	×
	↑	↗	→	↗	↖	→	↖	↖	↗	↑	↑	↑	↗
	1	0	0	0	1	0	1	1	0	1	1	1	0
Bolek	+	+	×	+	×	×	×	+	×	+	+	×	×
	↑	→	↗	↑	↖	↗	↖	→	↗	↑	↑	↖	↗
	1	0	0	1	1	0	1	0	0	1	1	1	0
A/B	√				√		√		√	√	√		√
klucz	1				1		1		0	1	1		0

- Porównując bity wysłane przez Alicję z bitami zarejestrowanymi przez Bolka możemy podzielić bity zarejestrowane przez Bolka na trzy kategorie:
  - bity pewne (średnio 50 %) — te dla których Bolek wybrał prawidłową bazę i które mogą być traktowane jako klucz kryptograficzny;
  - bity prawidłowe pomimo złego wyboru bazy (średnio 25 %);
  - bity nieprawidłowe (średnio 25 %).

- Porównując bity wysłane przez Alicję z bitami zarejestrowanymi przez Bolka możemy podzielić bity zarejestrowane przez Bolka na trzy kategorie:
  - bity pewne (średnio 50 %) — te dla których Bolek wybrał prawidłową bazę i które mogą być traktowane jako klucz kryptograficzny;
  - bity prawidłowe pomimo złego wyboru bazy (średnio 25 %);
  - bity nieprawidłowe (średnio 25 %).

- Porównując bity wysłane przez Alicję z bitami zarejestrowanymi przez Bolka możemy podzielić bity zarejestrowane przez Bolka na trzy kategorie:
  - bity pewne (średnio 50 %) — te dla których Bolek wybrał prawidłową bazę i które mogą być traktowane jako klucz kryptograficzny;
  - bity prawidłowe pomimo złego wyboru bazy (średnio 25 %);
  - bity nieprawidłowe (średnio 25 %).

- Porównując bity wysłane przez Alicję z bitami zarejestrowanymi przez Bolka możemy podzielić bity zarejestrowane przez Bolka na trzy kategorie:
  - bity pewne (średnio 50 %) — te dla których Bolek wybrał prawidłową bazę i które mogą być traktowane jako klucz kryptograficzny;
  - bity prawidłowe pomimo złego wyboru bazy (średnio 25 %);
  - bity nieprawidłowe (średnio 25 %).

- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $1/2$, prawdopodobieństwo zarejestrowania prawidłowej polaryzacji przy prawidłowym wyborze bazy wynosi 1, prawdopodobieństwo pomiaru prawidłowej polaryzacji przy nieprawidłowo wybranej bazie wynosi $1/2$,
- zatem prawdopodobieństwo tego, że zarejestrowany bit będzie prawidłowy (taki sam jak bit wysłany) jest równe $\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$.
- Prawdopodobieństwo zarejestrowania bitu nieprawidłowego (błędnego) wynosi więc $1 - \frac{3}{4} = \frac{1}{4}$.

- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $1/2$, prawdopodobieństwo zarejestrowania prawidłowej polaryzacji przy prawidłowym wyborze bazy wynosi 1, prawdopodobieństwo pomiaru prawidłowej polaryzacji przy nieprawidłowo wybranej bazie wynosi $1/2$,
- zatem prawdopodobieństwo tego, że zarejestrowany bit będzie prawidłowy (taki sam jak bit wysłany) jest równe $\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$.
- Prawdopodobieństwo zarejestrowania bitu nieprawidłowego (błędnego) wynosi więc $1 - \frac{3}{4} = \frac{1}{4}$.

- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $1/2$, prawdopodobieństwo zarejestrowania prawidłowej polaryzacji przy prawidłowym wyborze bazy wynosi 1, prawdopodobieństwo pomiaru prawidłowej polaryzacji przy nieprawidłowo wybranej bazie wynosi $1/2$,
- zatem prawdopodobieństwo tego, że zarejestrowany bit będzie prawidłowy (taki sam jak bit wysłany) jest równe $\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$.
- Prawdopodobieństwo zarejestrowania bitu nieprawidłowego (błędnego) wynosi więc $1 - \frac{3}{4} = \frac{1}{4}$.

Alicja	+	×	+	×	×	+	×	×	×	+	+	+	×
	↑	↗	→	↗	↖	→	↖	↖	↗	↑	↑	↑	↗
	1	0	0	0	1	0	1	1	0	1	1	1	0
Bolek	+	+	×	+	×	×	×	+	×	+	+	×	×
	↑	→	↗	↑	↖	↗	↖	→	↗	↑	↑	↖	↗
	1	0	0	1	1	0	1	0	0	1	1	1	0
pewne	1				1		1		0	1	1		0
dobre		0	0			0						1	
złe				1				0					

- Jeśli Ewa podsłuchuje stosując strategię tzw. nieprzeźroczystego podsłuchu, to wybiera losowo bazę prostą lub ukośną, dokonuje pomiaru polaryzacji w tej bazie i następnie przesyła do Bolka foton o takiej polaryzacji jaką zmierzyła.
- Dokonywane przez Ewę pomiary muszą wprowadzić błędy, które Alicja i Bolek mogą wykryć przy uzgadnianiu klucza.
- W podanym niżej przykładzie ostatni bit klucza został zmieniony. Średnio 25% bitów klucza zostanie zmienionych.

- Jeśli Ewa podsłuchuje stosując strategię tzw. nieprzeźroczystego podsłuchu, to wybiera losowo bazę prostą lub ukośną, dokonuje pomiaru polaryzacji w tej bazie i następnie przesyła do Bolka foton o takiej polaryzacji jaką zmierzyła.
- Dokonywane przez Ewę pomiary muszą wprowadzić błędy, które Alicja i Bolek mogą wykryć przy uzgadnianiu klucza.
- W podanym niżej przykładzie ostatni bit klucza został zmieniony. Średnio 25% bitów klucza zostanie zmienionych.

- Jeśli Ewa podsłuchuje stosując strategię tzw. nieprzeźroczystego podsłuchu, to wybiera losowo bazę prostą lub ukośną, dokonuje pomiaru polaryzacji w tej bazie i następnie przesyła do Bolka foton o takiej polaryzacji jaką zmierzyła.
- Dokonywane przez Ewę pomiary muszą wprowadzić błędy, które Alicja i Bolek mogą wykryć przy uzgadnianiu klucza.
- W podanym niżej przykładzie ostatni bit klucza został zmieniony. Średnio 25% bitów klucza zostanie zmienionych.

Alicja	+	×	+	×	×	+	×	×	×	+	+	+	×
	↑	↗	→	↗	↖	→	↖	↖	↗	↑	↑	↑	↗
	1	0	0	0	1	0	1	1	0	1	1	1	0
Ewa	+	+	+	×	+	×	+	×	+	+	+	×	+
	↑	→	→	↗	→	↗	↑	↖	↑	↑	↑	↖	→
	1	0	0	0	0	0	1	1	1	1	1	1	0
Bolek	+	+	×	+	×	×	×	+	×	+	+	×	×
	↑	→	↗	↑	↖	↗	↖	→	↗	↑	↑	↖	↖
	1	0	0	1	1	0	1	0	0	1	1	1	1
klucz	1				1		1		0	1	1		1

- Takie błędy Alicja i Bolek mogą wykryć wybierając losowo pewną liczbę bitów klucza i porównując publicznym kanałem ich wartości. Te bity oczywiście następnie się wyrzuca.
- Jeśli liczba błędów przekracza założony poziom to uznaje się, że kanał był podsłuchiwany i procedurę uzgadniania klucza rozpoczyna się od nowa.
- Mechanika kwantowa nie dopuszcza możliwości pasywnego podsłuchu. Bezpieczeństwo kwantowego systemu kryptograficznego gwarantowane jest przez prawa fizyki!

- Takie błędy Alicja i Bolek mogą wykryć wybierając losowo pewną liczbę bitów klucza i porównując publicznym kanałem ich wartości. Te bity oczywiście następnie się wyrzuca.
- Jeśli liczba błędów przekracza założony poziom to uznaje się, że kanał był podsłuchiwany i procedurę uzgadniania klucza rozpoczyna się od nowa.
- Mechanika kwantowa nie dopuszcza możliwości pasywnego podsłuchu. Bezpieczeństwo kwantowego systemu kryptograficznego gwarantowane jest przez prawa fizyki!

- Takie błędy Alicja i Bolek mogą wykryć wybierając losowo pewną liczbę bitów klucza i porównując publicznym kanałem ich wartości. Te bity oczywiście następnie się wyrzuca.
- Jeśli liczba błędów przekracza założony poziom to uznaje się, że kanał był podsłuchiwany i procedurę uzgadniania klucza rozpoczyna się od nowa.
- Mechanika kwantowa nie dopuszcza możliwości pasywnego podsłuchu. Bezpieczeństwo kwantowego systemu kryptograficznego gwarantowane jest przez prawa fizyki!

20.2 Protokół B92 (Bennett, 1992)

- W 1992 r. Charles Bennett zaproponował protokół wymiany klucza oparty na dwóch nieortogonalnych stanach kwantowych.
- Niech takimi stanami będą $\{|\rightarrow\rangle, |\nearrow\rangle\}$.
- Bolek wykonuje pomiary polaryzacji w stanach ortogonalnych do $\{|\rightarrow\rangle, |\nearrow\rangle\}$, tzn. w stanach $\{|\uparrow\rangle, |\nwarrow\rangle\}$.

20.2 Protokół B92 (Bennett, 1992)

- W 1992 r. Charles Bennett zaproponował protokół wymiany klucza oparty na dwóch nieortogonalnych stanach kwantowych.
- Niech takimi stanami będą $\{|\rightarrow\rangle, |\nearrow\rangle\}$.
- Bolek wykonuje pomiary polaryzacji w stanach ortogonalnych do $\{|\rightarrow\rangle, |\nearrow\rangle\}$, tzn. w stanach $\{|\uparrow\rangle, |\nwarrow\rangle\}$.

20.2 Protokół B92 (Bennett, 1992)

- W 1992 r. Charles Bennett zaproponował protokół wymiany klucza oparty na dwóch nieortogonalnych stanach kwantowych.
- Niech takimi stanami będą $\{|\rightarrow\rangle, |\nearrow\rangle\}$.
- Bolek wykonuje pomiary polaryzacji w stanach ortogonalnych do $\{|\rightarrow\rangle, |\nearrow\rangle\}$, tzn. w stanach $\{|\uparrow\rangle, |\nwarrow\rangle\}$.

20.2 Protokół B92 (Bennett, 1992)

- W 1992 r. Charles Bennett zaproponował protokół wymiany klucza oparty na dwóch nieortogonalnych stanach kwantowych.
- Niech takimi stanami będą $\{|\rightarrow\rangle, |\nearrow\rangle\}$.
- Bolek wykonuje pomiary polaryzacji w stanach ortogonalnych do $\{|\rightarrow\rangle, |\nearrow\rangle\}$, tzn. w stanach $\{|\uparrow\rangle, |\nwarrow\rangle\}$.

- **Alfabet kwantowy**

  Alicja przygotowuje fotony o polaryzacji horyzontalnej $|\rightarrow\rangle$ lub polaryzacji 45° $|\nearrow\rangle$ przypisując im wartości binarne

$$
\begin{aligned}
|\rightarrow\rangle &\equiv 0 \\
|\nearrow\rangle &\equiv 1
\end{aligned}
$$

20.2.1 Etapy B92

1. Alicja wybiera losowo jedną z dwóch polaryzacji $\{|\rightarrow\rangle, |\nearrow\rangle\}$ i przesyła do Bolka foton o takiej polaryzacji. Powtarzając tę procedurę, Alicja wysyła do Bolka losowy ciąg zer i jedynek.

2. Bolek losowo wybiera jeden ze stanów $\{|\uparrow\rangle, |\nwarrow\rangle\}$ i mierzy polaryzację w takim stanie. Jeśli wybrał polaryzację ortogonalną do polaryzacji wybranej przez Alicję, to nie zarejestruje fotonu. W przeciwnym razie z prawdopodobieństwem $1/2$ zarejestruje foton. Jeśli zarejestrował foton o polaryzacji $|\uparrow\rangle$ to przypisuje mu wartość binarną 1, zaś fotonowi o polaryzacji $|\nwarrow\rangle$ przypisuje wartość binarną 0.

20.2.1 Etapy B92

1. Alicja wybiera losowo jedną z dwóch polaryzacji $\{|\rightarrow\rangle, |\nearrow\rangle\}$ i przesyła do Bolka foton o takiej polaryzacji. Powtarzając tę procedurę, Alicja wysyła do Bolka losowy ciąg zer i jedynek.

2. Bolek losowo wybiera jeden ze stanów $\{|\uparrow\rangle, |\nwarrow\rangle\}$ i mierzy polaryzację w takim stanie. Jeśli wybrał polaryzację ortogonalną do polaryzacji wybranej przez Alicję, to nie zarejestruje fotonu. W przeciwnym razie z prawdopodobieństwem $1/2$ zarejestruje foton. Jeśli zarejestrował foton o polaryzacji $|\uparrow\rangle$ to przypisuje mu wartość binarną 1, zaś fotonowi o polaryzacji $|\nwarrow\rangle$ przypisuje wartość binarną 0.

20.2.1 Etapy B92

1. Alicja wybiera losowo jedną z dwóch polaryzacji $\{|\rightarrow\rangle, |\nearrow\rangle\}$ i przesyła do Bolka foton o takiej polaryzacji. Powtarzając tę procedurę, Alicja wysyła do Bolka losowy ciąg zer i jedynek.

2. Bolek losowo wybiera jeden ze stanów $\{|\uparrow\rangle, |\nwarrow\rangle\}$ i mierzy polaryzację w takim stanie. Jeśli wybrał polaryzację ortogonalną do polaryzacji wybranej przez Alicję, to nie zarejestruje fotonu. W przeciwnym razie z prawdopodobieństwem $1/2$ zarejestruje foton. Jeśli zarejestrował foton o polaryzacji $|\uparrow\rangle$ to przypisuje mu wartość binarną 1, zaś fotonowi o polaryzacji $|\nwarrow\rangle$ przypisuje wartość binarną 0.

3. Bolek przekazuje Alicji publicznym kanałem informację dla których fotonów uzyskał wynik pozytywny (T), czyli zarejestrował foton, ale nie zdradza jaką polaryzację zmierzył.

4 Alicja i Bolek przechowują ciąg bitów, dla których Bolek zarejestrował foton. Ciąg ten stanowi klucz kryptograficzny.

3. Bolek przekazuje Alicji publicznym kanałem informację dla których fotonów uzyskał wynik pozytywny (T), czyli zarejestrował foton, ale nie zdradza jaką polaryzację zmierzył.

4 Alicja i Bolek przechowują ciąg bitów, dla których Bolek zarejestrował foton. Ciąg ten stanowi klucz kryptograficzny.

Przykład:

Alicja	$\nearrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\nearrow$	$\rightarrow$	$\nearrow$	$\nearrow$	$\rightarrow$	$\nearrow$	$\nearrow$	$\nearrow$	$\rightarrow$
	1	0	0	0	1	0	1	1	0	1	1	1	0
Bolek	$\nwarrow$	$\nwarrow$	$\uparrow$	$\nwarrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\nwarrow$	$\uparrow$	$\nwarrow$	$\nwarrow$	$\uparrow$	$\uparrow$
	N	T	N	T	T	N	N	N	N	N	N	T	N
		0		0	1							1	
A/B		$\surd$		$\surd$	$\surd$							$\surd$	
klucz		0		0	1							1	

Przykład:

Alicja	$\nearrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\nearrow$	$\rightarrow$	$\nearrow$	$\nearrow$	$\rightarrow$	$\nearrow$	$\nearrow$	$\nearrow$	$\rightarrow$
	1	0	0	0	1	0	1	1	0	1	1	1	0
Bolek	$\nwarrow$	$\nwarrow$	$\uparrow$	$\nwarrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\nwarrow$	$\uparrow$	$\nwarrow$	$\nwarrow$	$\uparrow$	$\uparrow$
	N	T	N	T	T	N	N	N	N	N	N	T	N
		0		0	1							1	
A/B		$\surd$		$\surd$	$\surd$							$\surd$	
klucz		0		0	1							1	

Podobnie jak w przypadku protokołu BB84 obecność Ewy spowoduje błędy w kluczu, które Alicja i Bolek mogą wykryć.

- Kryptografia kwantowa szybko się rozwija. Tutaj przedstawiłem tylko najprostsze protokoły. Istnieją inne protokoły kwantowe uzgadniania klucza, np. protokół zaproponowany prze Ekerta w 1991 r oparty na zjawisku EPR. Do kodowania można używać np. fazy fotonu, a nie polaryzacji.
- Kryptografia kwantowa jest już faktem!.
- Grupa prof. Gisina w Genewie przeprowadziła udane eksperymenty z kwantową dystrybucją klucza na odległości 67 km, używając komercyjnych światłowodów. Trwają intensywne prace nad kwantową dystrybucją klucza w otwartej przestrzeni.

- Kryptografia kwantowa szybko się rozwija. Tutaj przedstawiłem tylko najprostsze protokoły. Istnieją inne protokoły kwantowe uzgadniania klucza, np. protokół zaproponowany prze Ekerta w 1991 r oparty na zjawisku EPR. Do kodowania można używać np. fazy fotonu, a nie polaryzacji.
- Kryptografia kwantowa jest już faktem!.
- Grupa prof. Gisina w Genewie przeprowadziła udane eksperymenty z kwantową dystrybucją klucza na odległości 67 km, używając komercyjnych światłowodów. Trwają intensywne prace nad kwantową dystrybucją klucza w otwartej przestrzeni.

- Kryptografia kwantowa szybko się rozwija. Tutaj przedstawiłem tylko najprostsze protokoły. Istnieją inne protokoły kwantowe uzgadniania klucza, np. protokół zaproponowany prze Ekerta w 1991 r oparty na zjawisku EPR. Do kodowania można używać np. fazy fotonu, a nie polaryzacji.
- Kryptografia kwantowa jest już faktem!.
- Grupa prof. Gisina w Genewie przeprowadziła udane eksperymenty z kwantową dystrybucją klucza na odległości 67 km, używając komercyjnych światłowodów. Trwają intensywne prace nad kwantową dystrybucją klucza w otwartej przestrzeni.

- Mechanika kwantowa, która z jednej strony może spowodować, że klasyczne algorytmy kryptograficzne staną się bezużyteczne, z drugiej strony daje możliwość wykorzystania jej praw do bezpiecznego przekazywania klucza kryptograficznego.