Kryptografia kwantowa

Wykład popularno-naukowy
dla młodzieży szkół średnich

Ryszard Tanaś

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

20 marca 2002

Enigma

niemiecka maszyna szyfrująca

Marian Rejewski

Jerzy Różycki

Henryk Zygalski

polscy matematycy, którzy złamali szyfr enigmy

Spis treści

1 Kryptografia klasyczna

1 Kryptografia klasyczna

1.1 Terminologia

1 Kryptografia klasyczna

1.1 Terminologia

- Kryptografia — dziedzina wiedzy zajmująca się zabezpieczaniem informacji (szyfrowanie)

1 Kryptografia klasyczna

1.1 Terminologia

- Kryptografia — dziedzina wiedzy zajmująca się zabezpieczaniem informacji (szyfrowanie)
- Kryptoanaliza — łamanie szyfrów, znajdowanie słabych punktów kryptosystemu

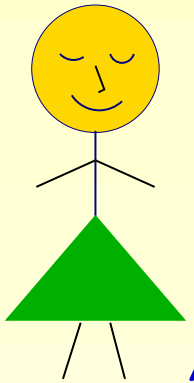
1 Kryptografia klasyczna

1.1 Terminologia

- Kryptografia — dziedzina wiedzy zajmująca się zabezpieczaniem informacji (szyfrowanie)
- Kryptoanaliza — łamanie szyfrów, znajdowanie słabych punktów kryptosystemu
- Kryptologia — dział matematyki, który zajmuje się podstawami metod kryptograficznych (kryptografia + kryptoanaliza)

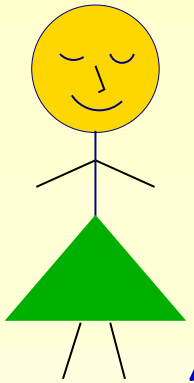
1.2 Główne postacie

1.2 Główne postacie

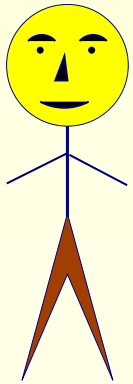


Alicja — nadawca informacji

1.2 Główne postacie

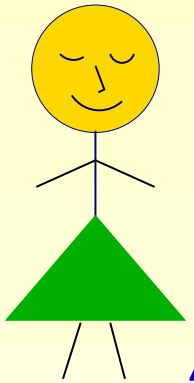


Alicja — nadawca informacji

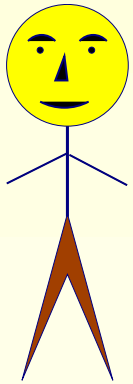


Bolek — odbiorca (adresat) informacji

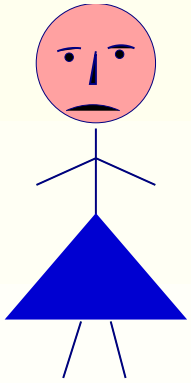
1.2 Główne postacie



Alicja — nadawca informacji

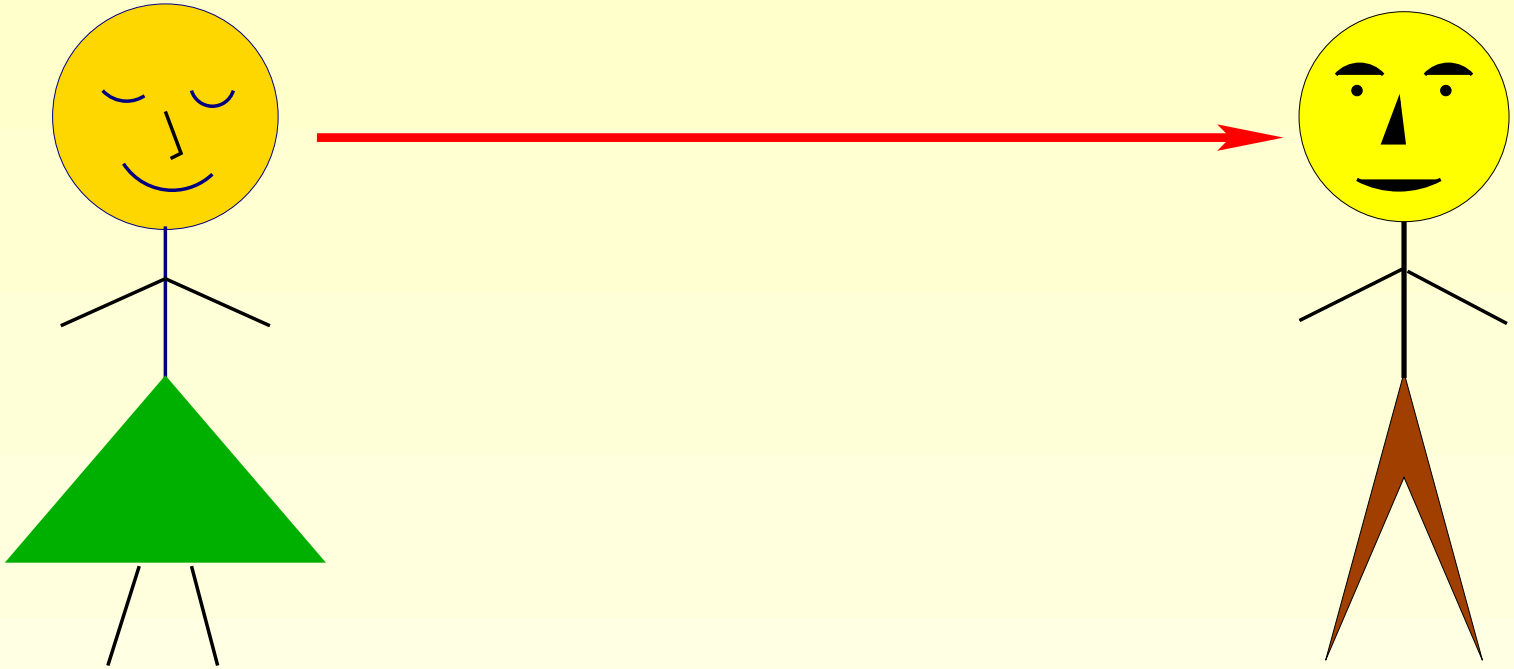


Bolek — odbiorca (adresat) informacji

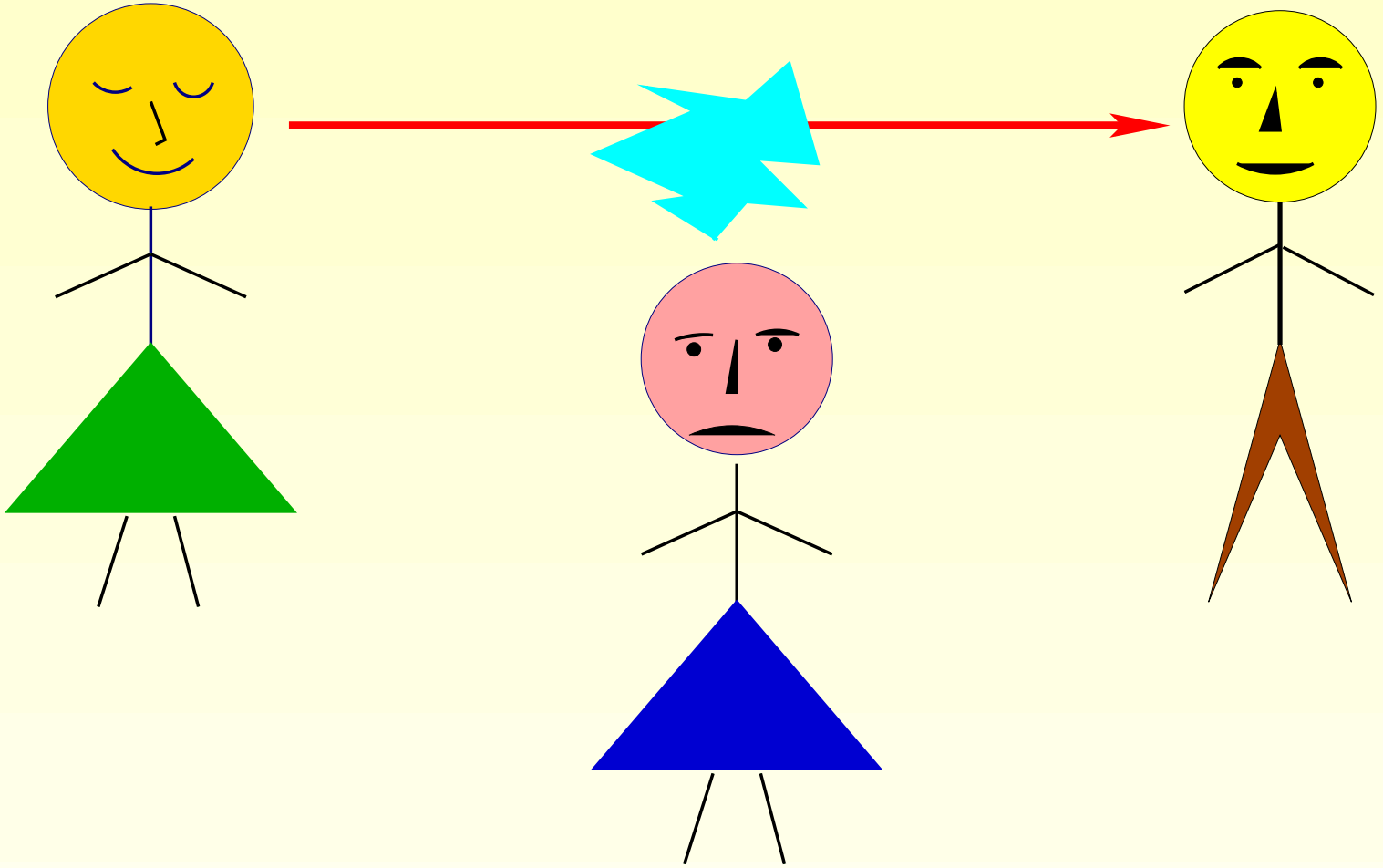


Ewa — usiłująca przechwycić informację przeznaczoną dla Bolka

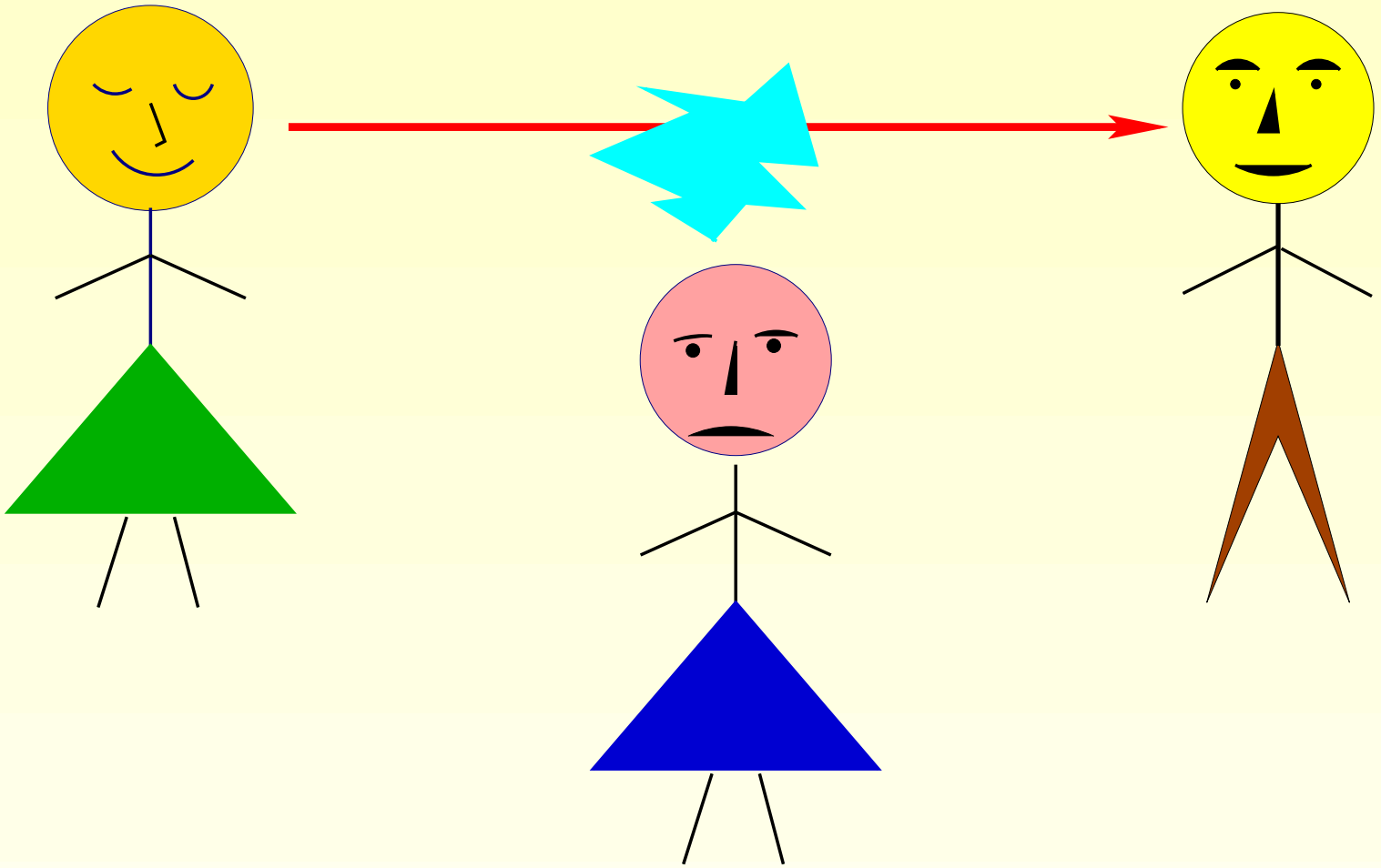
1.3 Kanał łączności



Alicja przesyła informacje do Bolka kanałem, który jest narażony na podsłuch

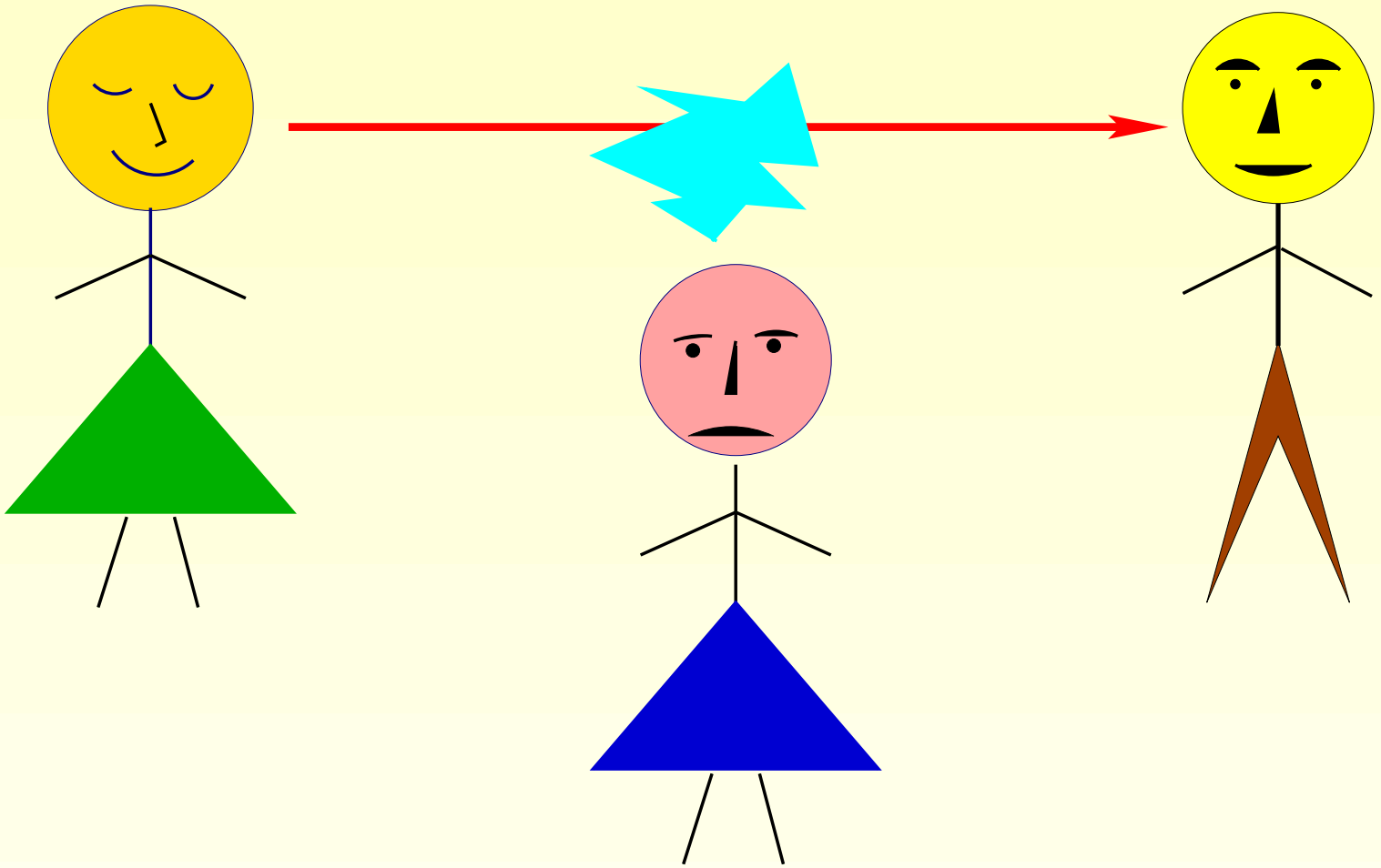


Ewa podsłuchuje usiłując dowiedzieć się co Alicja przesyła do Bolka



Ewa podsłuchuje usiłując dowiedzieć się co Alicja przesyła do Bolka

Co powinna zrobić Alicja?



Ewa podsłuchuje usiłując dowiedzieć się co Alicja przesyła do Bolka

Co powinna zrobić Alicja?

Szyfrować!

1.4 Proste szyfry

1.4 Proste szyfry

Szyfr Cezara

szyfr podstawieniowy monoalfabetyczny

1.4 Proste szyfry

Szyfr Cezara

szyfr podstawieniowy monoalfabetyczny

A B C D E F G H I J K L M N O P R S T U V W X Y Z
D E F G H I J K L M N O P R S T U V W X Y Z A B C

1.4 Proste szyfry

Szyfr Cezara

szyfr podstawieniowy monoalfabetyczny

A B C D E F G H I J K L M N O P R S T U V W X Y Z
D E F G H I J K L M N O P R S T U V W X Y Z A B C

tekst jawny $\longrightarrow$ K R Y P T O G R A F I A
kryptogram $\longrightarrow$ N U B T W S J U D I L D

Szyfr Vigenère'a

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y

klucz $\longrightarrow$ S Z Y M P A N S S Z Y M

tekst $\longrightarrow$ K R Y P T O G R A F I A

krypt. $\longrightarrow$ C P W C I O U I S E G M

Szyfr Vernama (one-time pad)

tekst jawny $\longrightarrow$	S	Z	Y	F	R
binarnie $\longrightarrow$	01010011	01011010	01011001	01000110	01010010
klucz $\longrightarrow$	01110010	01010101	11011100	10110011	00101011
kryptogram $\longrightarrow$	00100001	00001111	10000101	11110101	01111001

- Klucz jest losowym ciągiem bitów.
- Kryptogram jest także losowym ciągiem bitów i jeśli nie znamy klucza to nie dowiemy się niczego o tekście jawnym.
- Jeśli klucz jest tak długi jak wiadomość i użyty tylko raz, to szyfr ten gwarantuje bezpieczeństwo absolutne.
- Współczesne metody kryptograficzne sprowadzają się do obliczeń w systemie binarnym, czyli operacji na bitach.

Szyfr Vernama (one-time pad)

tekst jawny $\longrightarrow$	S	Z	Y	F	R
binarnie $\longrightarrow$	01010011	01011010	01011001	01000110	01010010
klucz $\longrightarrow$	01110010	01010101	11011100	10110011	00101011
kryptogram $\longrightarrow$	00100001	00001111	10000101	11110101	01111001

- Klucz jest losowym ciągiem bitów.
- Kryptogram jest także losowym ciągiem bitów i jeśli nie znamy klucza to nie dowiemy się niczego o tekście jawnym.
- Jeśli klucz jest tak długi jak wiadomość i użyty tylko raz, to szyfr ten gwarantuje bezpieczeństwo absolutne.
- Współczesne metody kryptograficzne sprowadzają się do obliczeń w systemie binarnym, czyli operacji na bitach.

Szyfr Vernama (one-time pad)

tekst jawny $\longrightarrow$	S	Z	Y	F	R
binarnie $\longrightarrow$	01010011	01011010	01011001	01000110	01010010
klucz $\longrightarrow$	01110010	01010101	11011100	10110011	00101011
kryptogram $\longrightarrow$	00100001	00001111	10000101	11110101	01111001

- Klucz jest losowym ciągiem bitów.
- Kryptogram jest także losowym ciągiem bitów i jeśli nie znamy klucza to nie dowiemy się niczego o tekście jawnym.
- Jeśli klucz jest tak długi jak wiadomość i użyty tylko raz, to szyfr ten gwarantuje bezpieczeństwo absolutne.
- Współczesne metody kryptograficzne sprowadzają się do obliczeń w systemie binarnym, czyli operacji na bitach.

Szyfr Vernama (one-time pad)

tekst jawny $\longrightarrow$	S	Z	Y	F	R
binarnie $\longrightarrow$	01010011	01011010	01011001	01000110	01010010
klucz $\longrightarrow$	01110010	01010101	11011100	10110011	00101011
kryptogram $\longrightarrow$	00100001	00001111	10000101	11110101	01111001

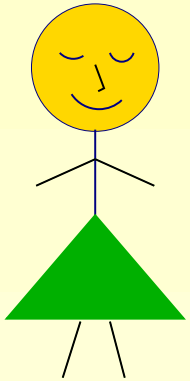
- Klucz jest losowym ciągiem bitów.
- Kryptogram jest także losowym ciągiem bitów i jeśli nie znamy klucza to nie dowiemy się niczego o tekście jawnym.
- Jeśli klucz jest tak długi jak wiadomość i użyty tylko raz, to szyfr ten gwarantuje bezpieczeństwo absolutne.
- Współczesne metody kryptograficzne sprowadzają się do obliczeń w systemie binarnym, czyli operacji na bitach.

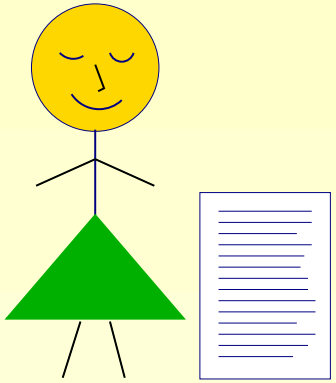
Szyfr Vernama (one-time pad)

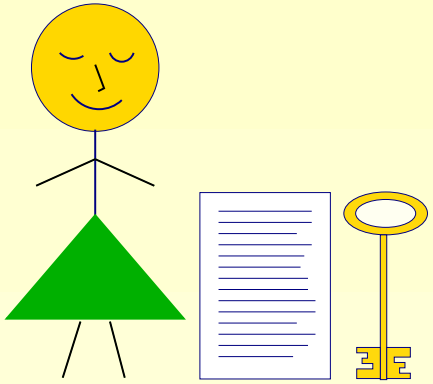
tekst jawny $\longrightarrow$	S	Z	Y	F	R
binarnie $\longrightarrow$	01010011	01011010	01011001	01000110	01010010
klucz $\longrightarrow$	01110010	01010101	11011100	10110011	00101011
kryptogram $\longrightarrow$	00100001	00001111	10000101	11110101	01111001

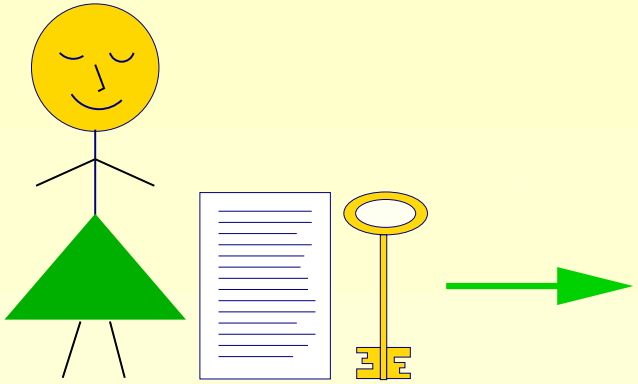
- Klucz jest losowym ciągiem bitów.
- Kryptogram jest także losowym ciągiem bitów i jeśli nie znamy klucza to nie dowiemy się niczego o tekście jawnym.
- Jeśli klucz jest tak długi jak wiadomość i użyty tylko raz, to szyfr ten gwarantuje bezpieczeństwo absolutne.
- Współczesne metody kryptograficzne sprowadzają się do obliczeń w systemie binarnym, czyli operacji na bitach.

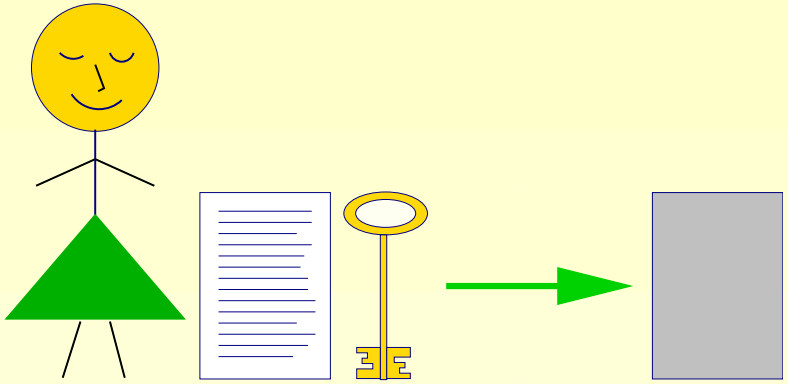
1.5 Systemy z kluczem tajnym

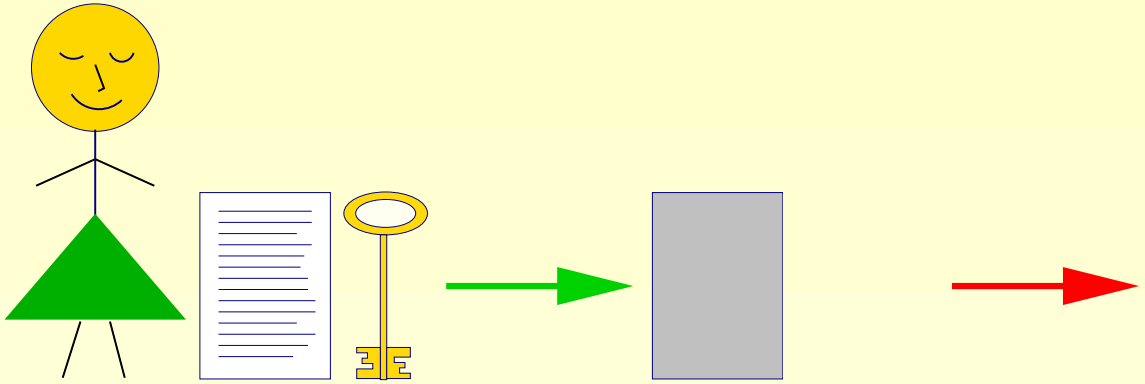


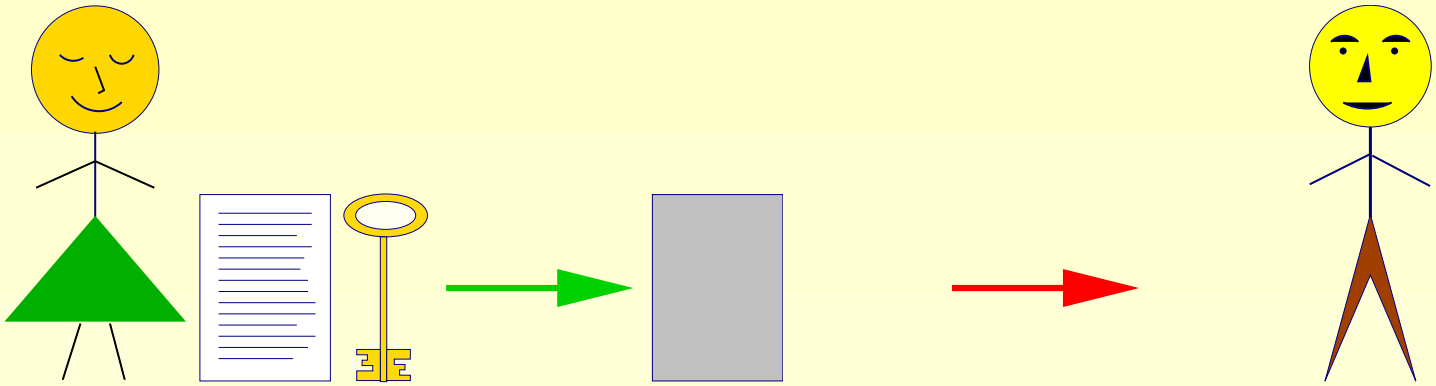


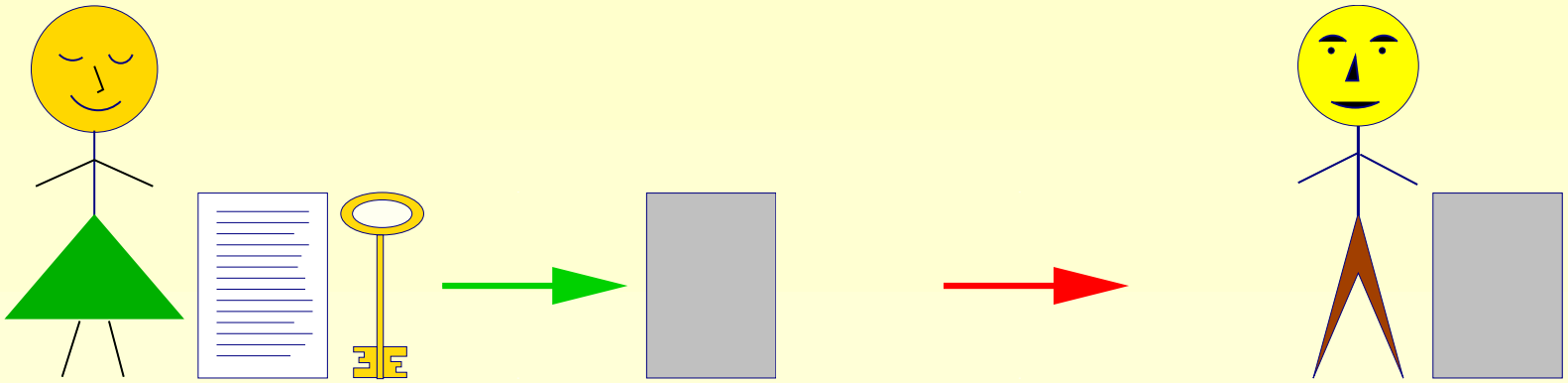


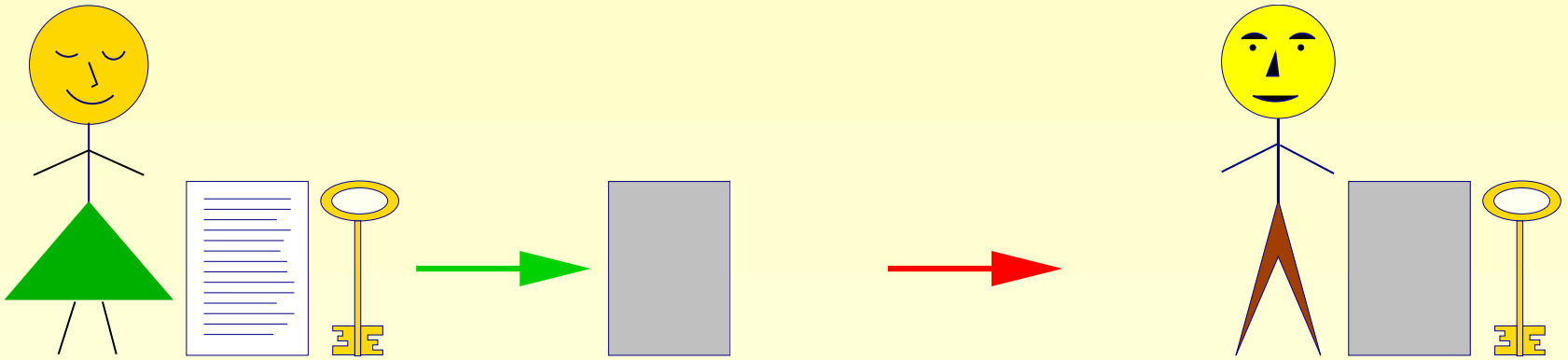


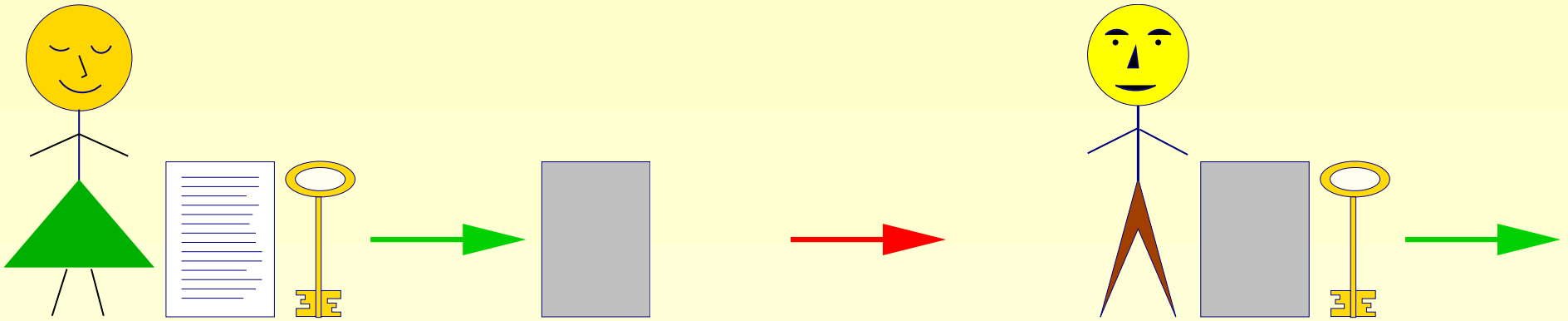


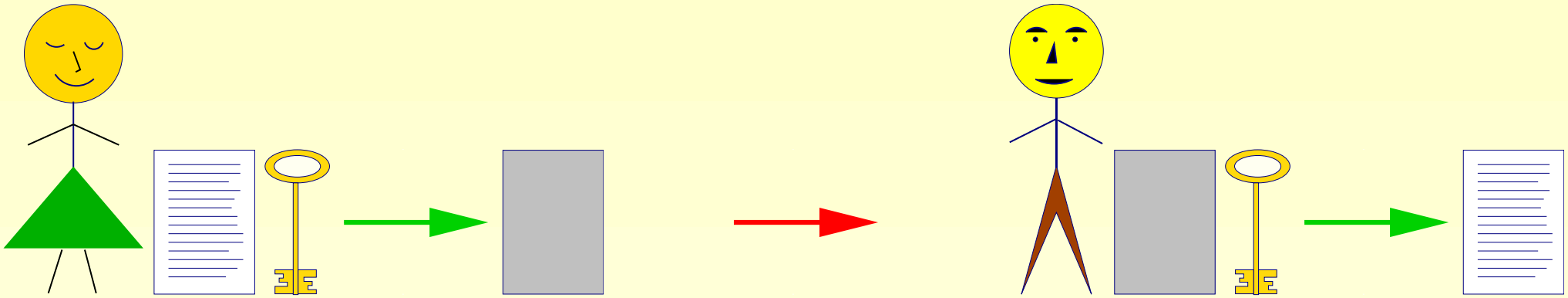


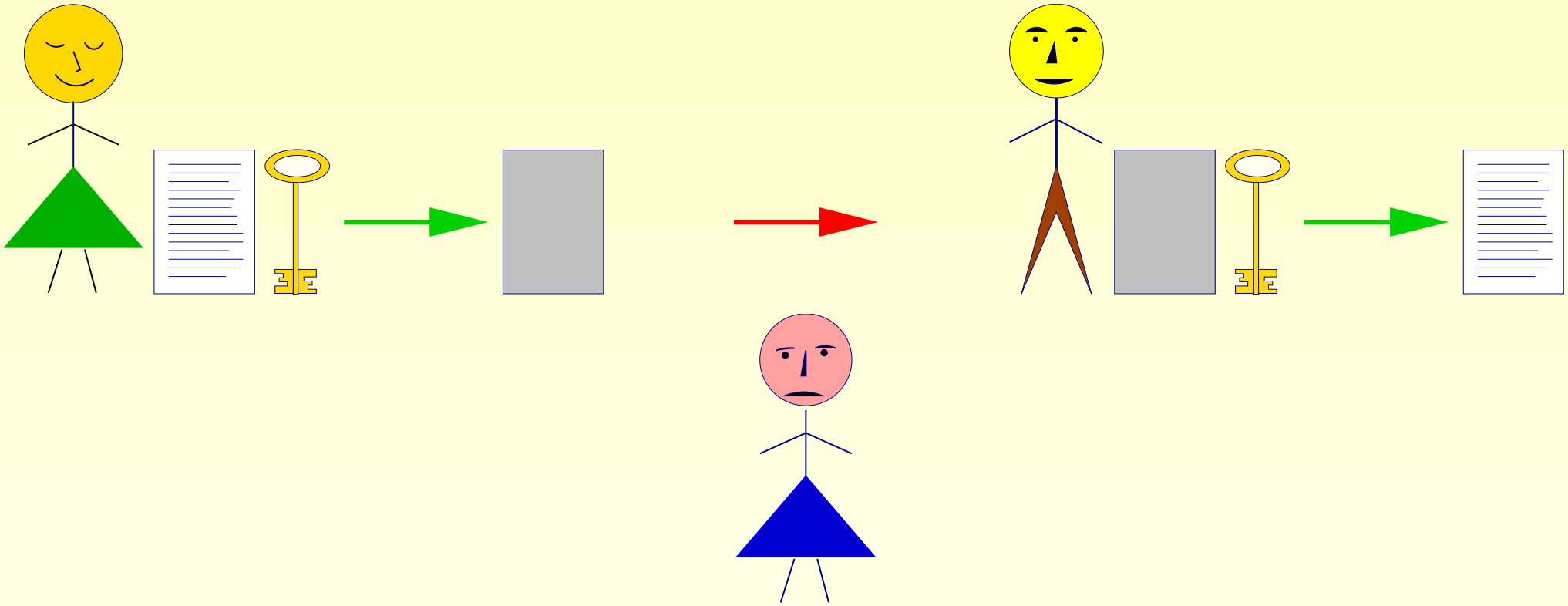


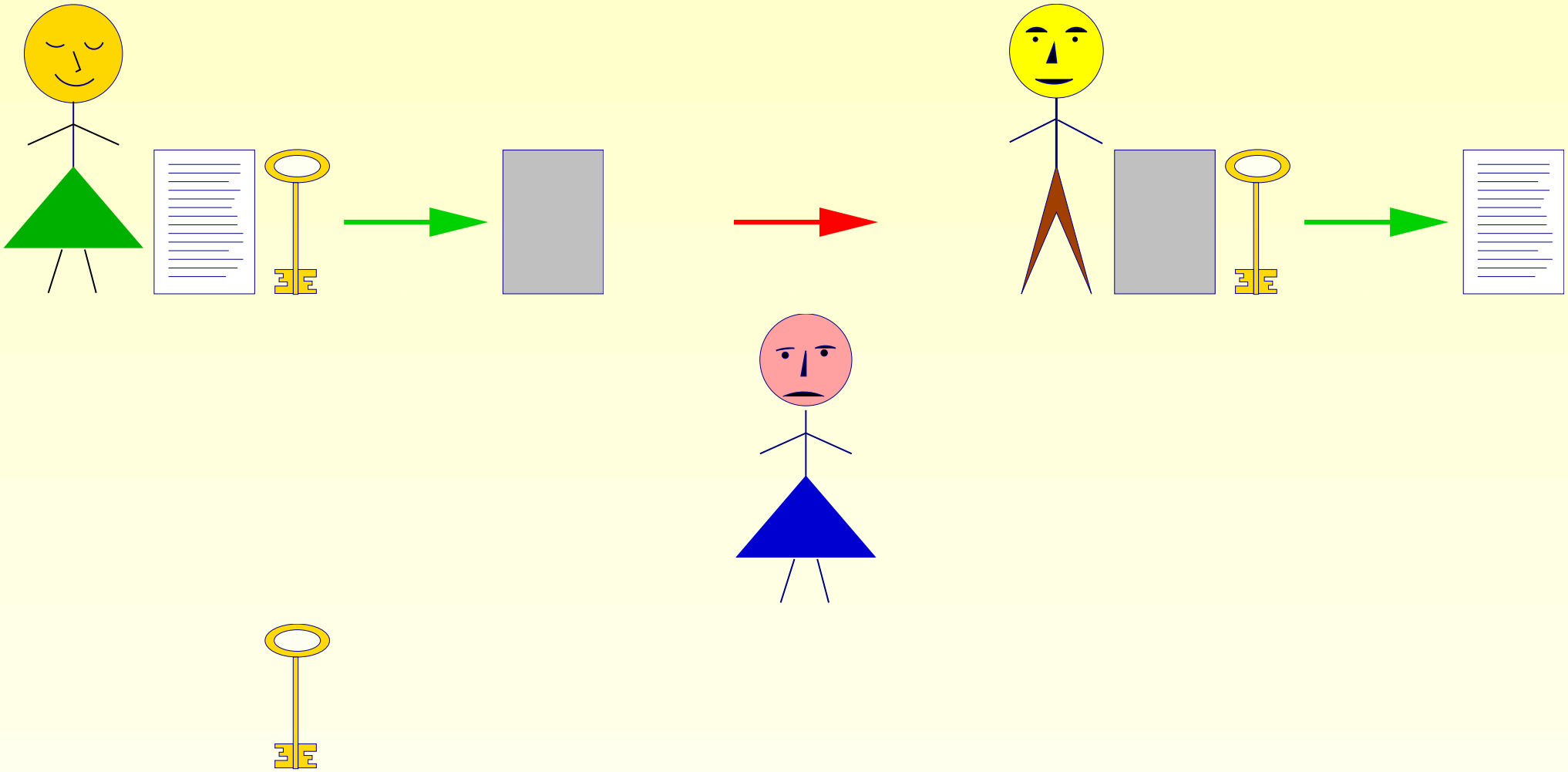


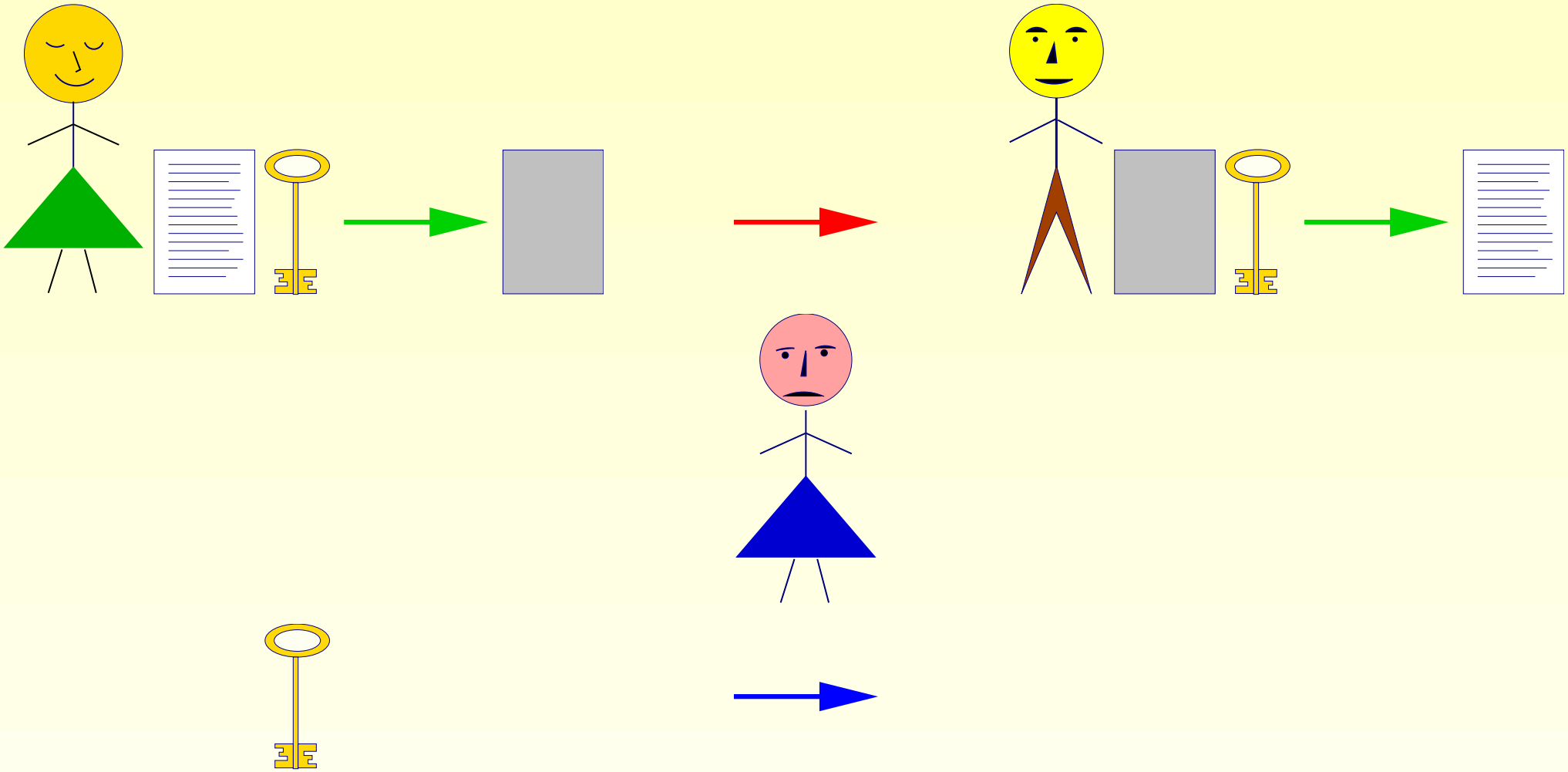


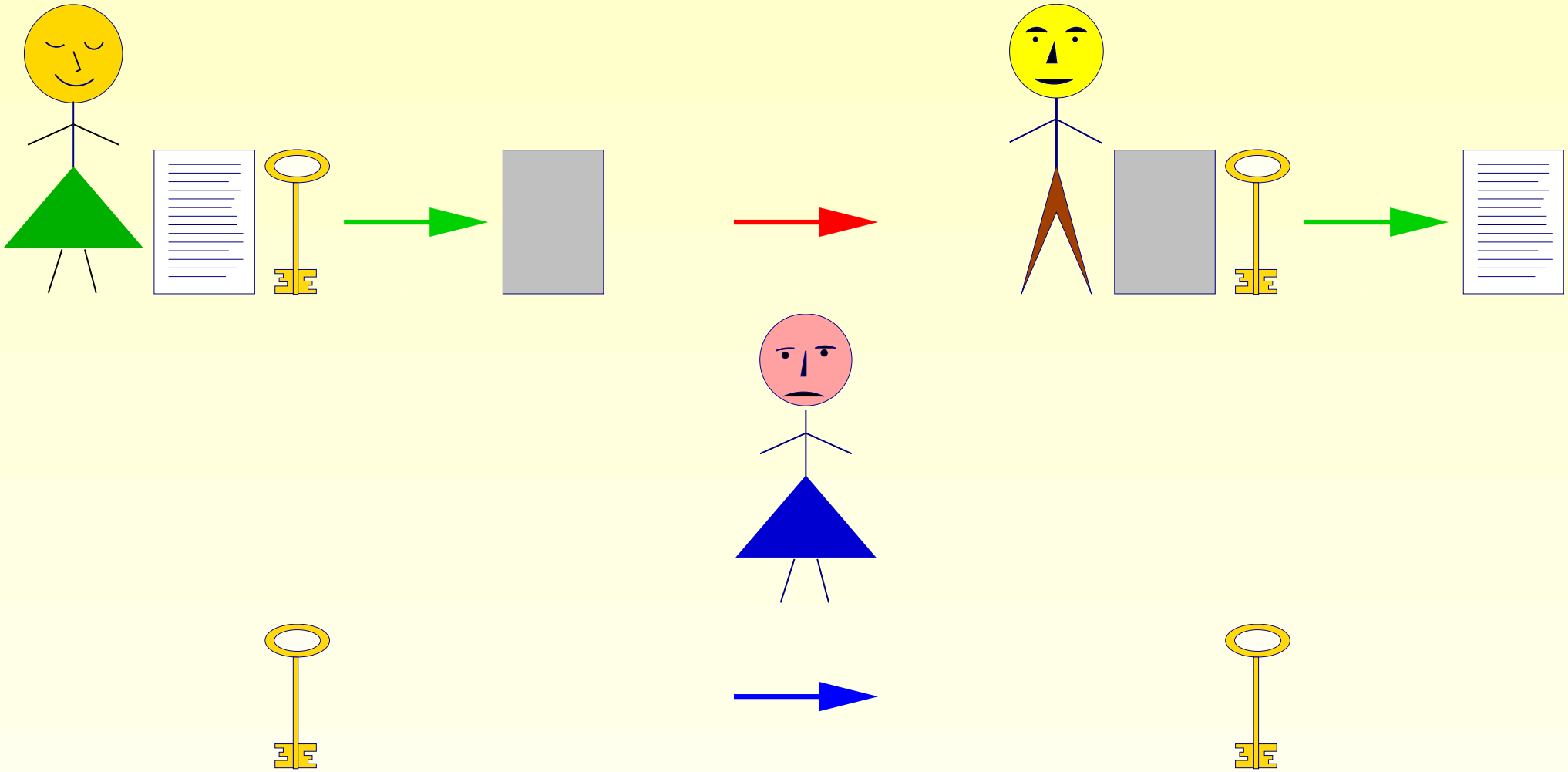


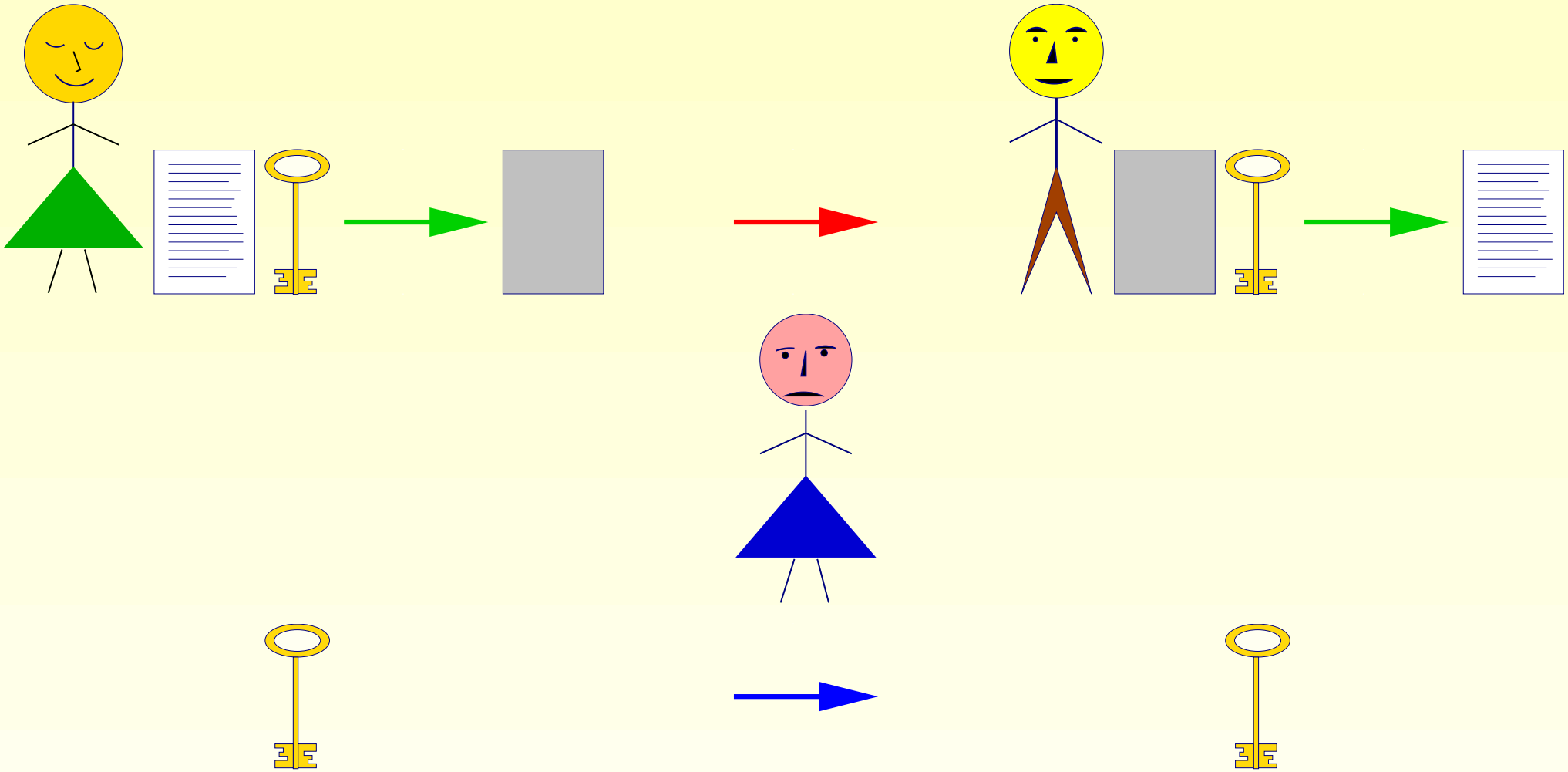








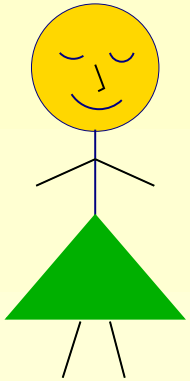


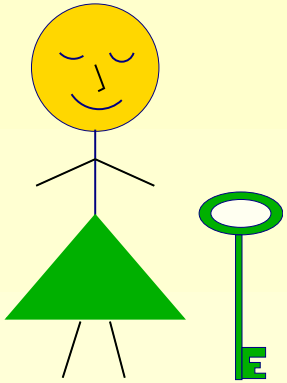


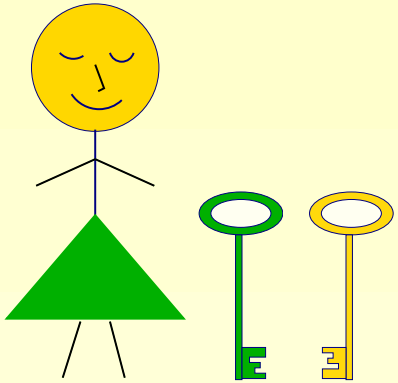
Pułapka

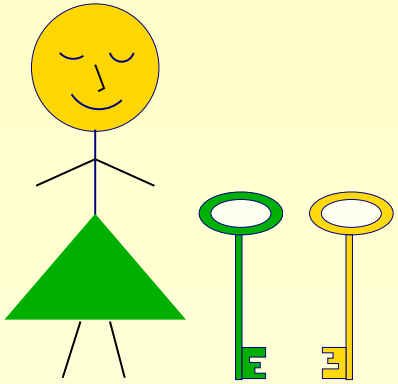
Aby zbudować bezpieczny kanał łączności trzeba mieć bezpieczny kanał łączności ...

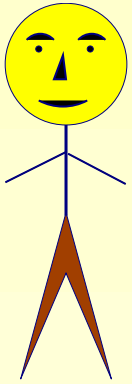
1.6 Systemy z kluczem publicznym

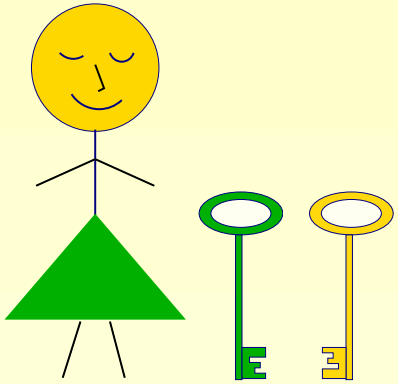


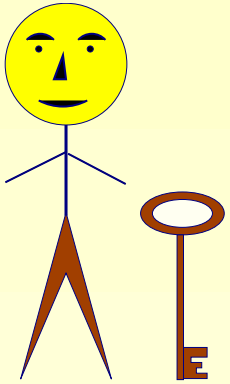


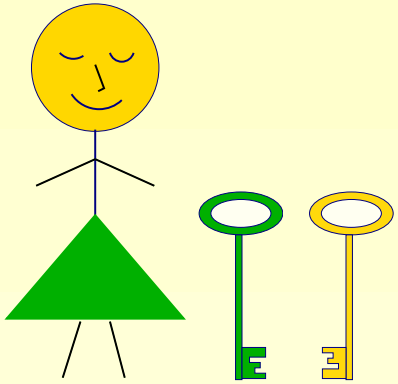


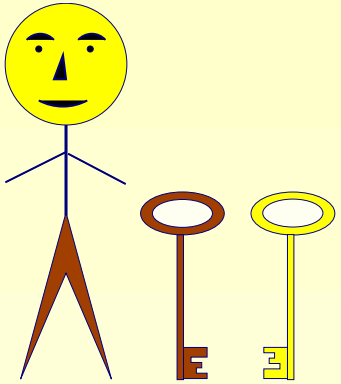


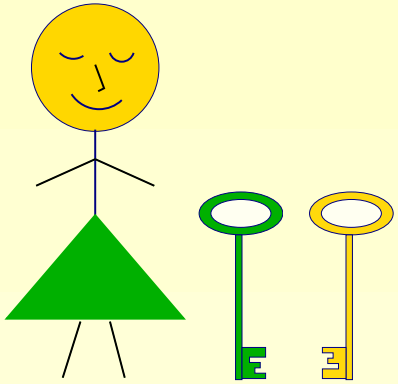




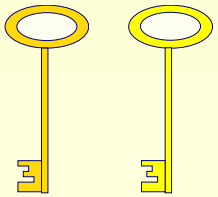




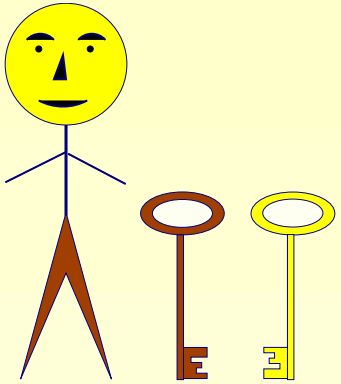


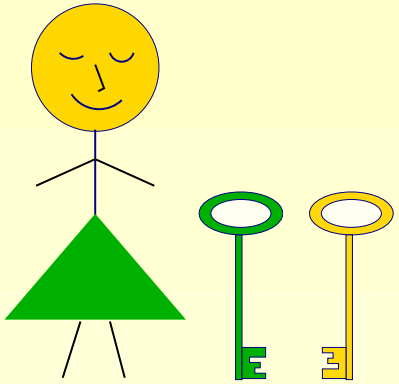


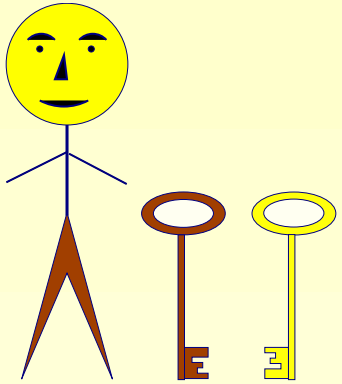
Klucze



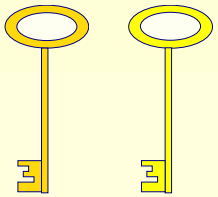
publiczne



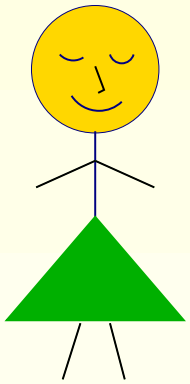


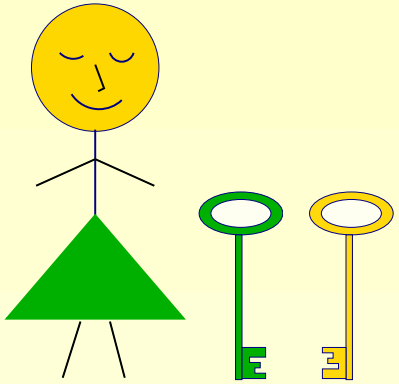


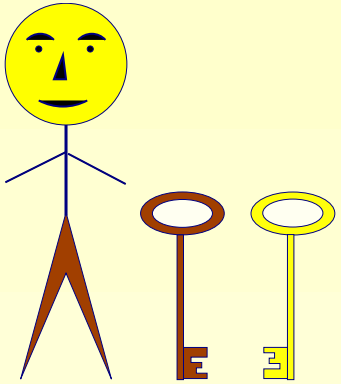
Klucze



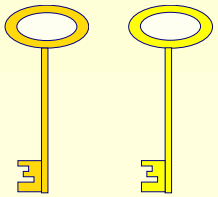
publiczne



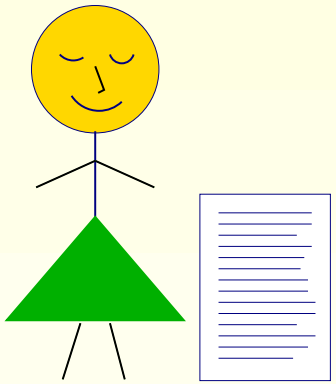


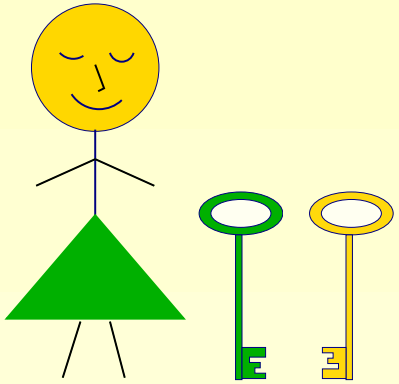


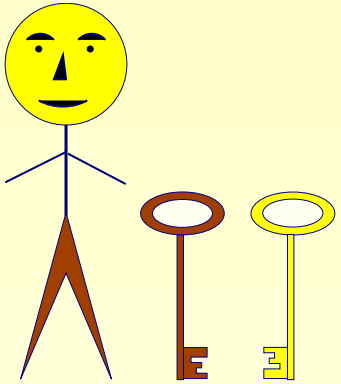
Klucze



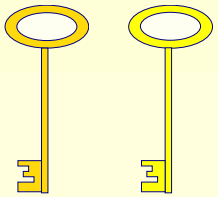
publiczne



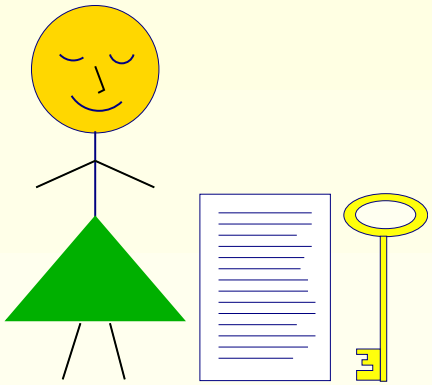


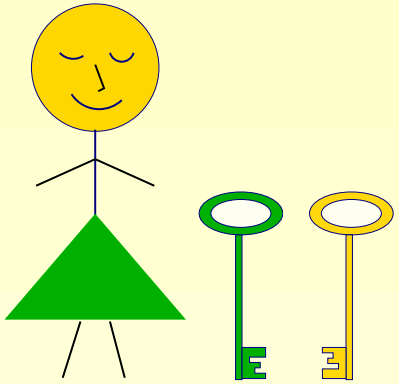


Klucze

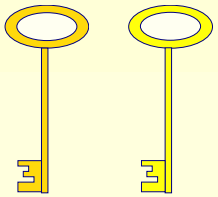


publiczne

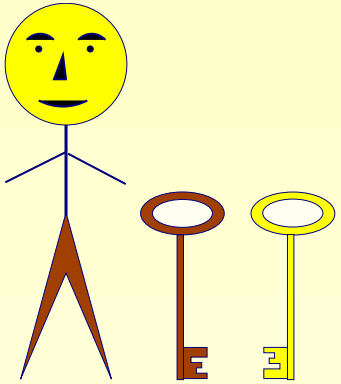


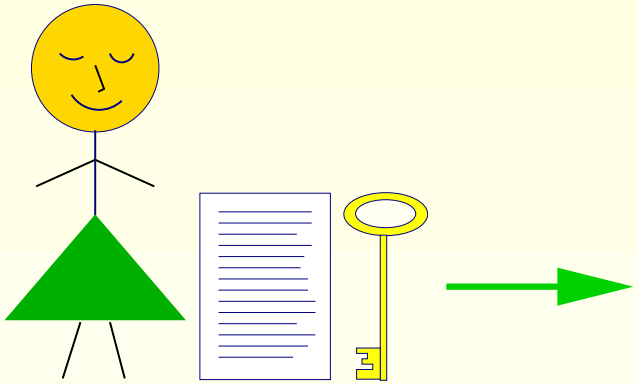


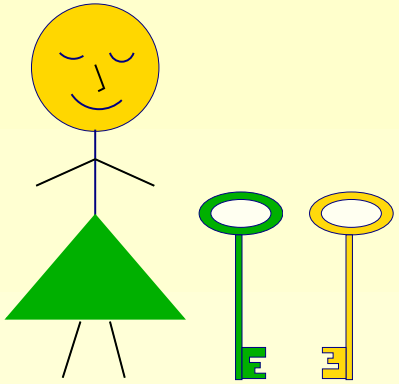
Klucze

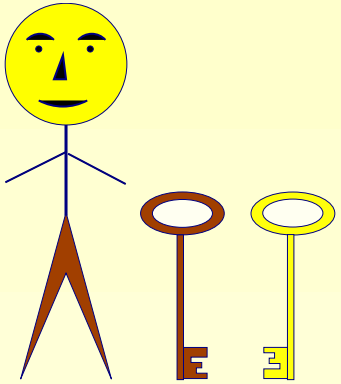


publiczne

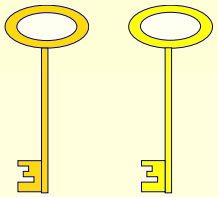




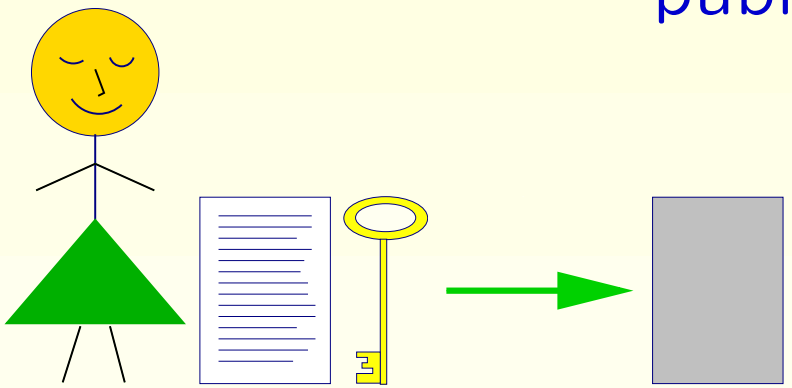


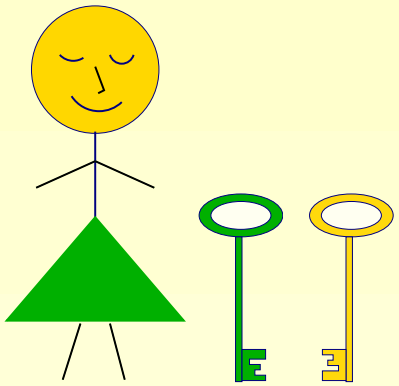


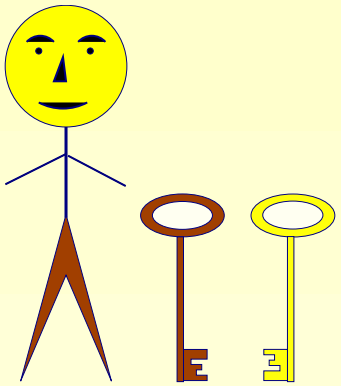
Klucze



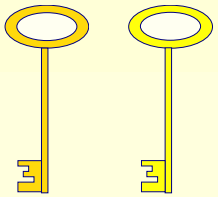
publiczne



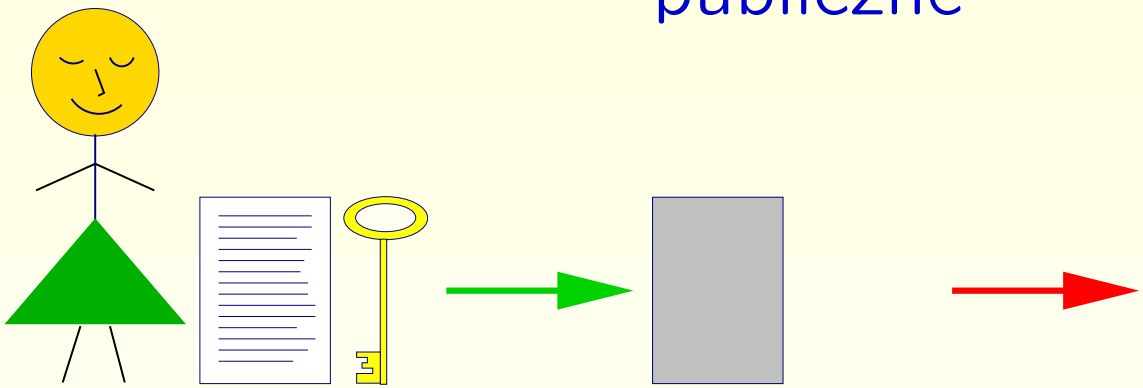


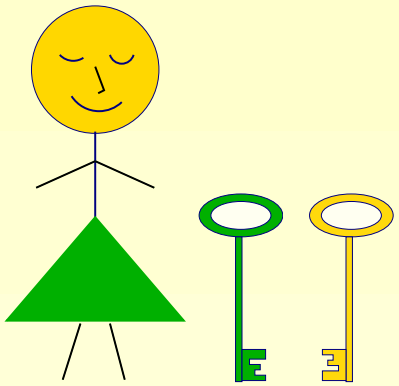


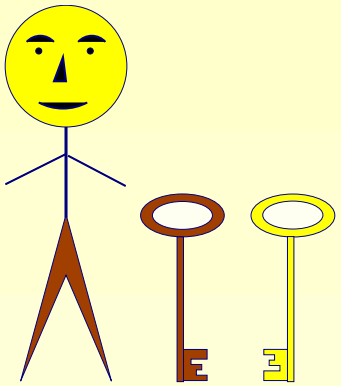
Klucze



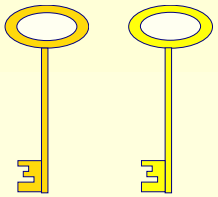
publiczne



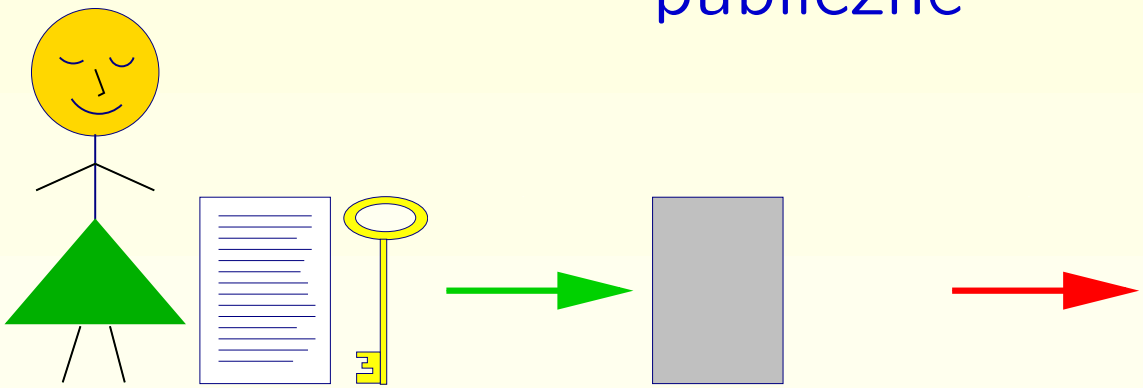


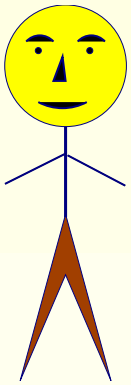


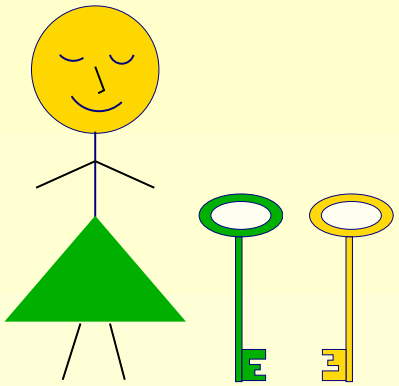
Klucze

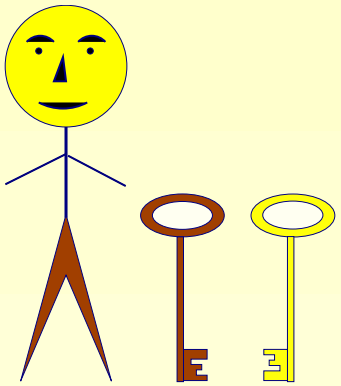


publiczne

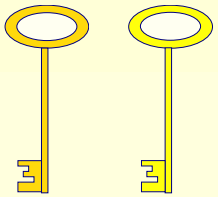




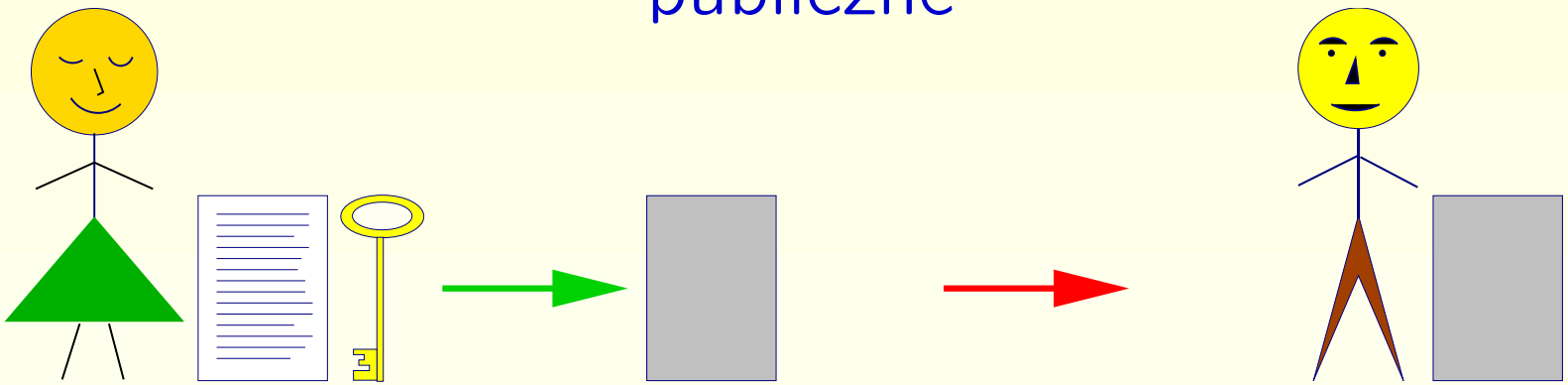


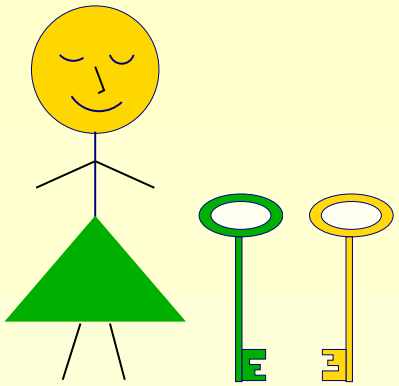


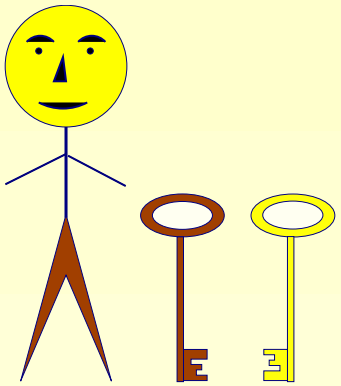
Klucze



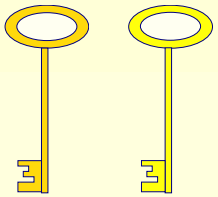
publiczne



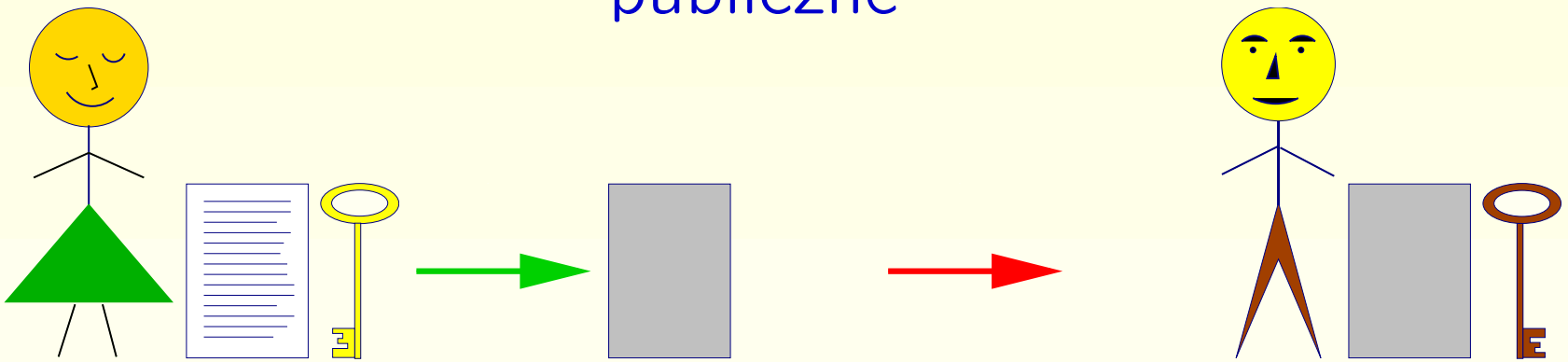


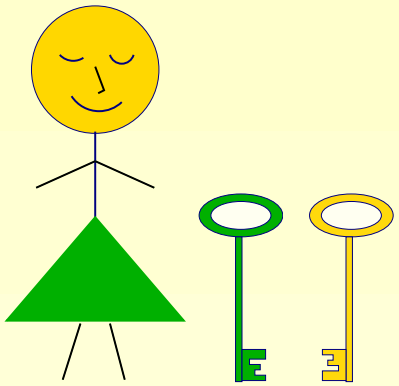


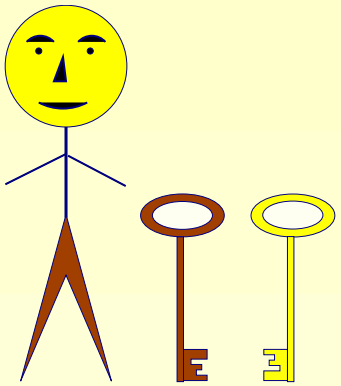
Klucze



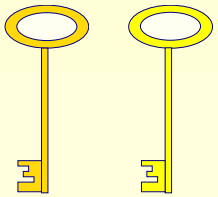
publiczne



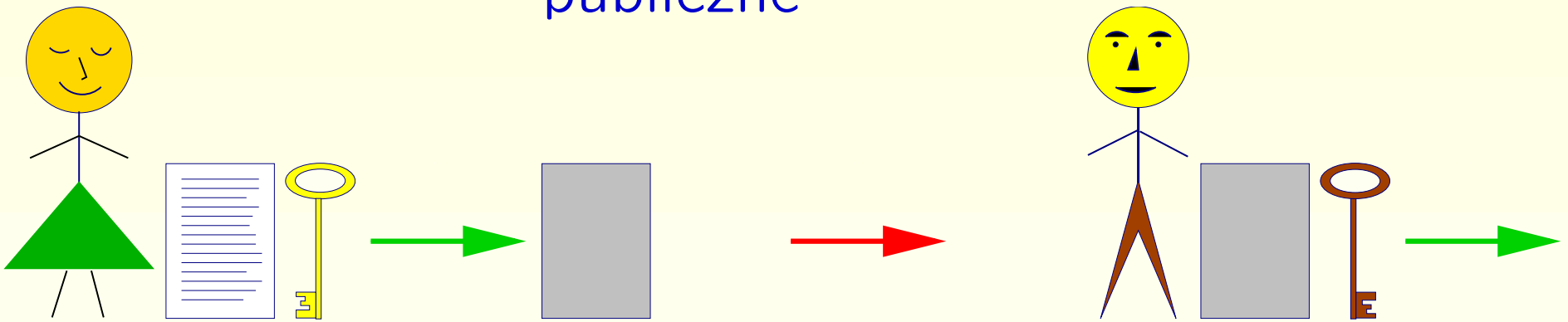


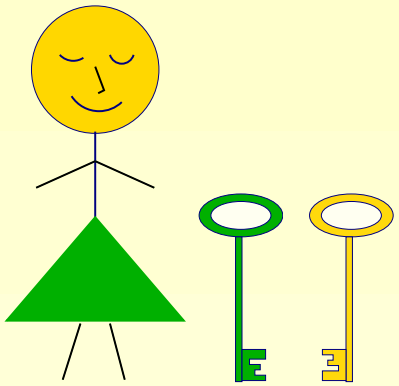


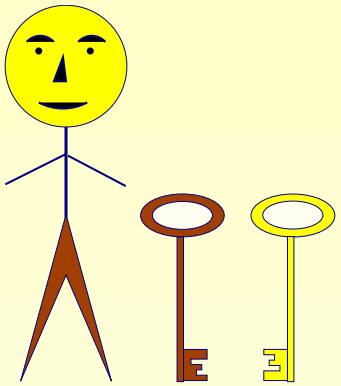
Klucze



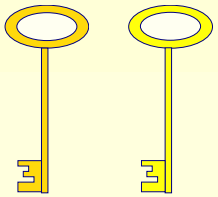
publiczne



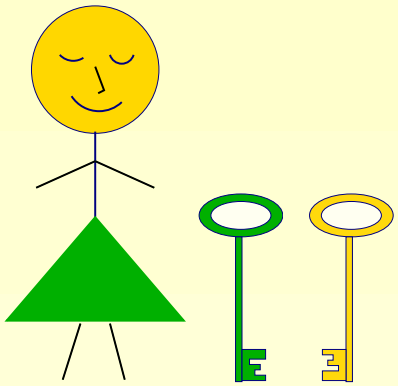


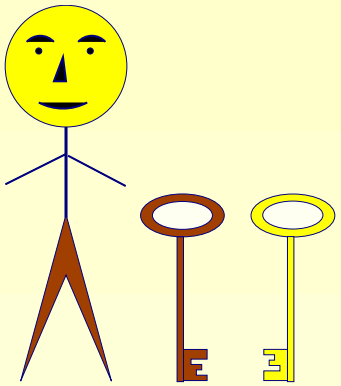


Klucze

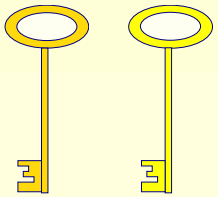


publiczne

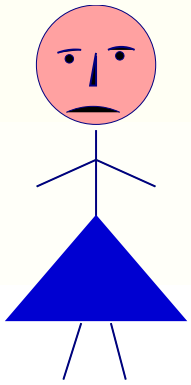


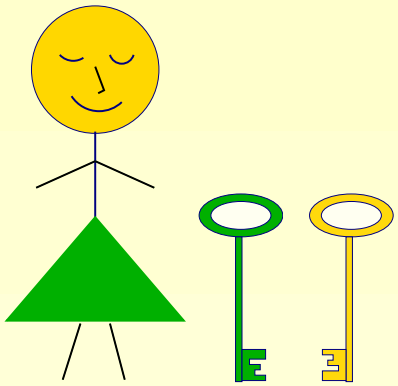


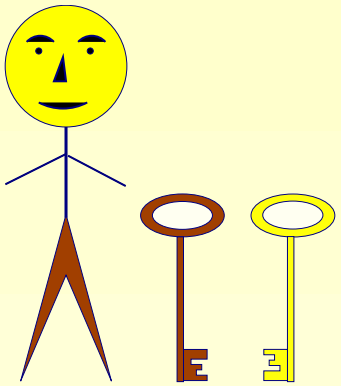
Klucze



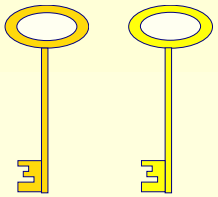
publiczne



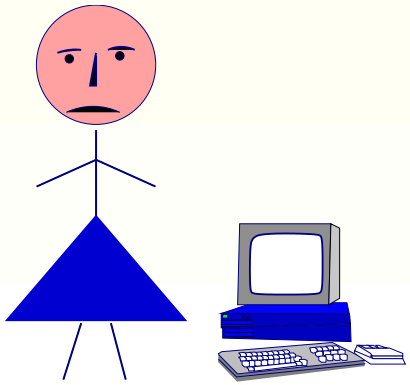




Klucze



publiczne



Jak to działa?

- Alicja i Bolek generują pary kluczy: jeden publiczny i jeden prywatny. Klucz publiczny udostępniają publicznie a prywatny skrzętnie chronią.
- Aby wysłać wiadomość do Bolka, Alicja bierze publiczny klucz Bolka, szyfuje nim wiadomość i kryptogram wysyła do Bolka.
- Bolek deszyfruje otrzymany kryptogram swoim kluczem prywatnym
- Nie ma potrzeby przesyłania tajnego klucza!
- Znakomicie! Nic lepszego nie potrzebujemy!

Jak to działa?

- Alicja i Bolek generują pary kluczy: jeden publiczny i jeden prywatny. Klucz publiczny udostępniają publicznie a prywatny skrzętnie chronią.
- Aby wysłać wiadomość do Bolka, Alicja bierze publiczny klucz Bolka, szyfuje nim wiadomość i kryptogram wysyła do Bolka.
- Bolek deszyfruje otrzymany kryptogram swoim kluczem prywatnym
- Nie ma potrzeby przesyłania tajnego klucza!
- Znakomicie! Nic lepszego nie potrzebujemy!

Jak to działa?

- Alicja i Bolek generują pary kluczy: jeden publiczny i jeden prywatny. Klucz publiczny udostępniają publicznie a prywatny skrzętnie chronią.
- Aby wysłać wiadomość do Bolka, Alicja bierze publiczny klucz Bolka, szyfuje nim wiadomość i kryptogram wysyła do Bolka.
- Bolek deszyfruje otrzymany kryptogram swoim kluczem prywatnym
- Nie ma potrzeby przesyłania tajnego klucza!
- Znakomicie! Nic lepszego nie potrzebujemy!

Jak to działa?

- Alicja i Bolek generują pary kluczy: jeden publiczny i jeden prywatny. Klucz publiczny udostępniają publicznie a prywatny skrzętnie chronią.
- Aby wysłać wiadomość do Bolka, Alicja bierze publiczny klucz Bolka, szyfuje nim wiadomość i kryptogram wysyła do Bolka.
- Bolek deszyfruje otrzymany kryptogram swoim kluczem prywatnym
- Nie ma potrzeby przesyłania tajnego klucza!
- Znakomicie! Nic lepszego nie potrzebujemy!

Jak to działa?

- Alicja i Bolek generują pary kluczy: jeden publiczny i jeden prywatny. Klucz publiczny udostępniają publicznie a prywatny skrzętnie chronią.
- Aby wysłać wiadomość do Bolka, Alicja bierze publiczny klucz Bolka, szyfuje nim wiadomość i kryptogram wysyła do Bolka.
- Bolek deszyfruje otrzymany kryptogram swoim kluczem prywatnym
- Nie ma potrzeby przesyłania tajnego klucza!
- Znakomicie! Nic lepszego nie potrzebujemy!

Jak to działa?

- Alicja i Bolek generują pary kluczy: jeden publiczny i jeden prywatny. Klucz publiczny udostępniają publicznie a prywatny skrzętnie chronią.
- Aby wysłać wiadomość do Bolka, Alicja bierze publiczny klucz Bolka, szyfuje nim wiadomość i kryptogram wysyła do Bolka.
- Bolek deszyfruje otrzymany kryptogram swoim kluczem prywatnym
- Nie ma potrzeby przesyłania tajnego klucza!
- Znakomicie! Nic lepszego nie potrzebujemy!

A jednak!?

- Bezpieczeństwo systemu kryptograficznego z kluczem publicznym jest oparte na istnieniu funkcji jednostronnych, dla których znalezienie wartości samej funkcji jest łatwe zaś znalezienie argumentu funkcji kiedy znamy jej wartość jest obliczeniowo trudne (jak trudne to zależy od aktualnego stanu wiedzy i rozwoju techniki)

A jednak!?

- Bezpieczeństwo systemu kryptograficznego z kluczem publicznym jest oparte na istnieniu funkcji jednostronnych, dla których znalezienie wartości samej funkcji jest łatwe zaś znalezienie argumentu funkcji kiedy znamy jej wartość jest obliczeniowo trudne (jak trudne to zależy od aktualnego stanu wiedzy i rozwoju techniki)
- Najbardziej znany kryptosystem z kluczem publicznym, RSA, opiera się na trudności z rozkładem liczby na czynniki (faktoryzacja) Weźmy np liczbę

A jednak!?

- Bezpieczeństwo systemu kryptograficznego z kluczem publicznym jest oparte na istnieniu funkcji jednostronnych, dla których znalezienie wartości samej funkcji jest łatwe zaś znalezienie argumentu funkcji kiedy znamy jej wartość jest obliczeniowo trudne (jak trudne to zależy od aktualnego stanu wiedzy i rozwoju techniki)
- Najbardziej znany kryptosystem z kluczem publicznym, RSA, opiera się na trudności z rozkładem liczby na czynniki (faktoryzacja) Weźmy np liczbę

$$29083 \quad = \quad \square \cdot \square$$

A jednak!?

- Bezpieczeństwo systemu kryptograficznego z kluczem publicznym jest oparte na istnieniu funkcji jednostronnych, dla których znalezienie wartości samej funkcji jest łatwe zaś znalezienie argumentu funkcji kiedy znamy jej wartość jest obliczeniowo trudne (jak trudne to zależy od aktualnego stanu wiedzy i rozwoju techniki)
- Najbardziej znany kryptosystem z kluczem publicznym, RSA, opiera się na trudności z rozkładem liczby na czynniki (faktoryzacja) Weźmy np liczbę

$$29083 = \square \cdot \square$$

$$29083 =$$

A jednak!?

- Bezpieczeństwo systemu kryptograficznego z kluczem publicznym jest oparte na istnieniu funkcji jednostronnych, dla których znalezienie wartości samej funkcji jest łatwe zaś znalezienie argumentu funkcji kiedy znamy jej wartość jest obliczeniowo trudne (jak trudne to zależy od aktualnego stanu wiedzy i rozwoju techniki)
- Najbardziej znany kryptosystem z kluczem publicznym, RSA, opiera się na trudności z rozkładem liczby na czynniki (faktoryzacja) Weźmy np liczbę

$$29083 = \square \cdot \square$$

$$29083 = 127 \cdot 229$$

- Systemy takie nie gwarantują pełnego bezpieczeństwa. Nie można wykluczyć, że ktoś znajdzie efektywny algorytm faktoryzacji liczb.

- Systemy takie nie gwarantują pełnego bezpieczeństwa. Nie można wykluczyć, że ktoś znajdzie efektywny algorytm faktoryzacji liczb.

  W istocie taki algorytm już istnieje.
  Jest to algorytm Shora! Wymaga on jednak komputera kwantowego!.

- Systemy takie nie gwarantują pełnego bezpieczeństwa. Nie można wykluczyć, że ktoś znajdzie efektywny algorytm faktoryzacji liczb.

  W istocie taki algorytm już istnieje.
  Jest to algorytm Shora! Wymaga on jednak komputera kwantowego!.

  Trwają intensywne prace nad konstrukcją takiego komputera!

- Systemy takie nie gwarantują pełnego bezpieczeństwa. Nie można wykluczyć, że ktoś znajdzie efektywny algorytm faktoryzacji liczb.

  W istocie taki algorytm już istnieje.
  Jest to algorytm Shora! Wymaga on jednak komputera kwantowego!.

  Trwają intensywne prace nad konstrukcją takiego komputera!

- Ewa wyposażona w komputer kwantowy z łatwością złamie szyfr RSA!

- Systemy takie nie gwarantują pełnego bezpieczeństwa. Nie można wykluczyć, że ktoś znajdzie efektywny algorytm faktoryzacji liczb.

  W istocie taki algorytm już istnieje.
  Jest to algorytm Shora! Wymaga on jednak komputera kwantowego!.

  Trwają intensywne prace nad konstrukcją takiego komputera!

- Ewa wyposażona w komputer kwantowy z łatwością złamie szyfr RSA!

- Czy jest jakieś wyjście?

- Systemy takie nie gwarantują pełnego bezpieczeństwa. Nie można wykluczyć, że ktoś znajdzie efektywny algorytm faktoryzacji liczb.

  W istocie taki algorytm już istnieje.
  Jest to algorytm Shora! Wymaga on jednak komputera kwantowego!.

  Trwają intensywne prace nad konstrukcją takiego komputera!

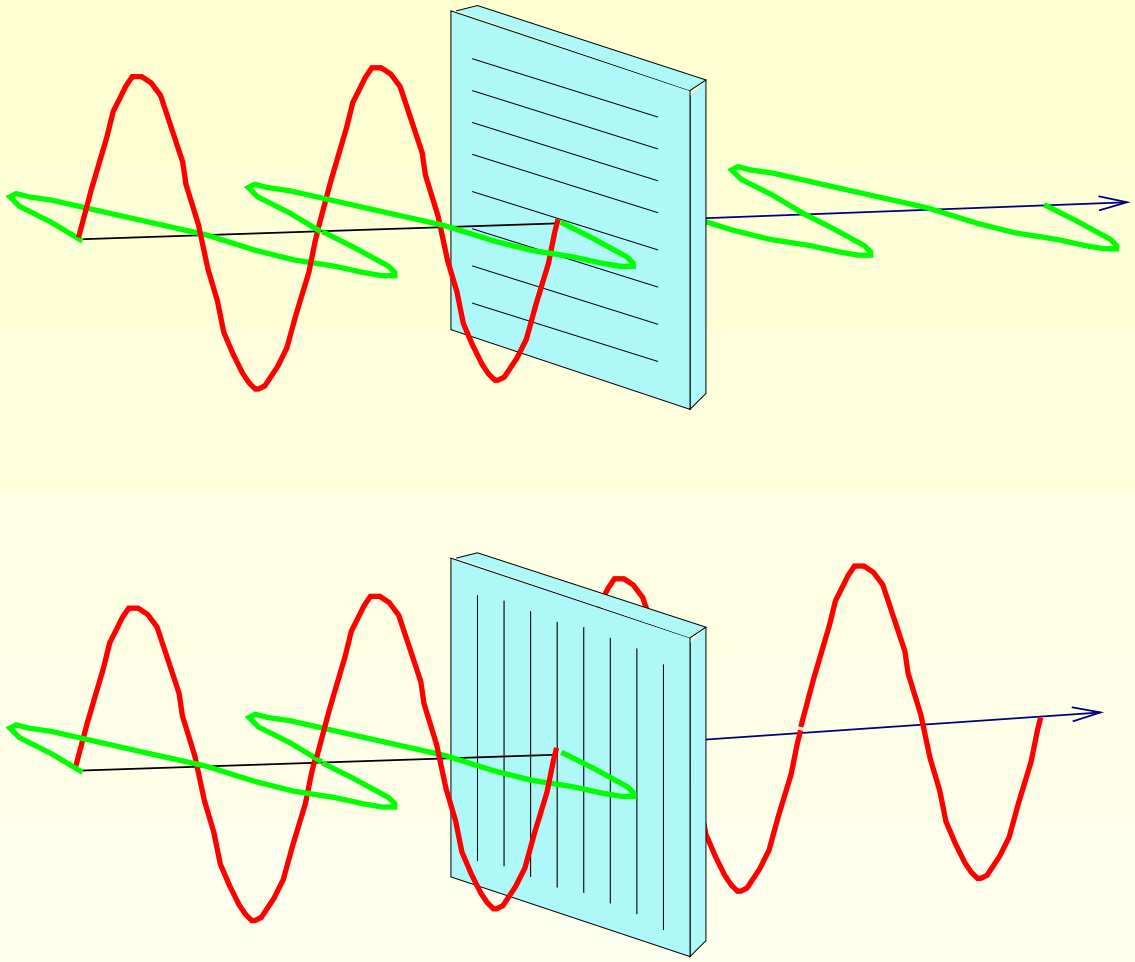
- Ewa wyposażona w komputer kwantowy z łatwością złamie szyfr RSA!

- Czy jest jakieś wyjście?

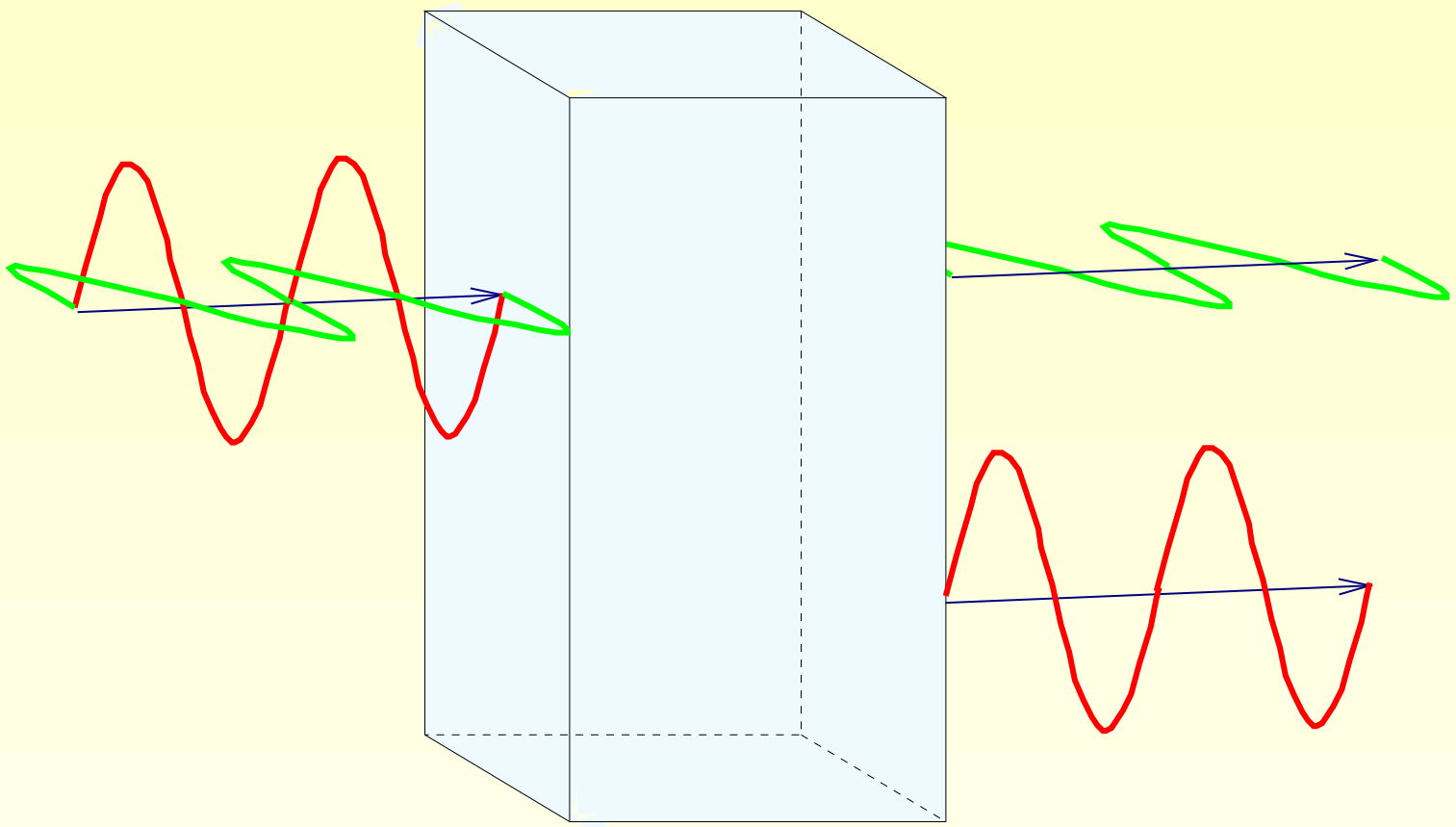
- Tak! Kryptografia kwantowa!

2 Kryptografia kwantowa

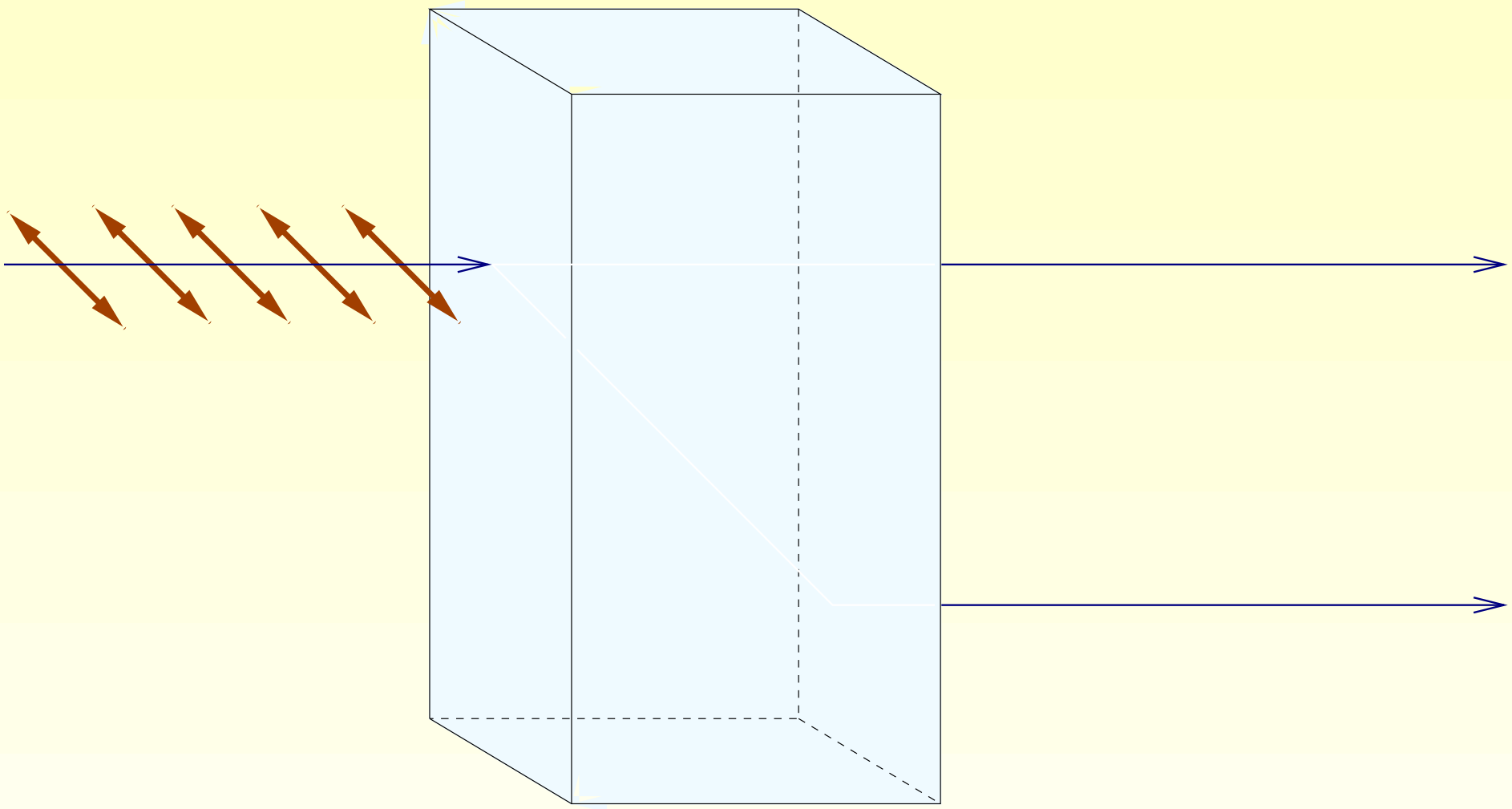
2.1 Polaryzacja światła



Polaryzator przepuszcza światło tylko o określonej polaryzacji: poziomej lub pionowej.

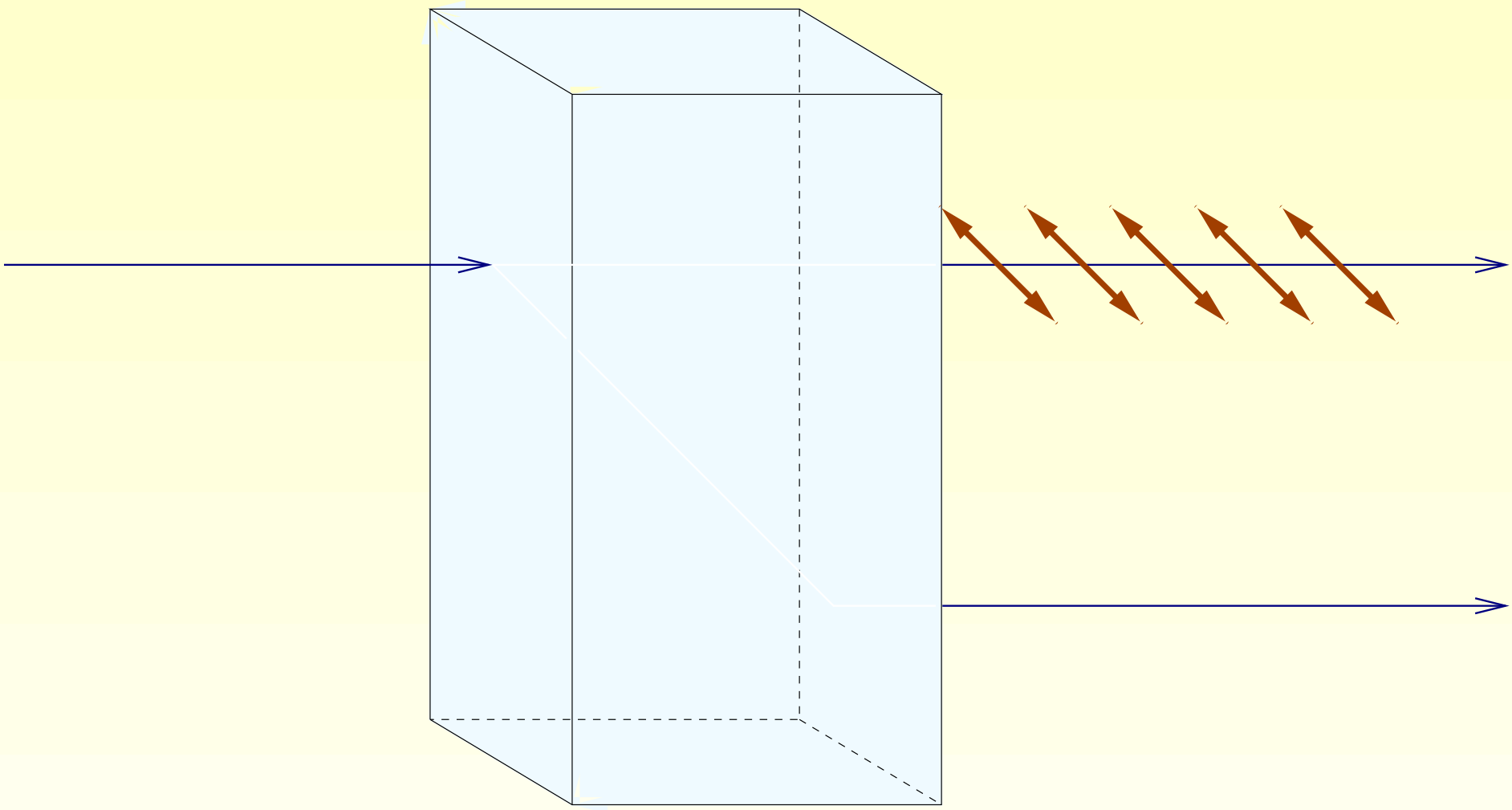


Dwójłomny kryształ kalcytu rozdziela falę świetlną na dwie składowe o wzajemnie prostopadłych polaryzacjach (promień zwyczajny i nadzwyczajny).

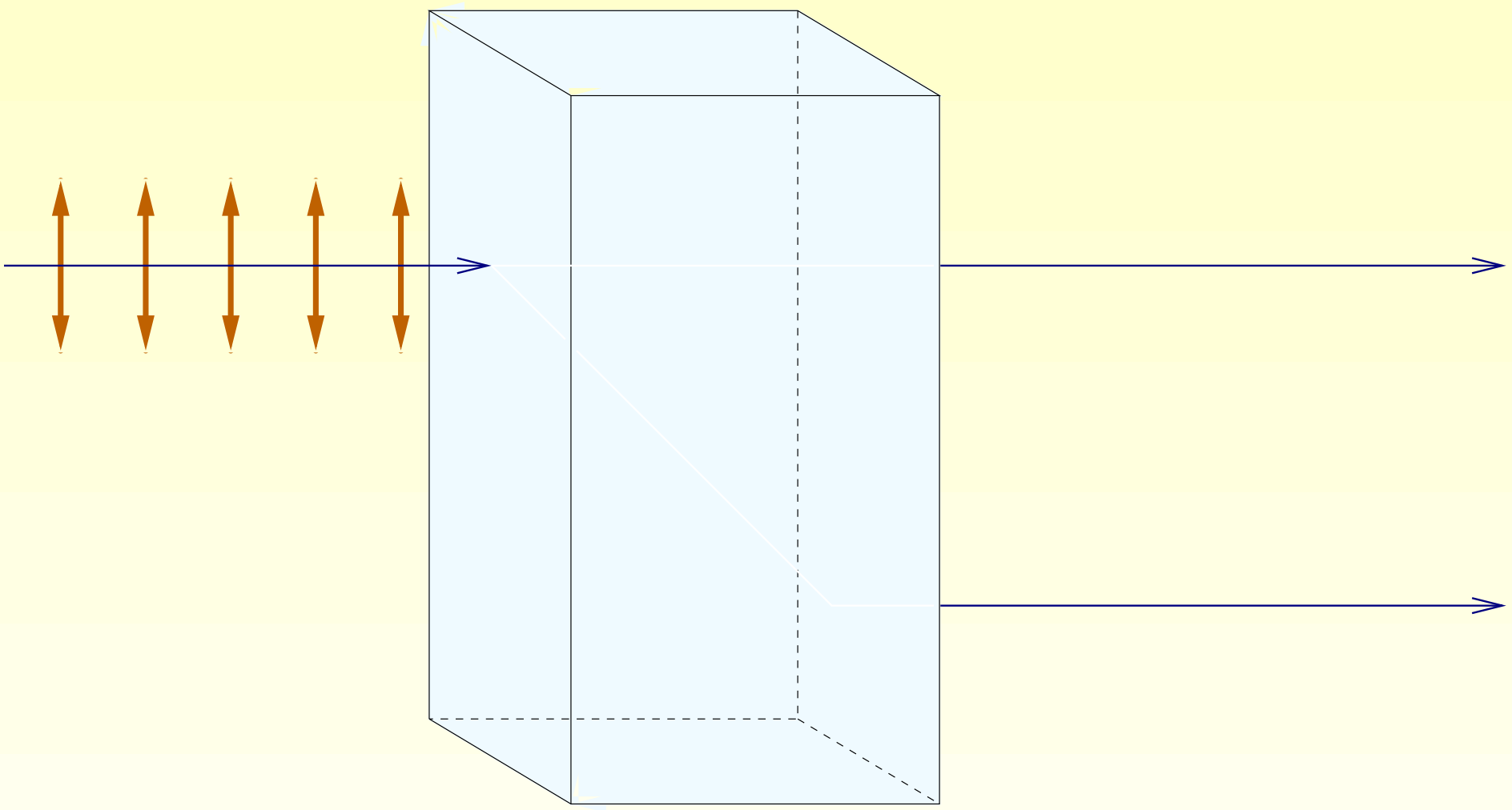


Poziomo spolaryzowane fotony padające na kryształ kalcytu

...

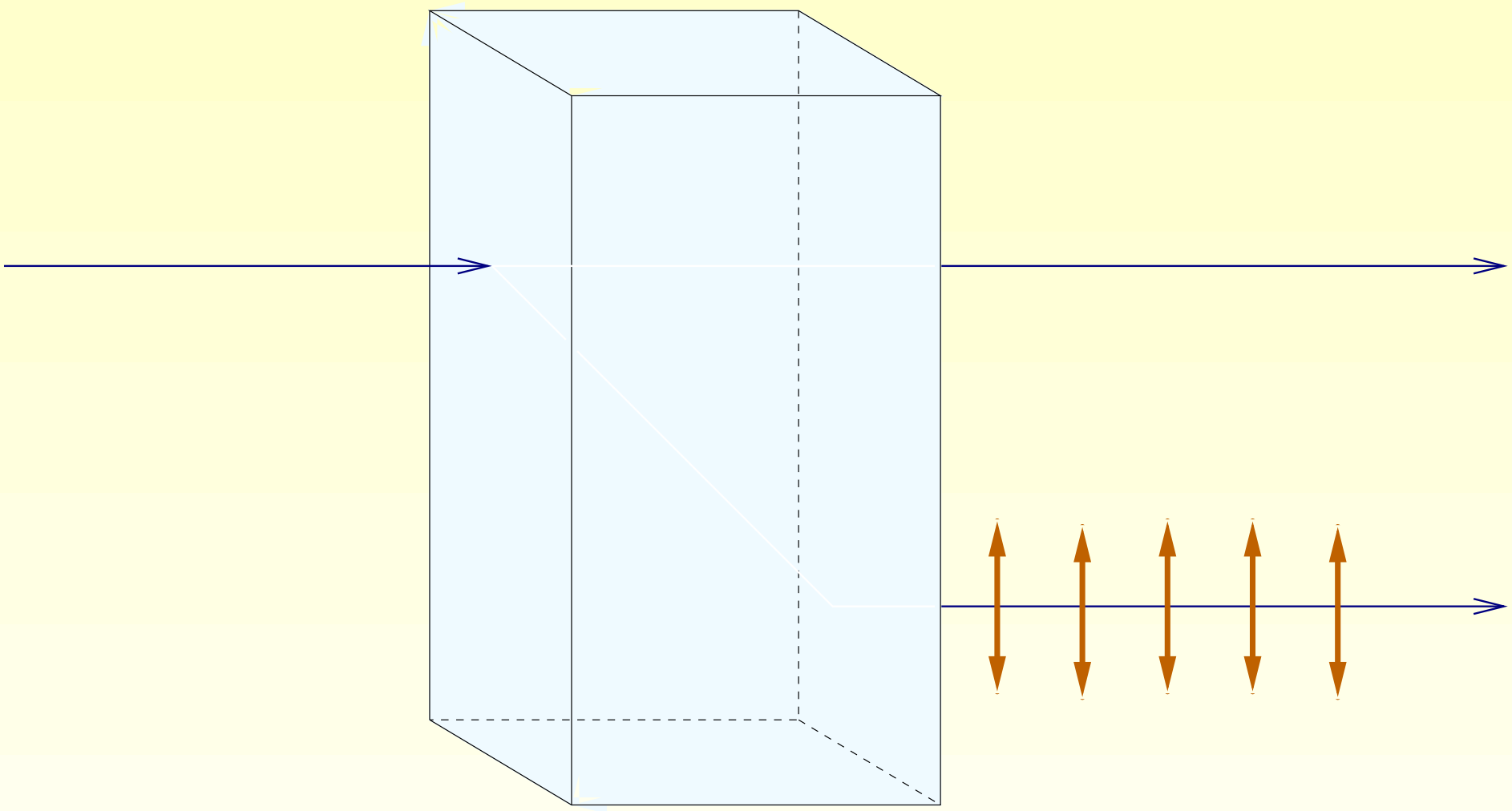


... przechodzą przez kryształ kalcytu bez zmiany kierunku propagacji tworząc promień zwyczajny.

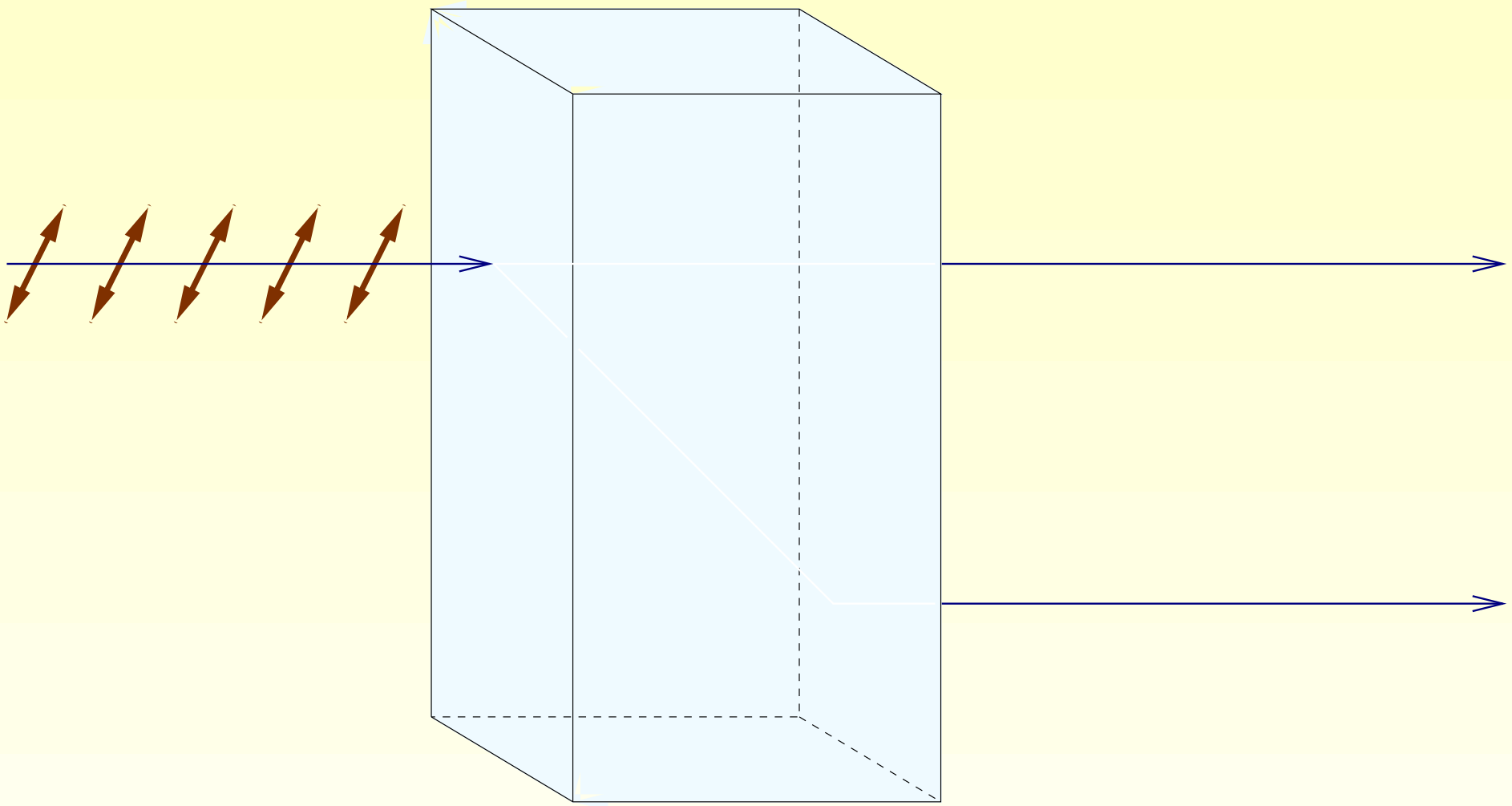


Pionowo spolaryzowane fotony padające na kryształ kalcytu

...

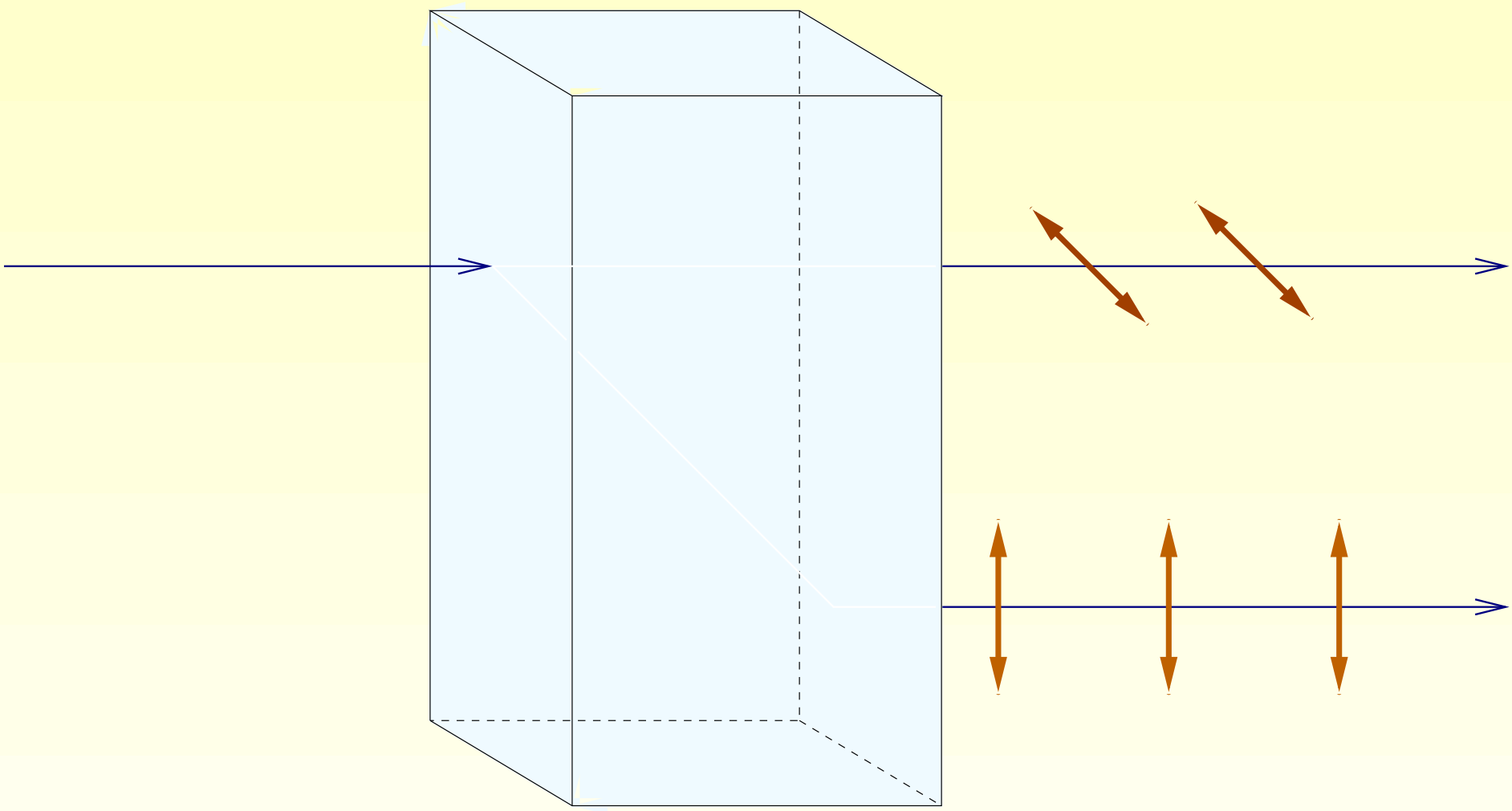


... zostają odchylone tworząc promień nadzwyczajny.

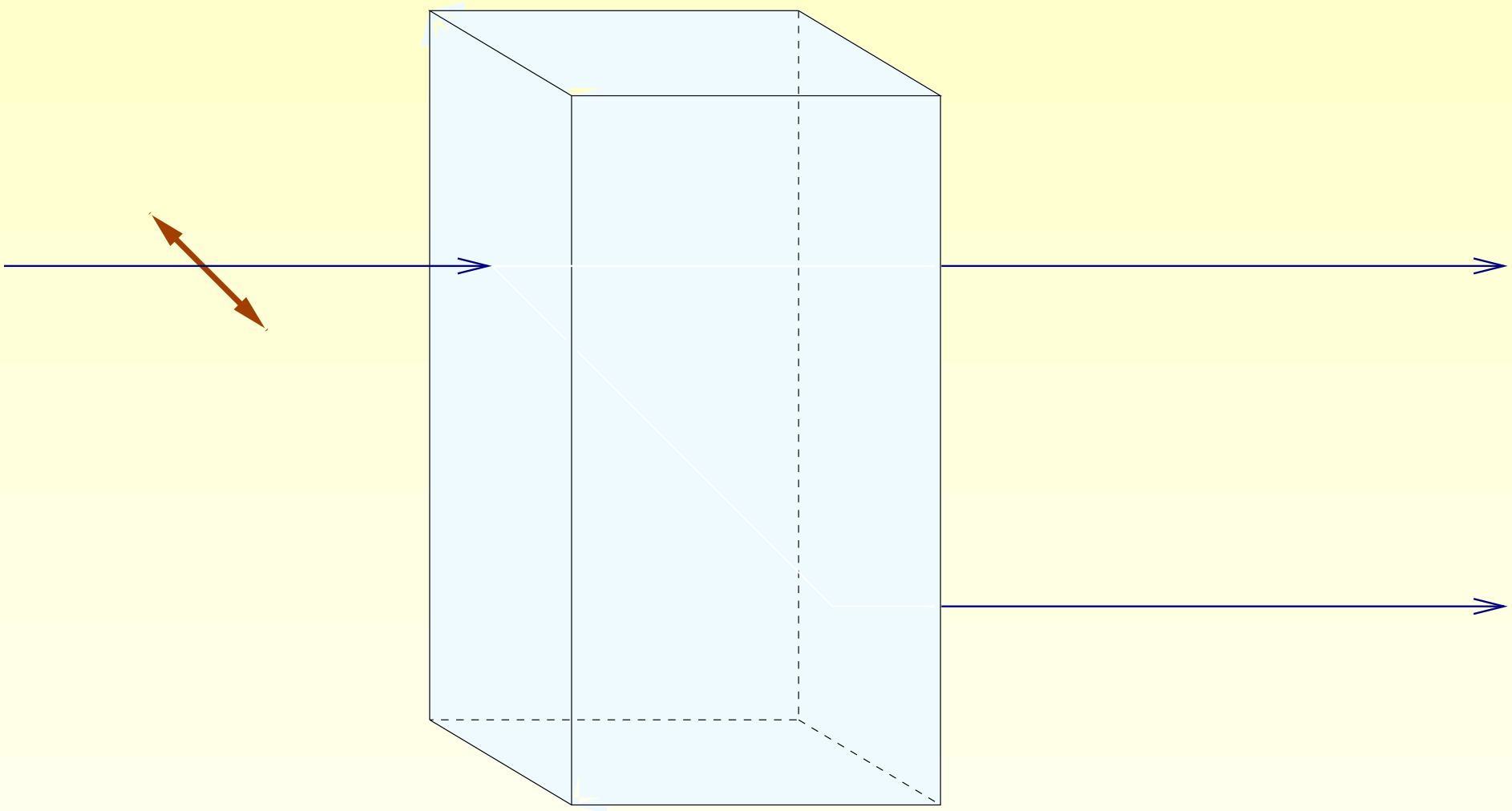


Fotony spolaryzowane ukośnie padające na kryształ kalcytu

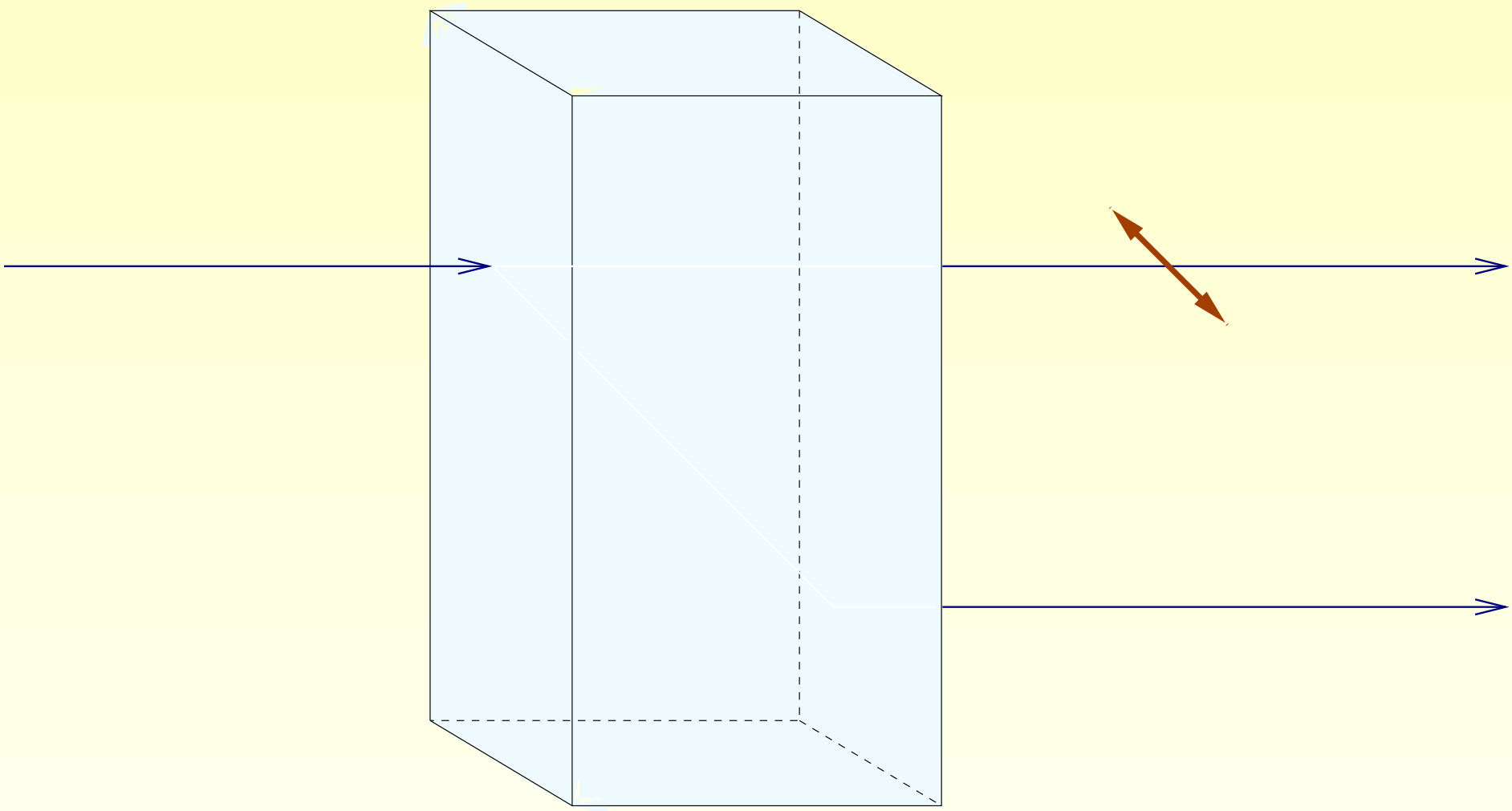
...



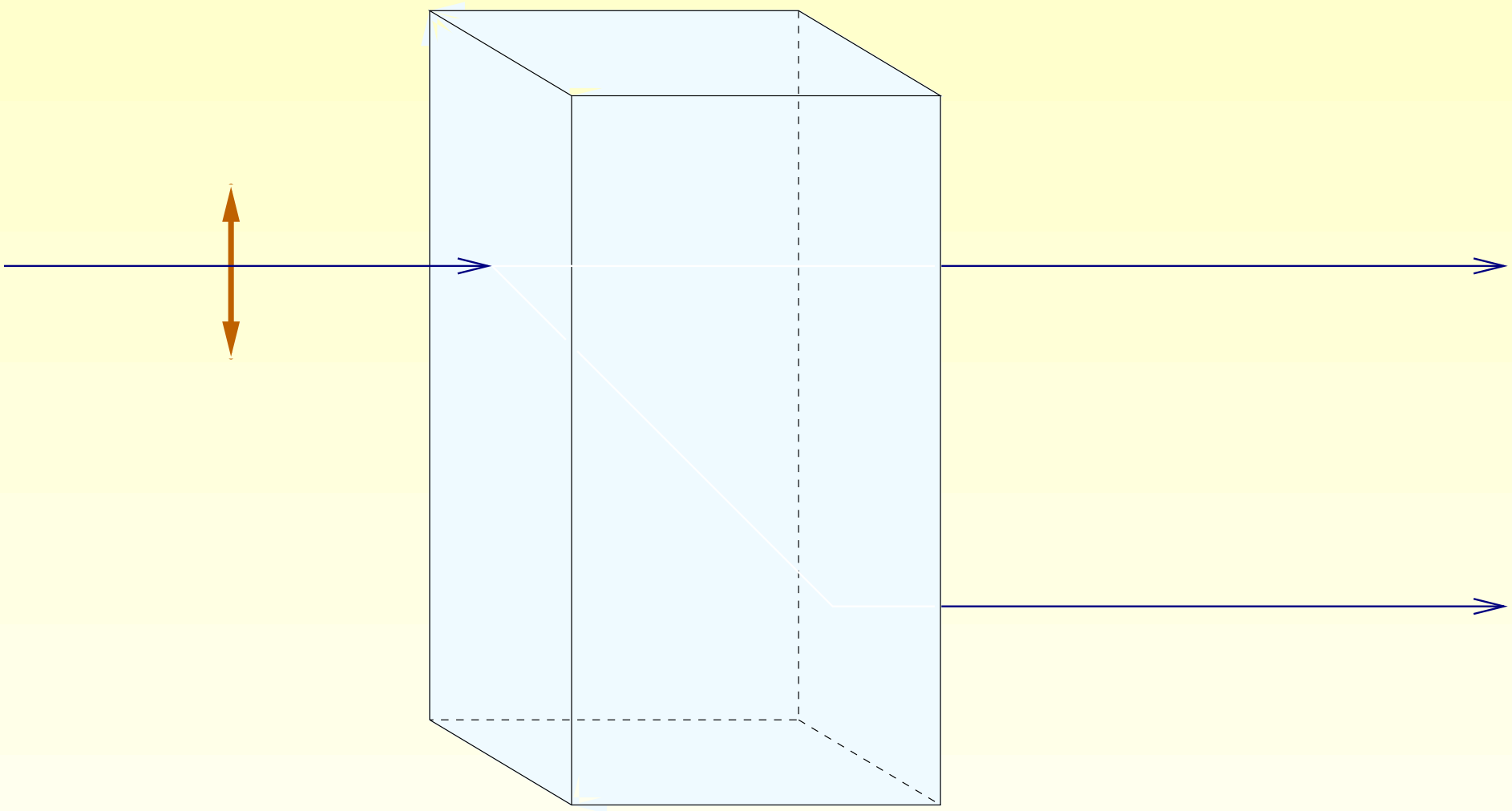
...otrzymują losowo polaryzację poziomą lub pionową i odpowiedni kierunek propagacji.



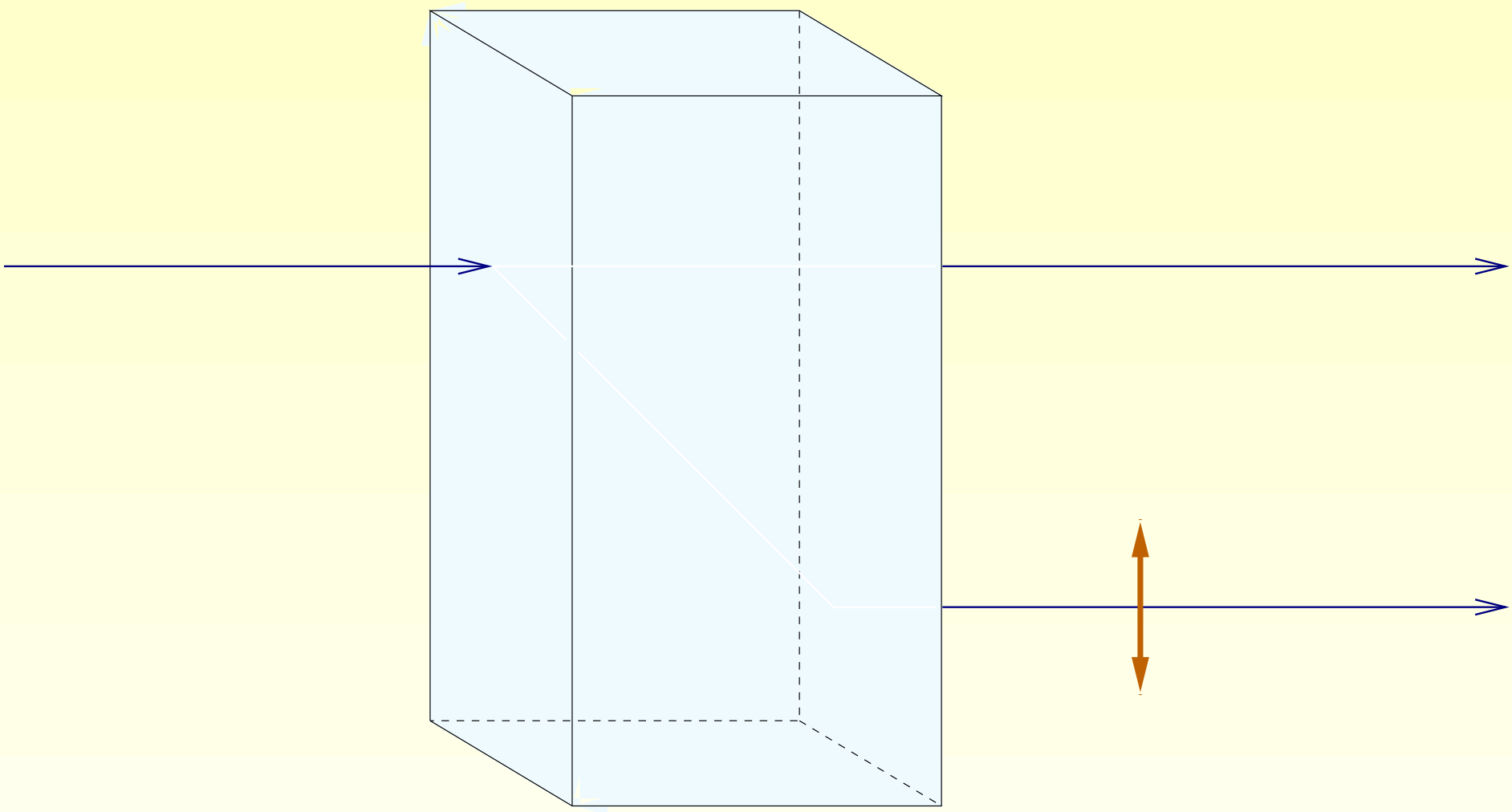
Pojedynczy foton o polaryzacji poziomej ...



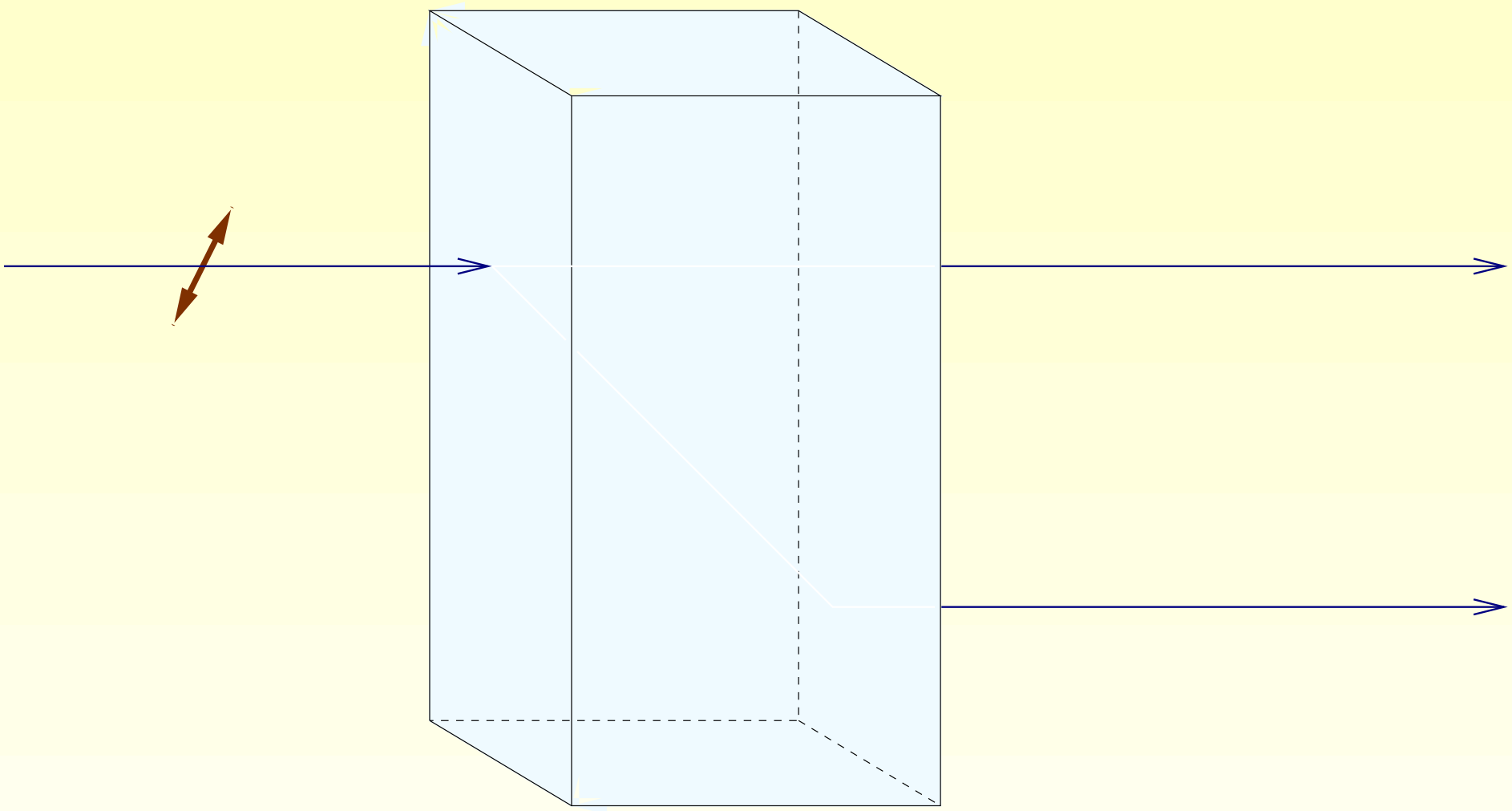
... przechodzi bez zmiany kierunku zachowując polaryzację poziomą.



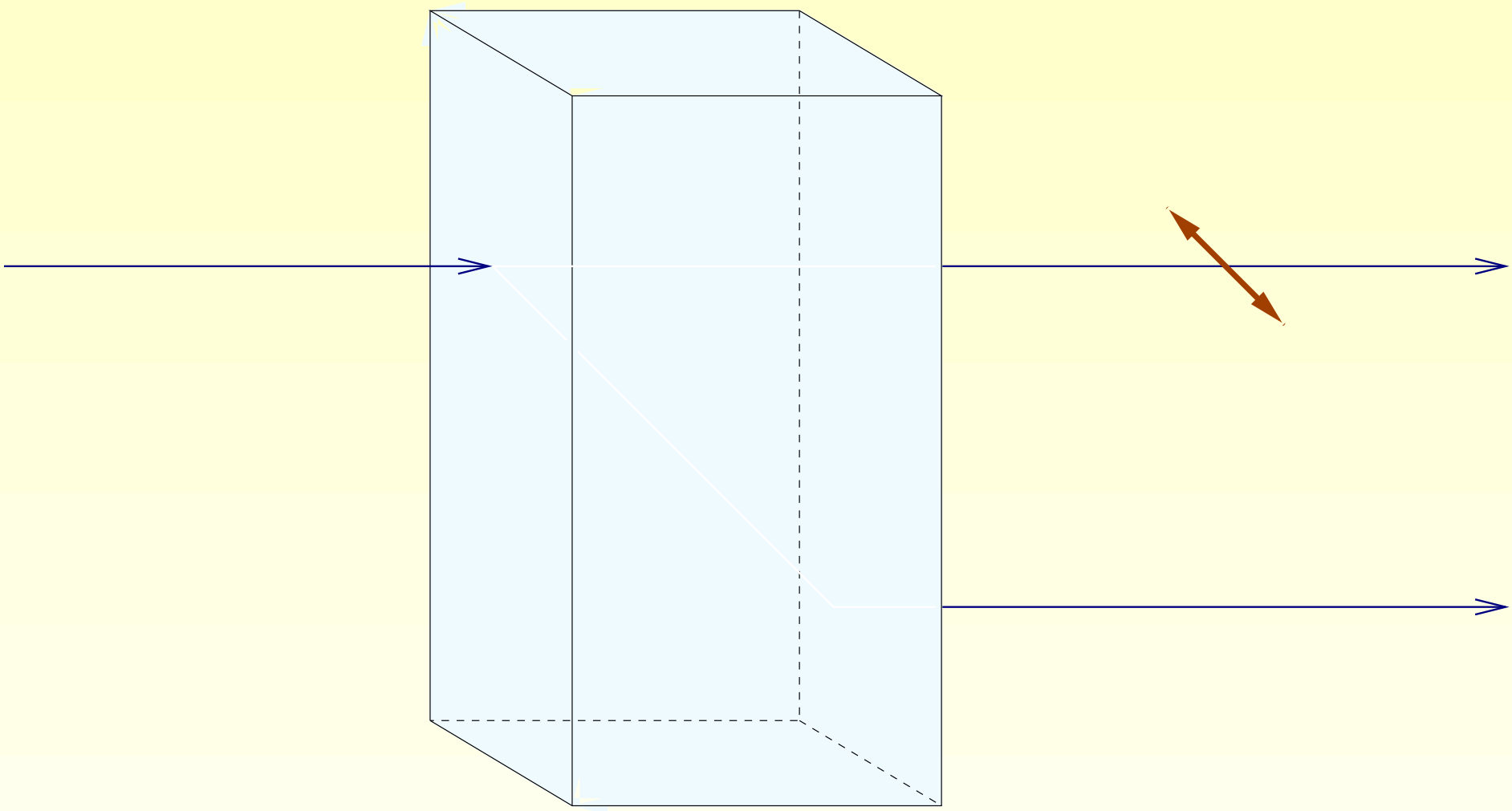
Pojedynczy foton o polaryzacji pionowej ...



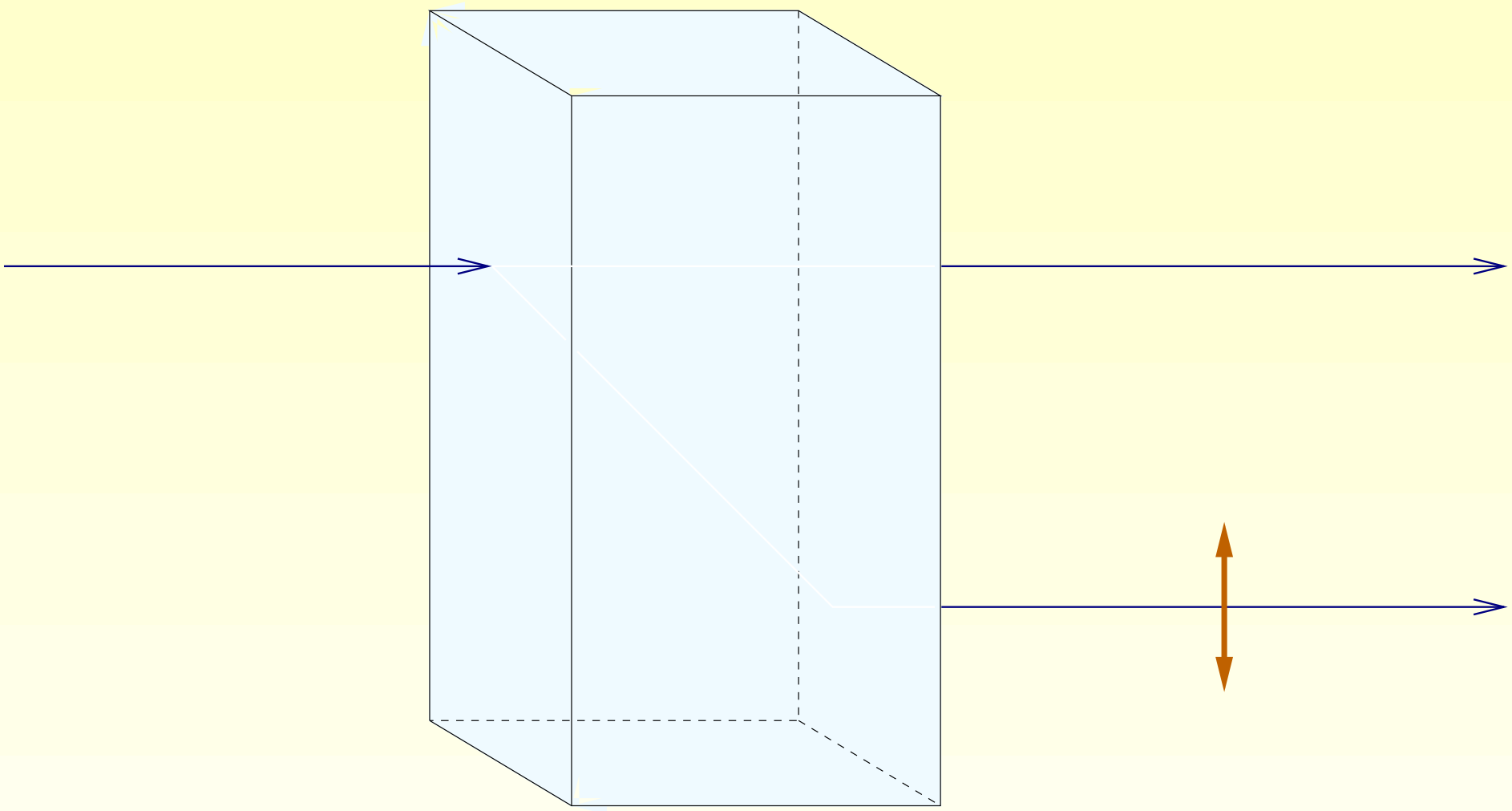
... zmienia kierunek propagacji zachowując polaryzację pionową.



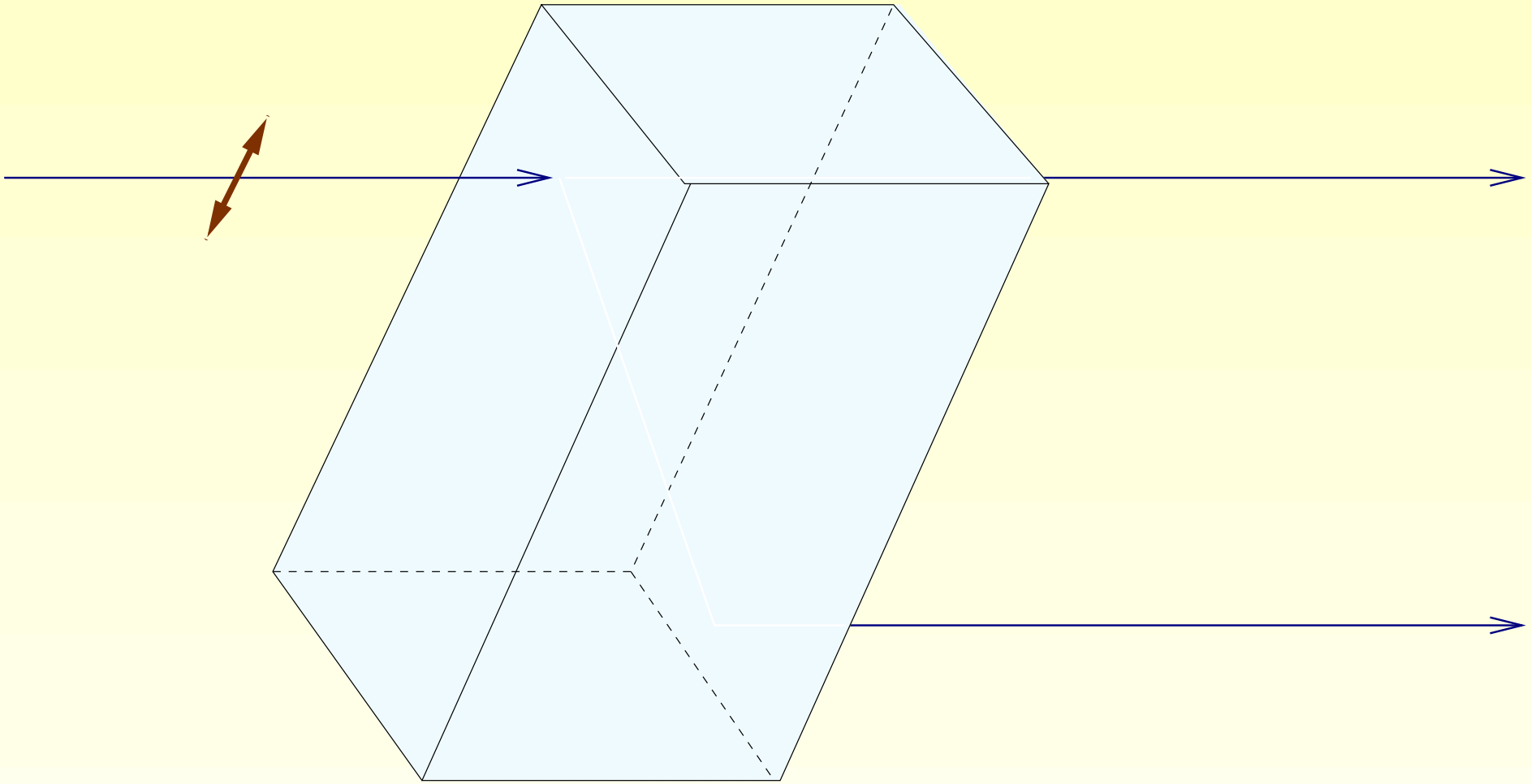
A co z pojedynczym fotonem o polaryzacji ukośnej w stosunku do osi kryształu?



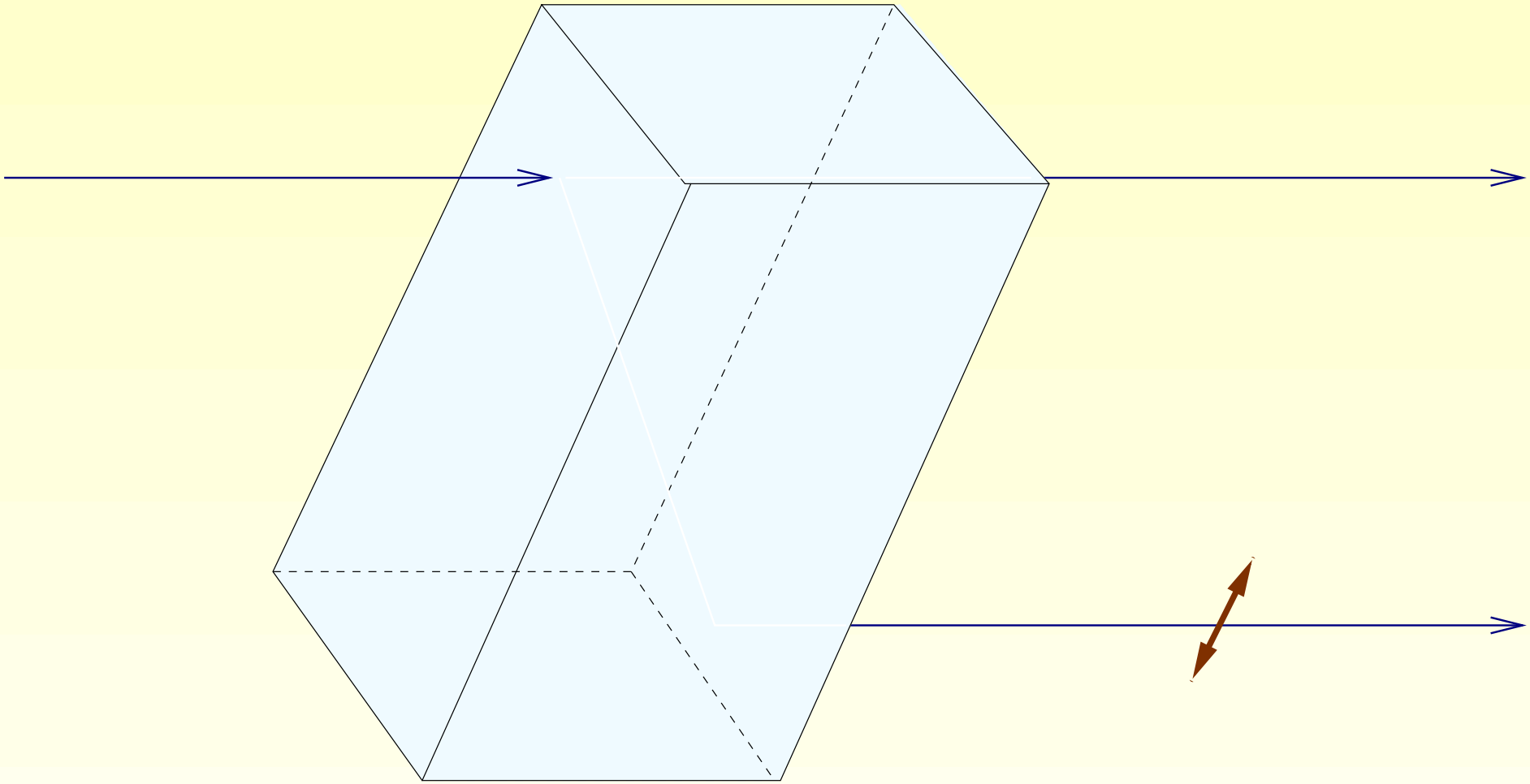
Foton o polaryzacji ukośnej znajdzie się z prawdopodobieństwem 1/2 w wiązce zwyczajnej z polaryzacją poziomą albo ...



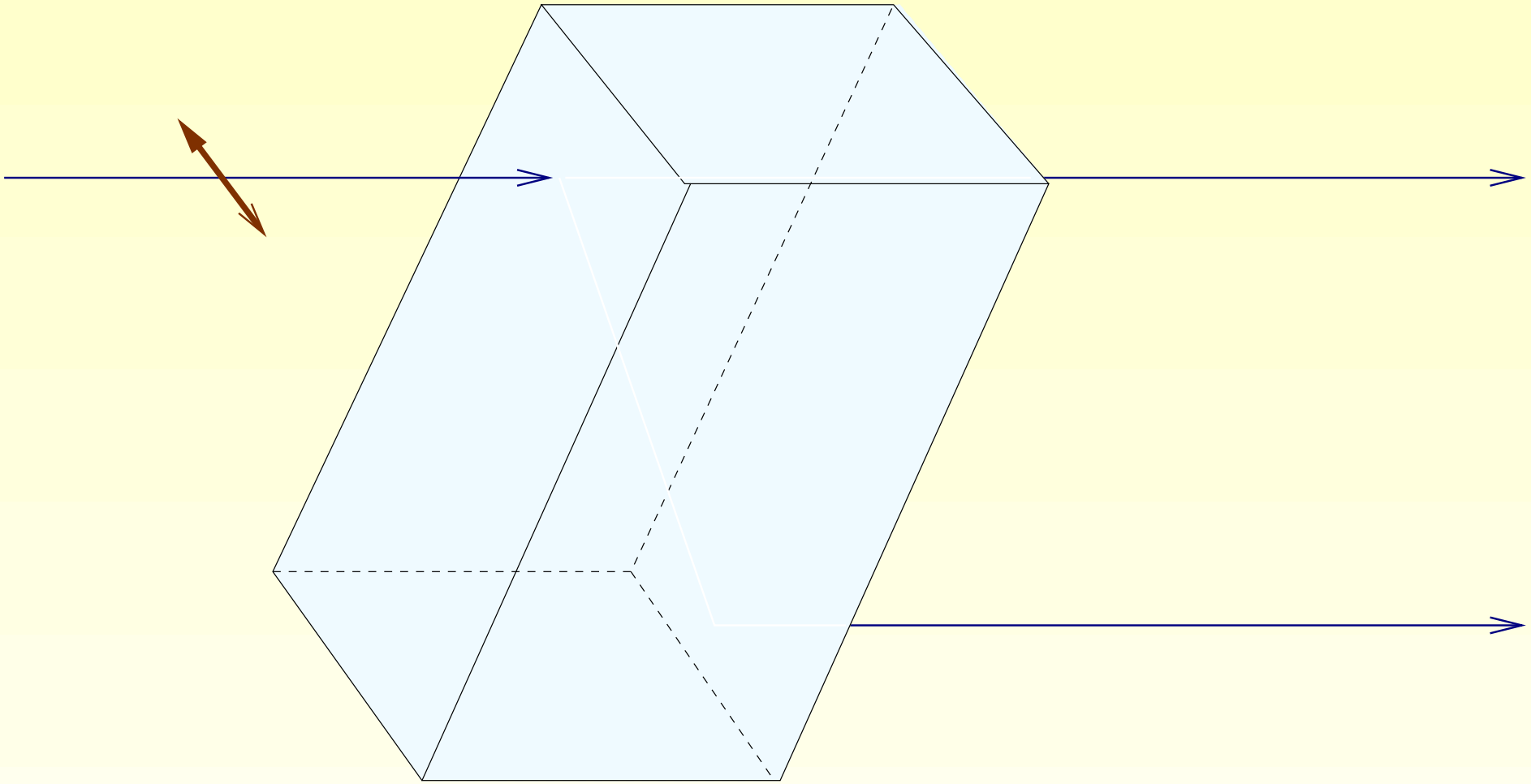
... z prawdopodobieństwem 1/2 w wiązce nadzwyczajnej z polaryzacją pionową. Obie te możliwości są jednakowo prawdopodobne: foton nie niesie już żadnej informacji o poprzedniej polaryzacji.



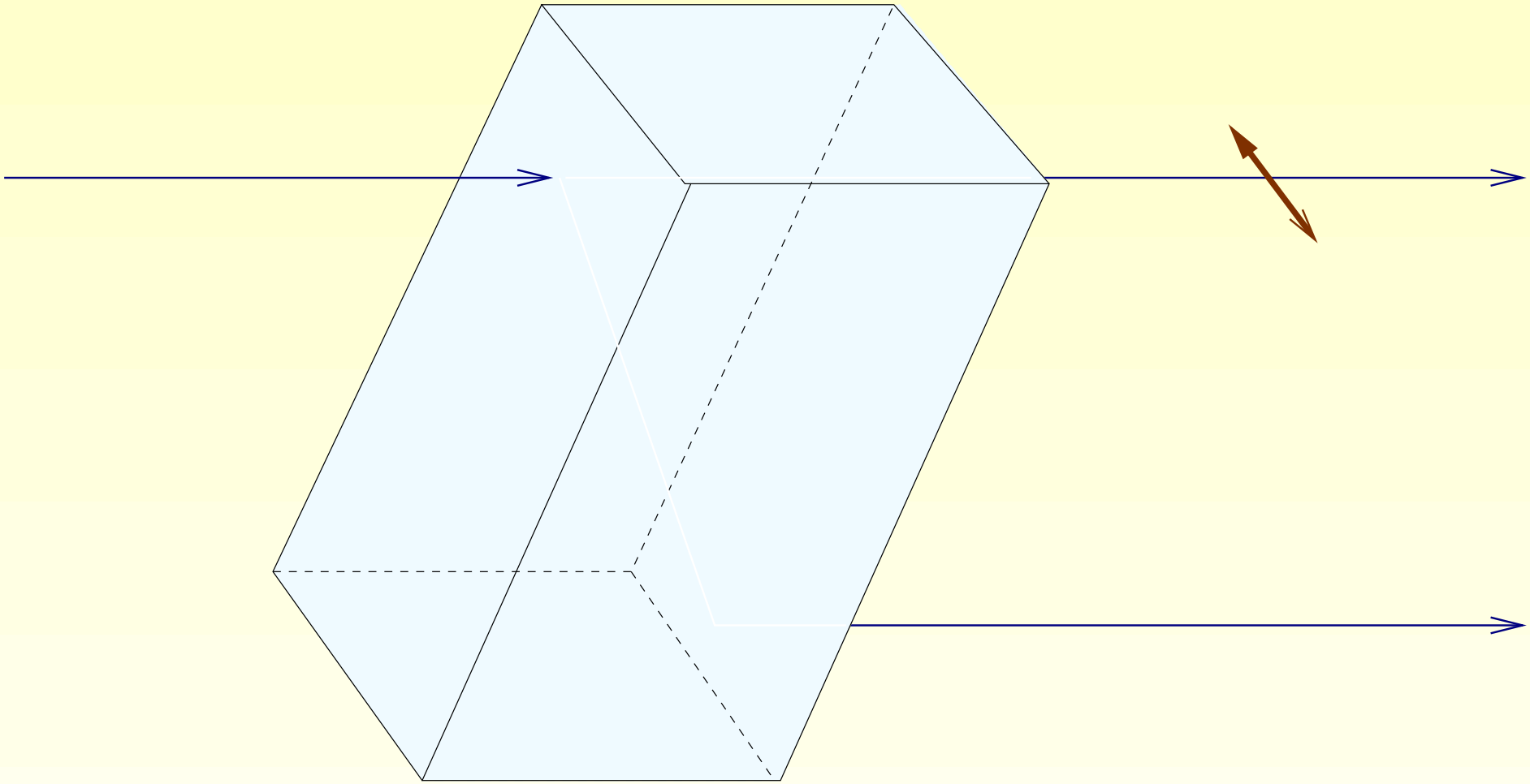
Jeśli obrócimy kryształ o -45° (135°), to foton ukośny -45° staje się fotonem pionowym w nowym układzie i ...



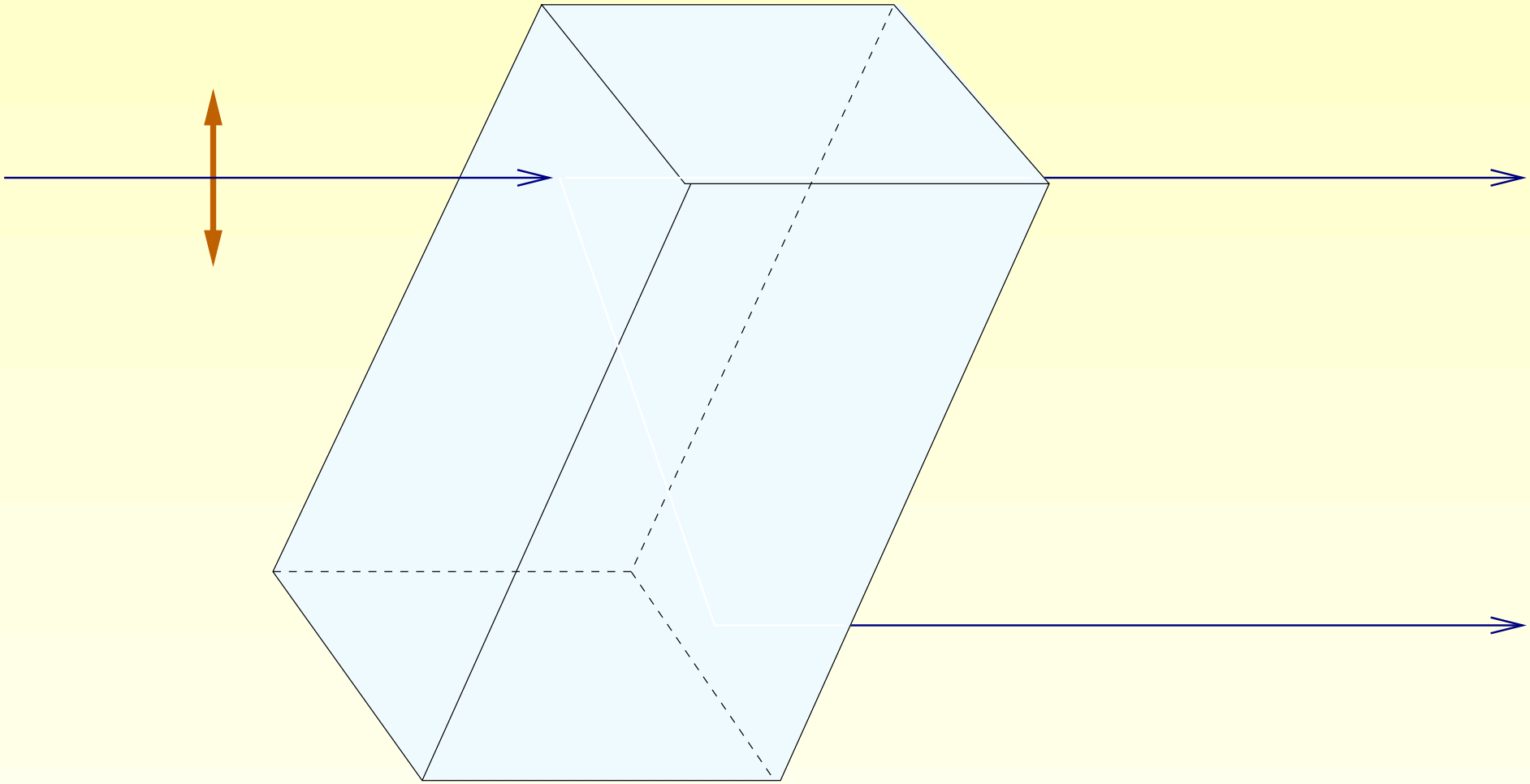
... przechodzi przez kryształ bez zmiany polaryzacji do wiązki nadzwyczajnej.



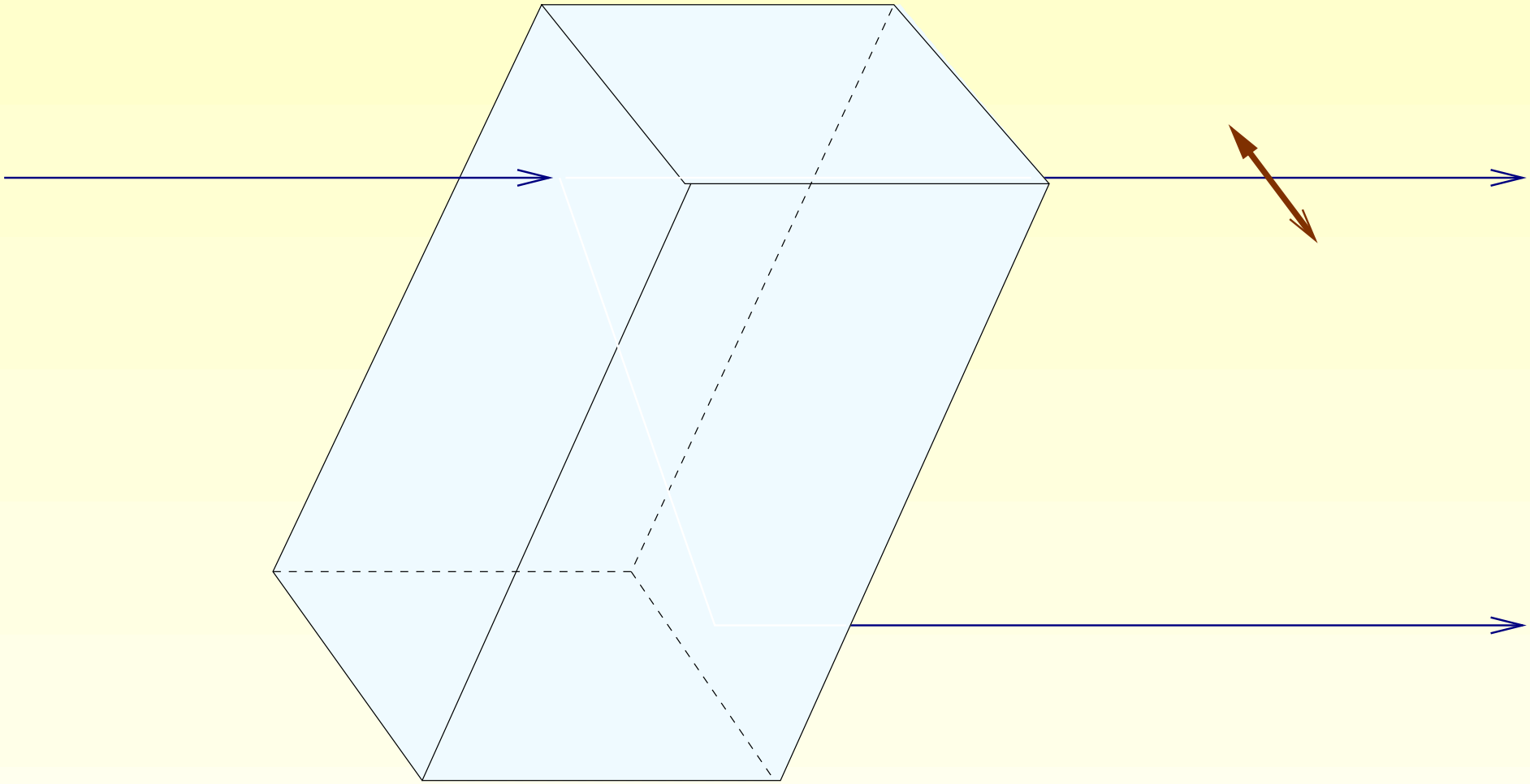
Prostopadły do kierunku -45° foton ukośny 45° staje się dla kryształu fotonem poziomym i ...



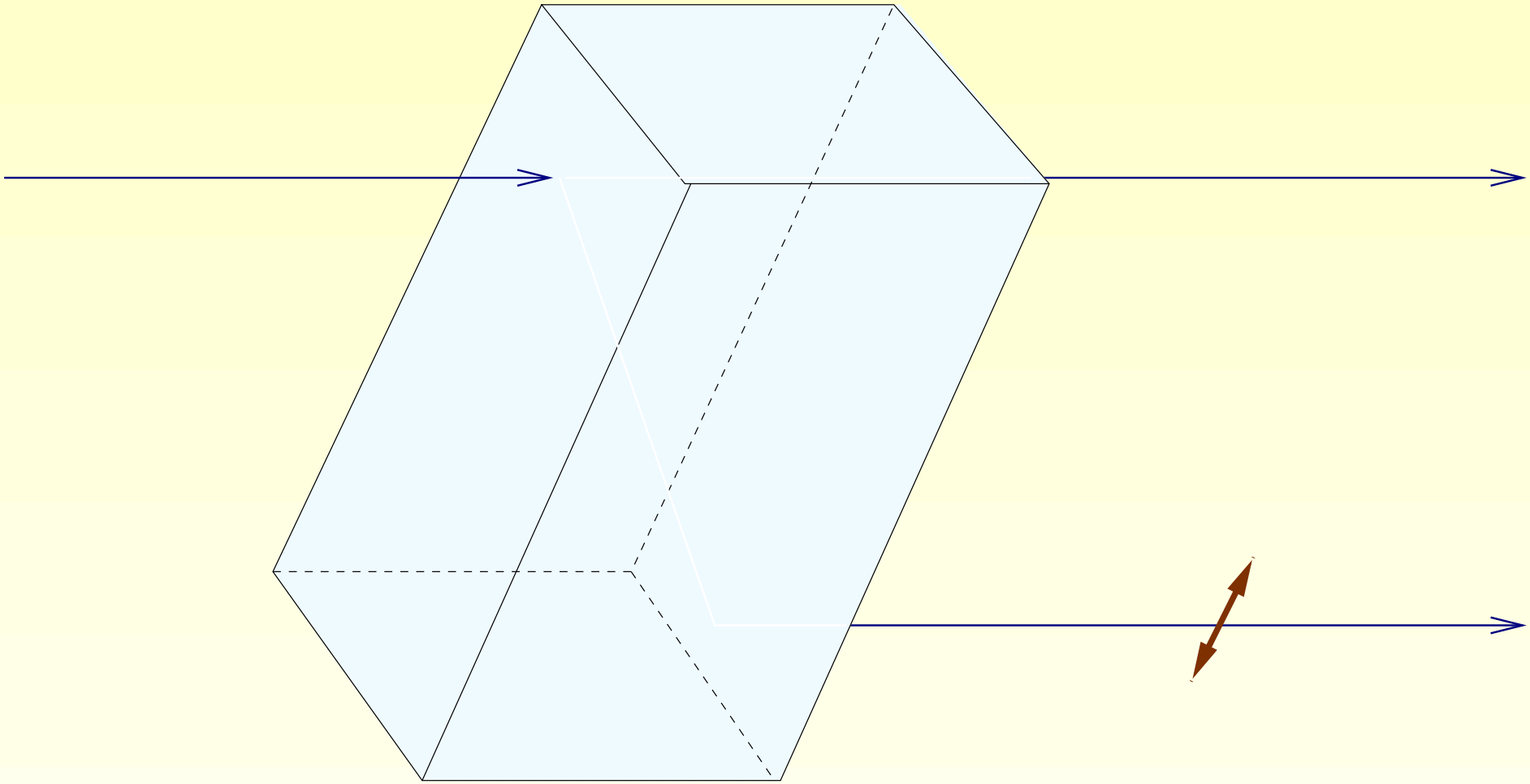
... przechodzi przez kryształ bez zmiany polaryzacji do wiązki zwyczajnej.



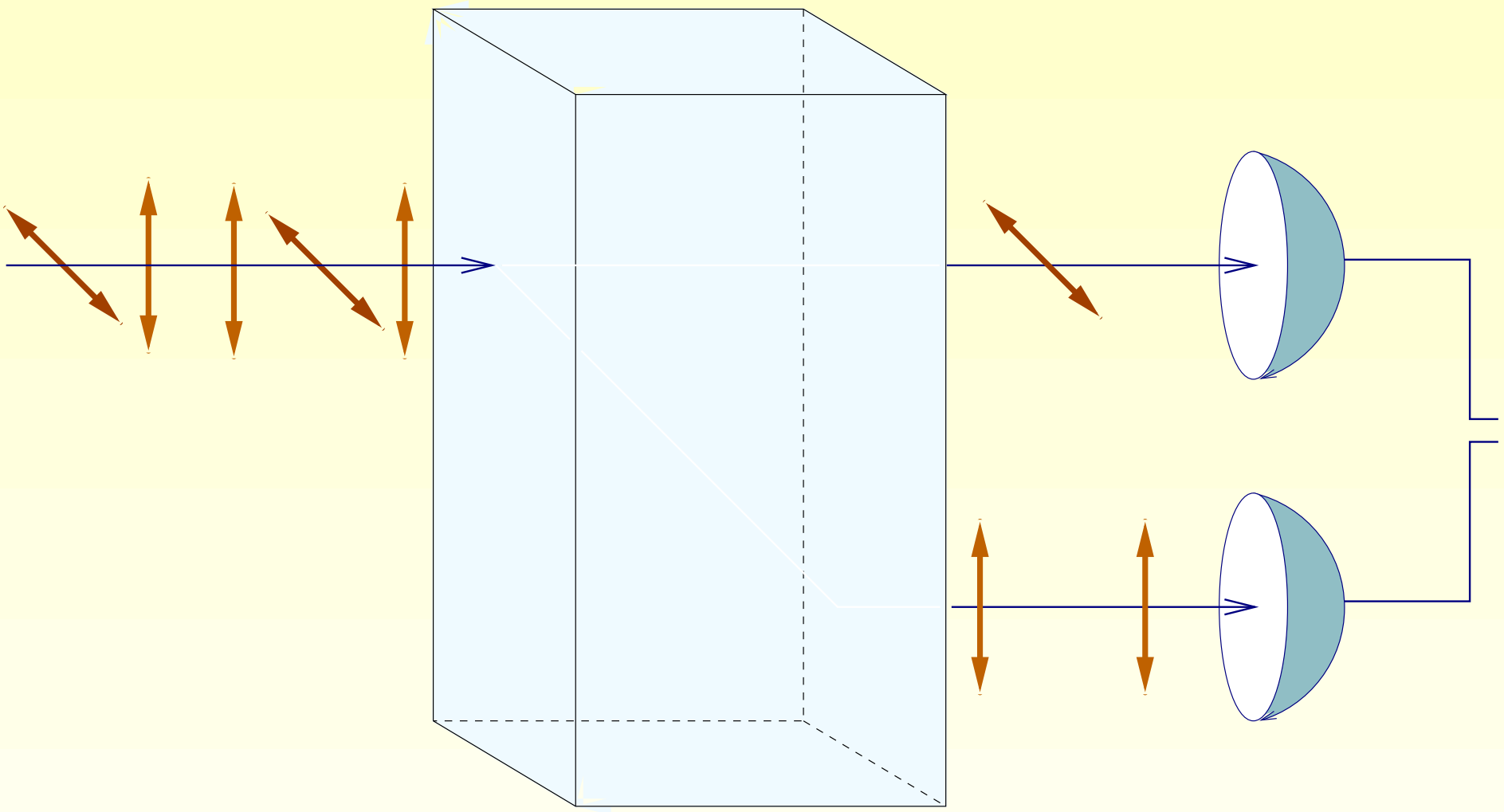
Foton o polaryzacji pionowej (poziomej) staje się ukośnym w stosunku do obróconego kryształu i ...



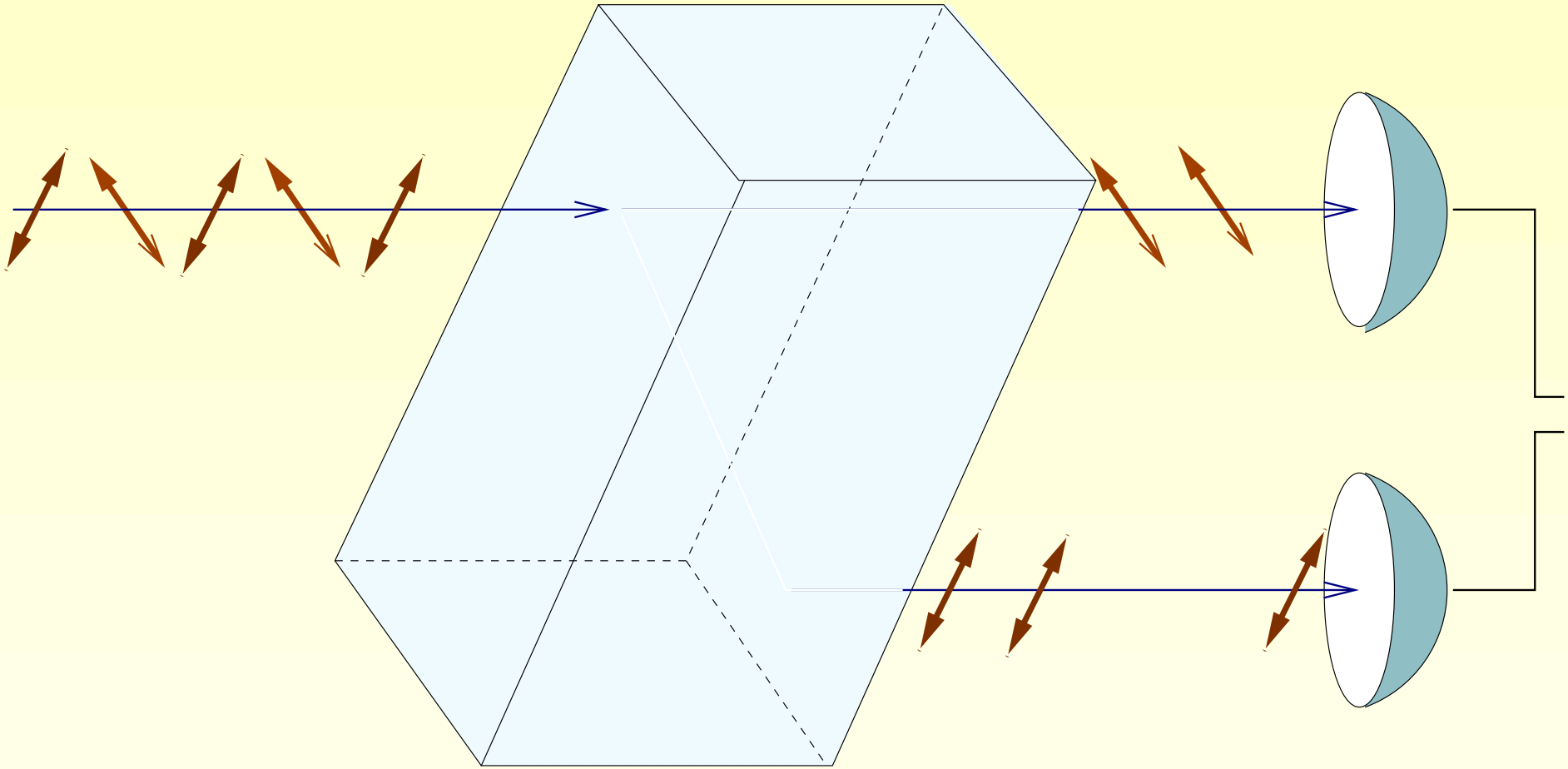
... z prawdopodobieństwem 1/2 przechodzi do wiązki zwyczajnej lub ...



... z prawdopodobieństwem 1/2 do wiązki nadzwyczajnej.
Znowu obie możliwości są jednakowo prawdopodobne i pomiar polaryzacji fotonu pionowego obróconym kryształem nie daje żadnej informacji o polaryzacji tego fotonu.



Dodając dwa detektory fotonów otrzymujemy przyrząd do pomiaru polaryzacji w bazie prostej, w której mierzy się w sposób pewny (bezbłędny) fotony o polaryzacjach 0° i 90°.



Obracając kryształ kalcytu o -45° (135°) otrzymujemy przyrząd do pomiaru polaryzacji w bazie ukośnej, w której mierzy się w sposób pewny (bezbłędny) fotony o polaryzacjach 45° i 135°.

- Kryształ kalcytu plus dwa detektory fotonów rejestrujące fotony z wiązki zwyczajnej i nadzwyczajnej nadaje się do rejestracji polaryzacji fotonów o kierunkach 0° i 90°. Takie ustawienie kryształu wyznacza tzw. bazę prostą.

- Kryształ kalcytu plus dwa detektory fotonów rejestrujące fotony z wiązki zwyczajnej i nadzwyczajnej nadaje się do rejestracji polaryzacji fotonów o kierunkach 0° i 90°. Takie ustawienie kryształu wyznacza tzw. bazę prostą.

- Pomiary w bazie prostej nie dają żadnych informacji o polaryzacji ukośnej, tzn. o polaryzacji fotonów padających na kryształ i spolaryzowanych liniowo pod kątem 45° lub 135° do osi kryształu.

- Kryształ kalcytu plus dwa detektory fotonów rejestrujące fotony z wiązki zwyczajnej i nadzwyczajnej nadaje się do rejestracji polaryzacji fotonów o kierunkach 0° i 90°. Takie ustawienie kryształu wyznacza tzw. bazę prostą.

- Pomiary w bazie prostej nie dają żadnych informacji o polaryzacji ukośnej, tzn. o polaryzacji fotonów padających na kryształ i spolaryzowanych liniowo pod kątem 45° lub 135° do osi kryształu.

- Aby mierzyć polaryzację ukośną należy obrócić oś kryształu o 45° (lub 135°) i wtedy urządzenie będzie mierzyło polaryzację 45° i 135°. Takie ustawienie kryształu wyznacza tzw. bazę ukośną.

- Pomiary w bazie ukośnej, z kolei, nie dają żadnej informacji o polaryzacji prostej.

- Pomiary w bazie ukośnej, z kolei, nie dają żadnej informacji o polaryzacji prostej.
- Polaryzacja prosta i polaryzacja ukośna to dwie wielkości fizyczne, które zgodnie z prawami mechanikii kwantowej nie są współmierzalne. Pomiar jednej z nich czyni drugą całkowicie nieokreśloną. Mamy tu do czynienia z zasadą nieoznaczoności Heisenberga.

- Pomiary w bazie ukośnej, z kolei, nie dają żadnej informacji o polaryzacji prostej.
- Polaryzacja prosta i polaryzacja ukośna to dwie wielkości fizyczne, które zgodnie z prawami mechanikii kwantowej nie są współmierzalne. Pomiar jednej z nich czyni drugą całkowicie nieokreśloną. Mamy tu do czynienia z zasadą nieoznaczoności Heisenberga.
- Mechanika kwantowa, jak się okazuje, umożliwia bezpieczne przekazywanie klucza kryptograficznego!

- Pomiary w bazie ukośnej, z kolei, nie dają żadnej informacji o polaryzacji prostej.
- Polaryzacja prosta i polaryzacja ukośna to dwie wielkości fizyczne, które zgodnie z prawami mechanikii kwantowej nie są współmierzalne. Pomiar jednej z nich czyni drugą całkowicie nieokreśloną. Mamy tu do czynienia z zasadą nieoznaczoności Heisenberga.
- Mechanika kwantowa, jak się okazuje, umożliwia bezpieczne przekazywanie klucza kryptograficznego!

  Zaraz zobaczymy w jaki sposób!

2.2 Alfabety kwantowe

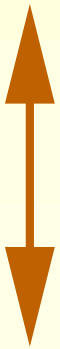
2.2 Alfabety kwantowe

Alfabet prosty

2.2 Alfabety kwantowe

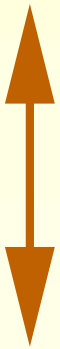
Alfabet prosty


=0


=1

2.2 Alfabety kwantowe

Alfabet prosty

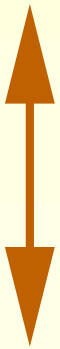


Alfabet ukośny

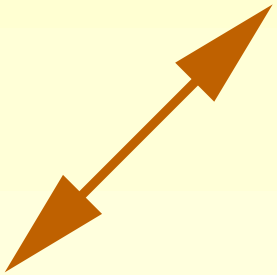
2.2 Alfabety kwantowe

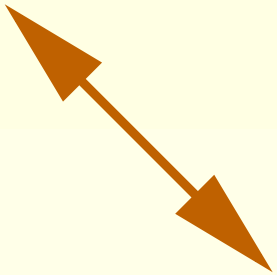
Alfabet prosty


=0


=1

Alfabet ukośny

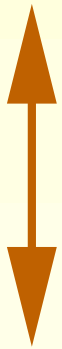

=0


=1

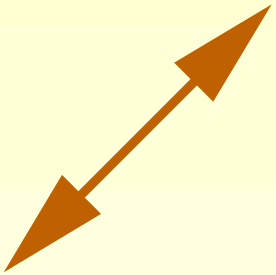
2.2 Alfabety kwantowe

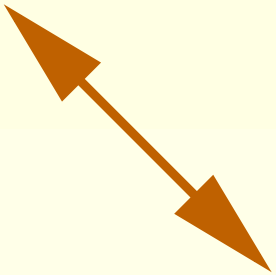
Alfabet prosty


=0


=1

Alfabet ukośny


=0

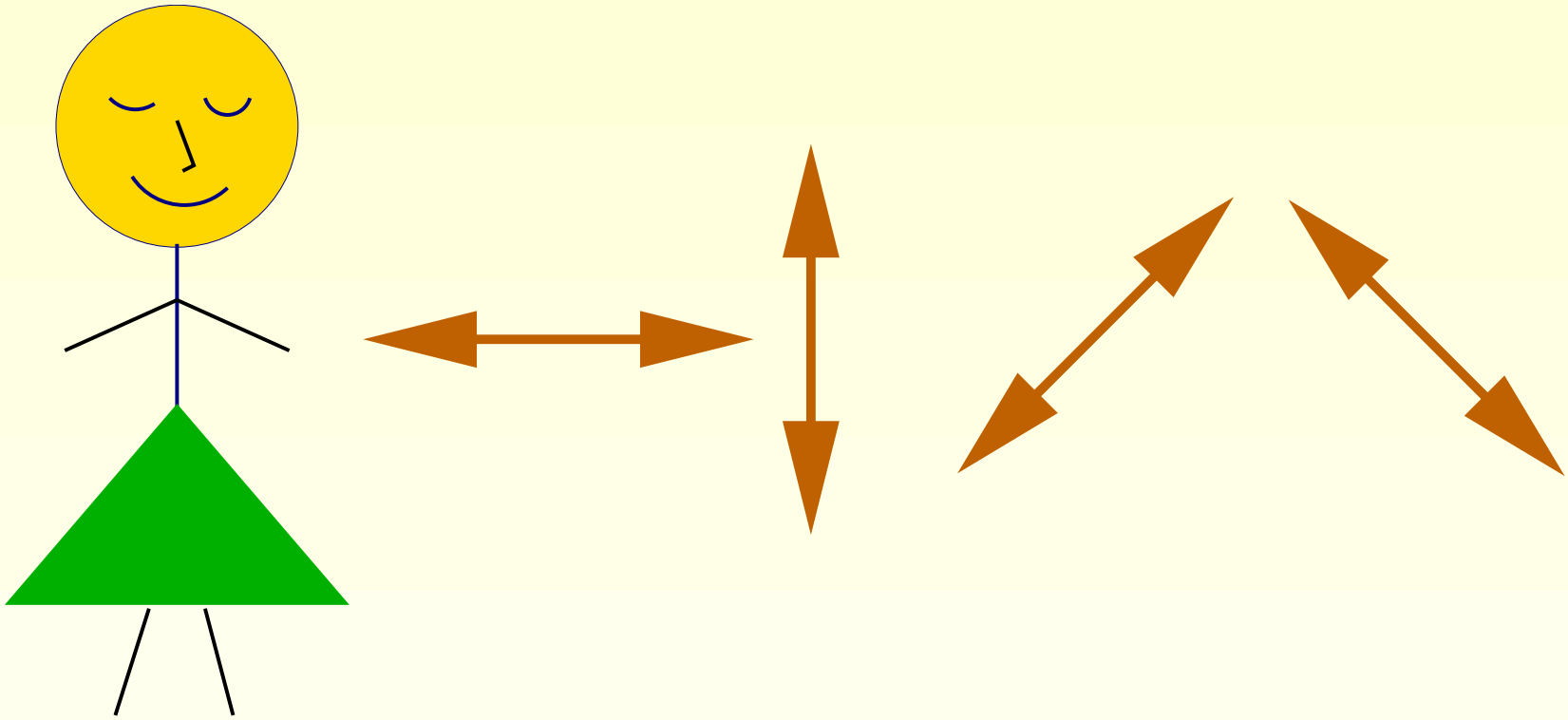

=1

Dysponujemy dwoma różnymi alfabetami kwantowymi. Dwie wzajemnie prostopadłe polaryzacje stanowią znaki alfabetu, którym możemy przypisać wartości binarne 0 lub 1 i w ten sposób kodować informację, którą chcemy przesłać kanałem kwantowym.

2.3 Protokół BB84 (Bennett i Brassard, 1984)

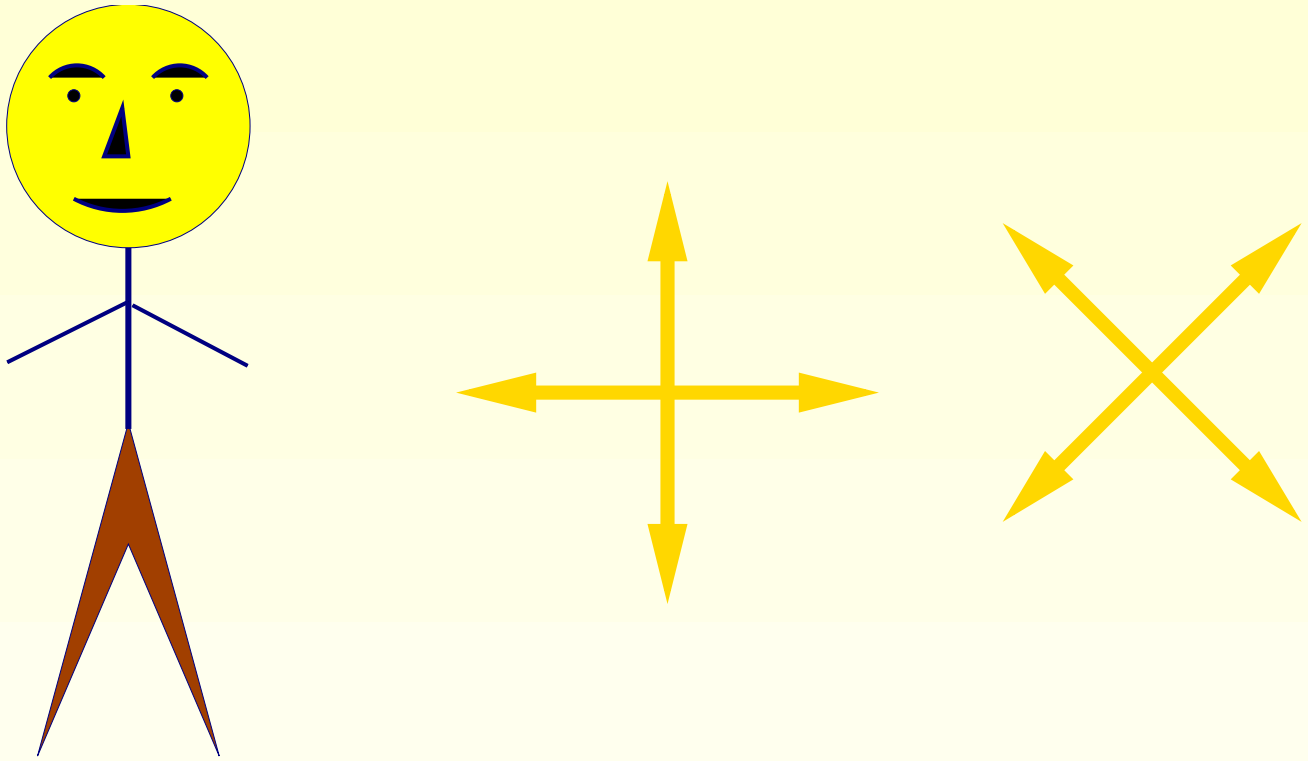
2.3 Protokół BB84 (Bennett i Brassard, 1984)

Krok 1



Alicja wybiera losowo jedną z czterech możliwych polaryzacji i wysyła do Bolka foton o takiej polaryzacji. Ciąg fotonów stanowi ciąg zer i jedynek z dwóch alfabetów kwantowych.

Krok 2



Bolek wybiera losowo bazę prostą lub ukośną i wykonuje pomiar polaryzacji fotonu, który otrzymał od Alicji.

Krok 3

Bolek notuje wyniki pomiarów zachowując je w tajemnicy.

Krok 3

Bolek notuje wyniki pomiarów zachowując je w tajemnicy.

Krok 4

Bolek publicznie informuje Alicję jakiej bazy używał do pomiaru, zaś Alicja informuje go czy wybrany losowo typ pomiaru (baza prosta lub ukośna) był właściwy czy nie.

Krok 3

Bolek notuje wyniki pomiarów zachowując je w tajemnicy.

Krok 4

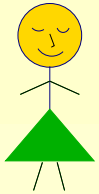
Bolek publicznie informuje Alicję jakiej bazy używał do pomiaru, zaś Alicja informuje go czy wybrany losowo typ pomiaru (baza prosta lub ukośna) był właściwy czy nie.

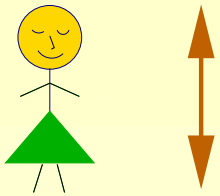
Krok 5

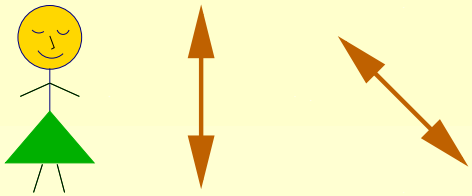
Alicja i Bolek przechowują wyniki pomiarów, dla których Bolek użył właściwej bazy. Wyniki tych pomiarów można zapisać w postaci binarnej

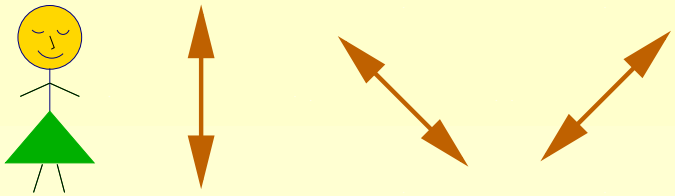
przypisując zera polaryzacji 0° i 45° zaś jedynki polaryzacji 90° i 135°. Uzyskany w ten sposób losowy ciąg zer i jedynek może stanowić klucz kryptograficzny.

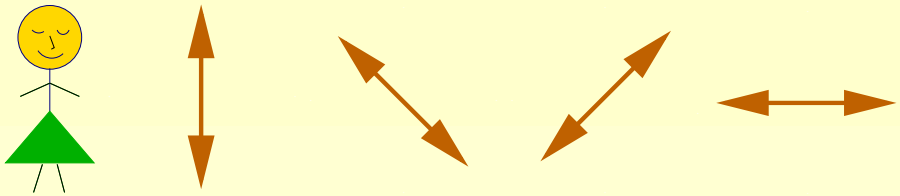
2.4 Jak to działa?

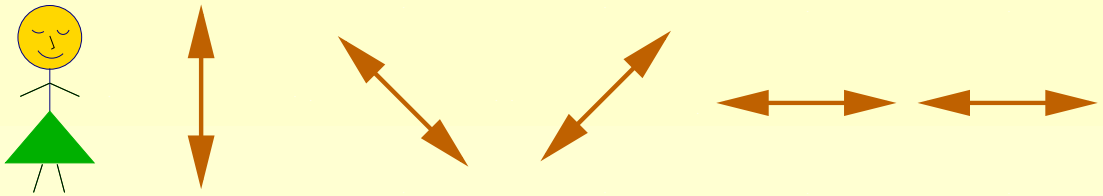


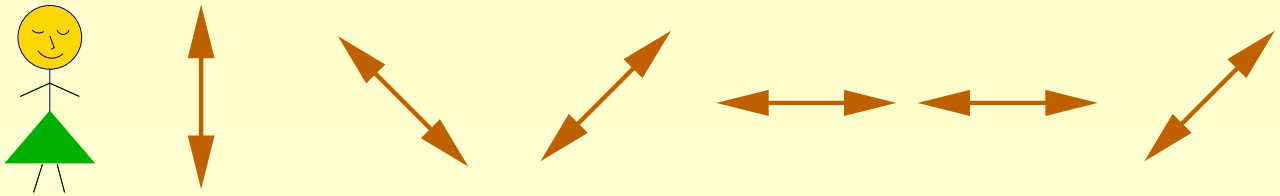


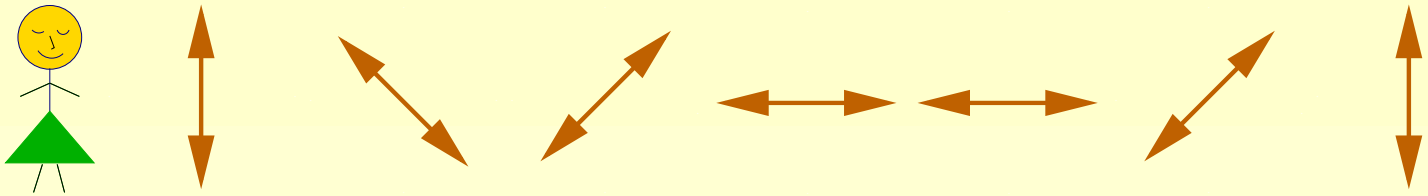


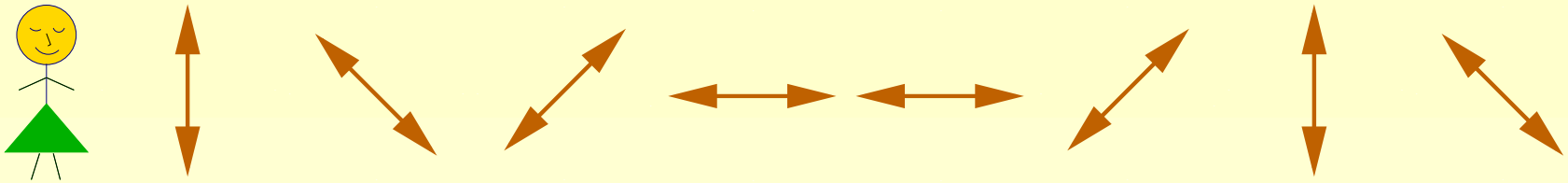


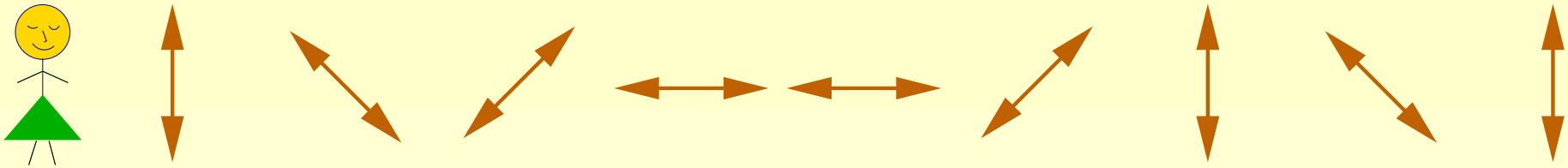


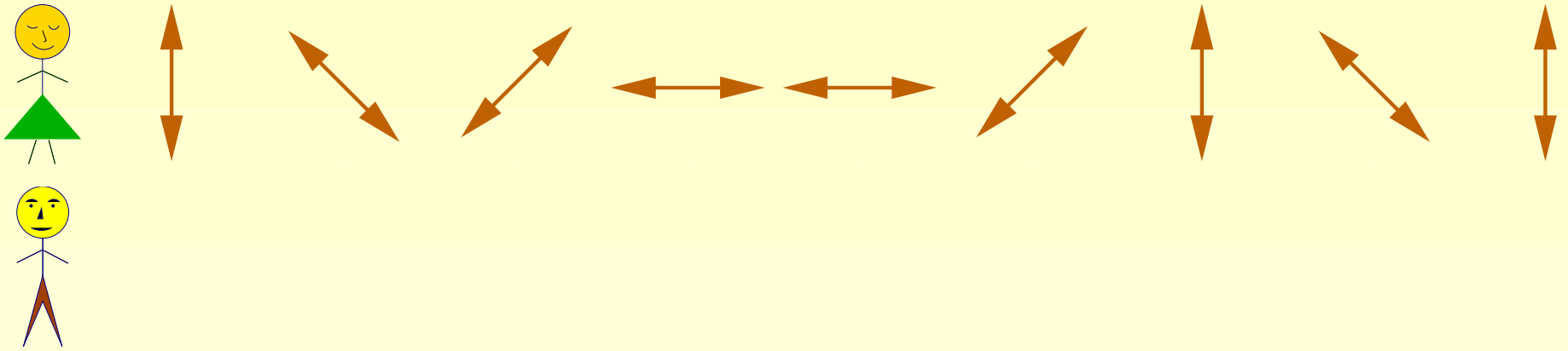


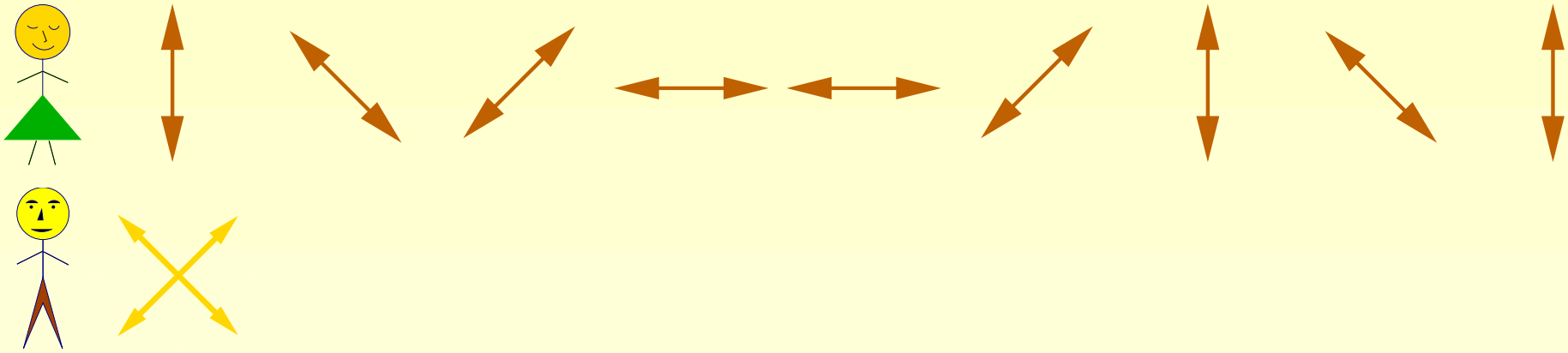


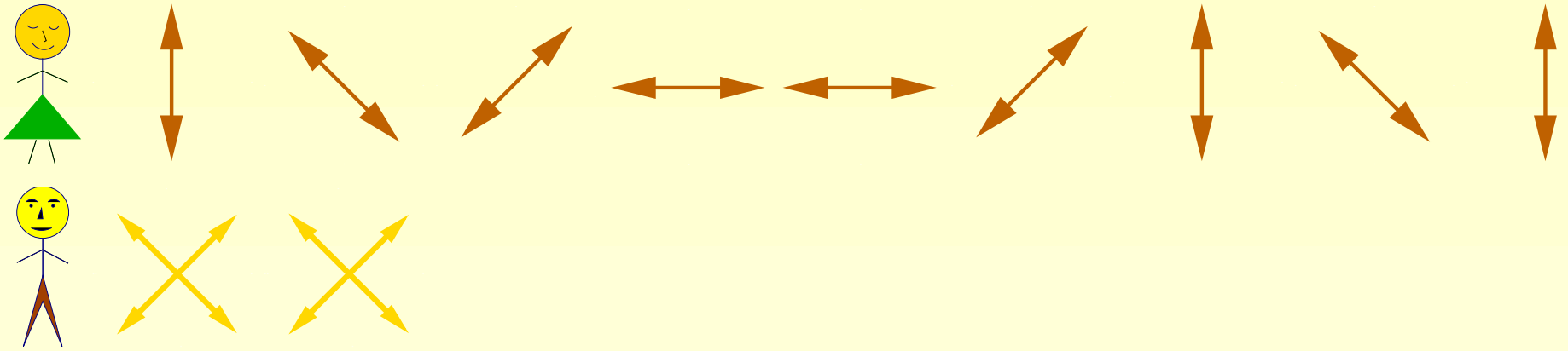


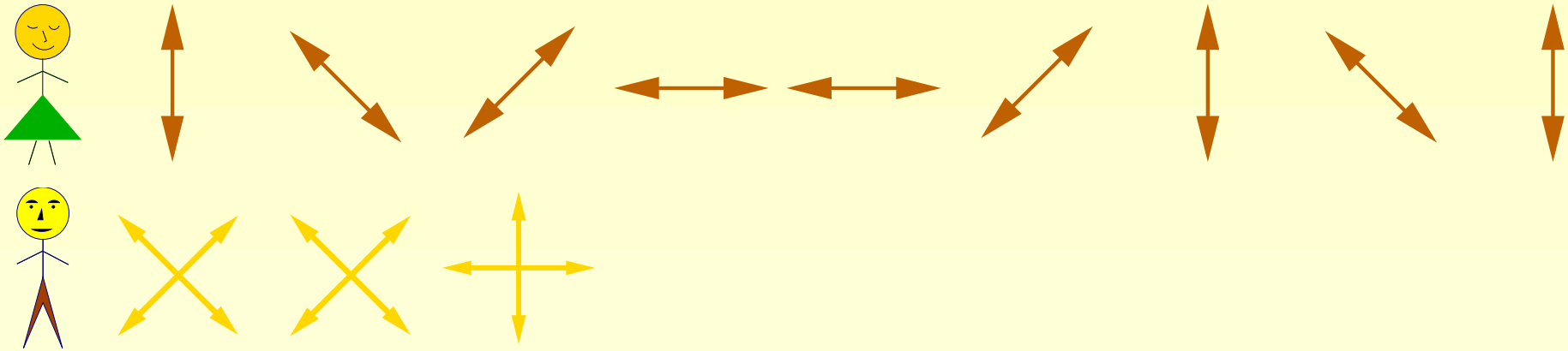


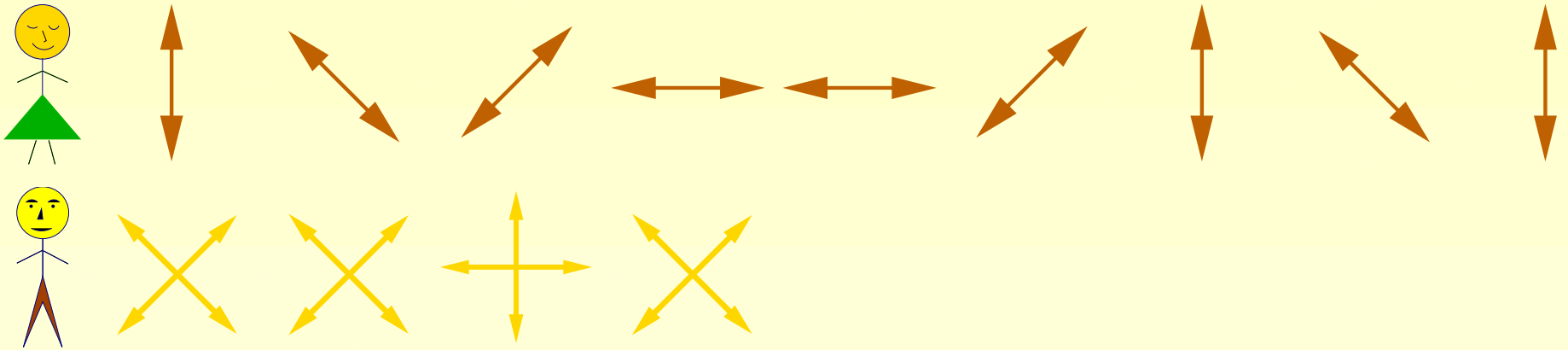


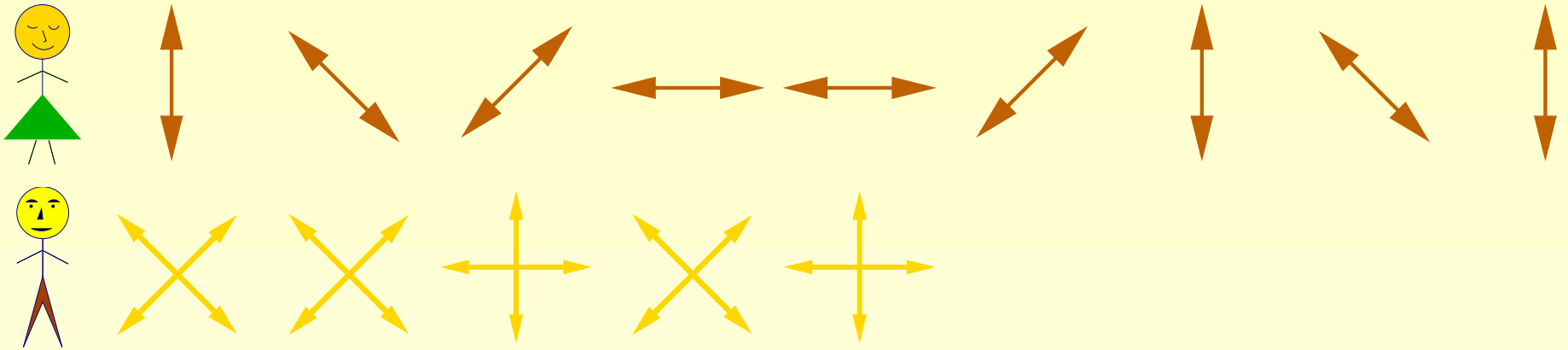


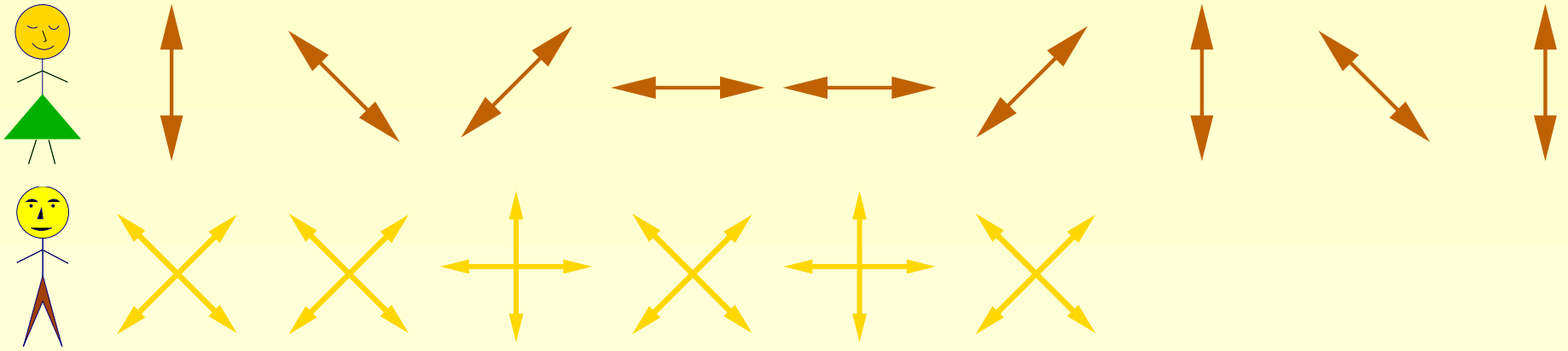


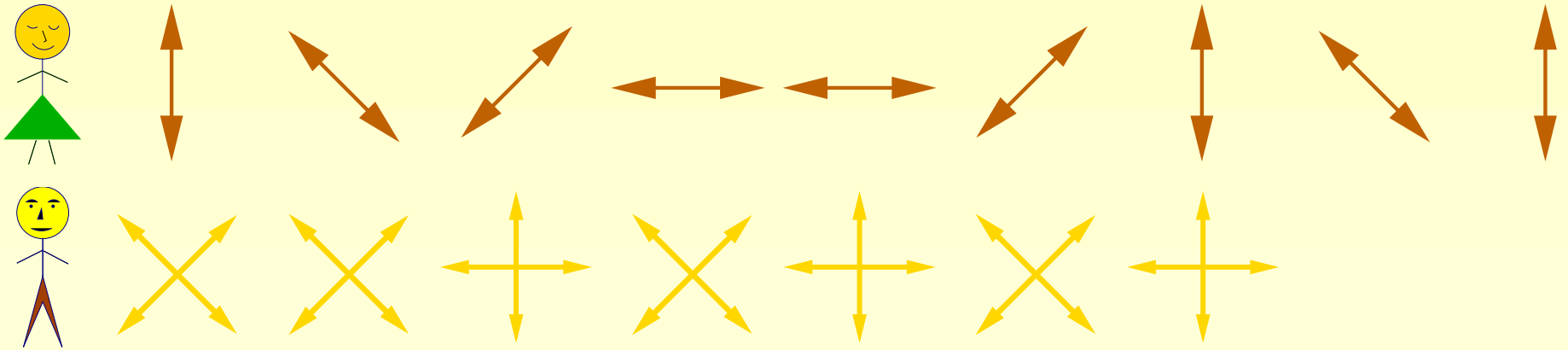


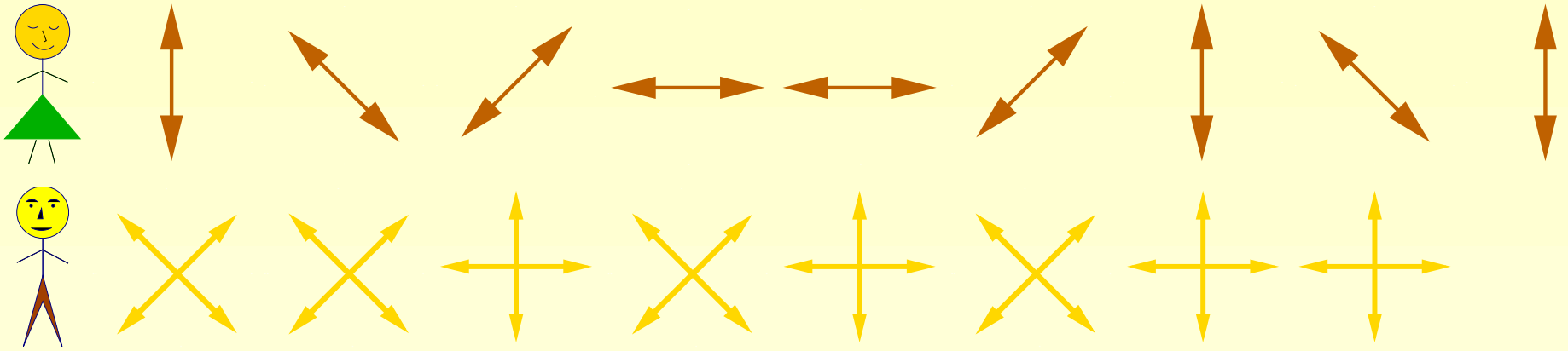


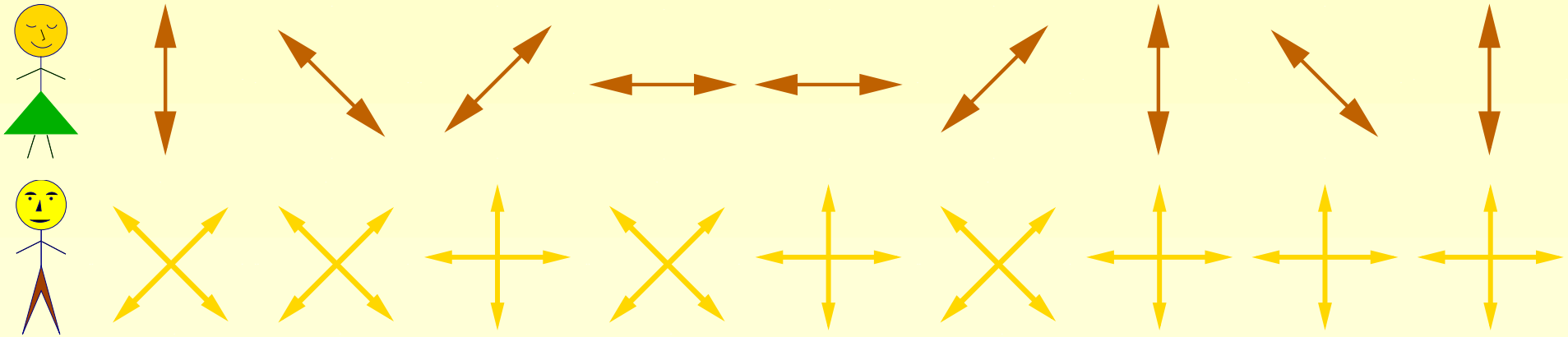


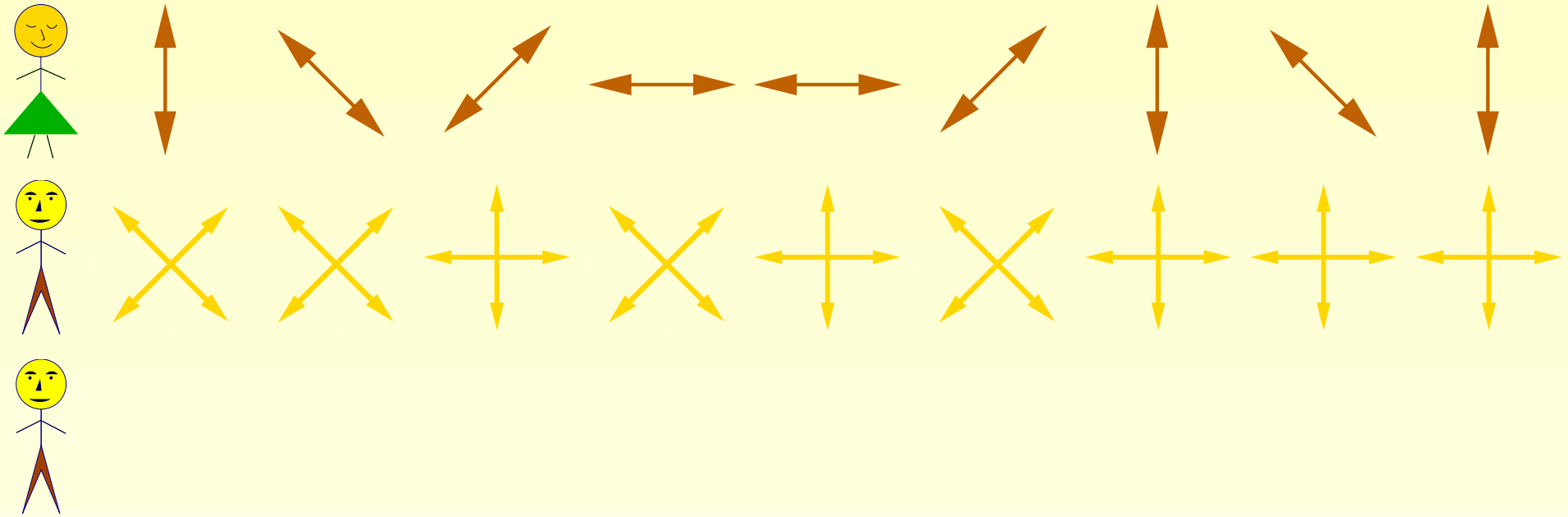


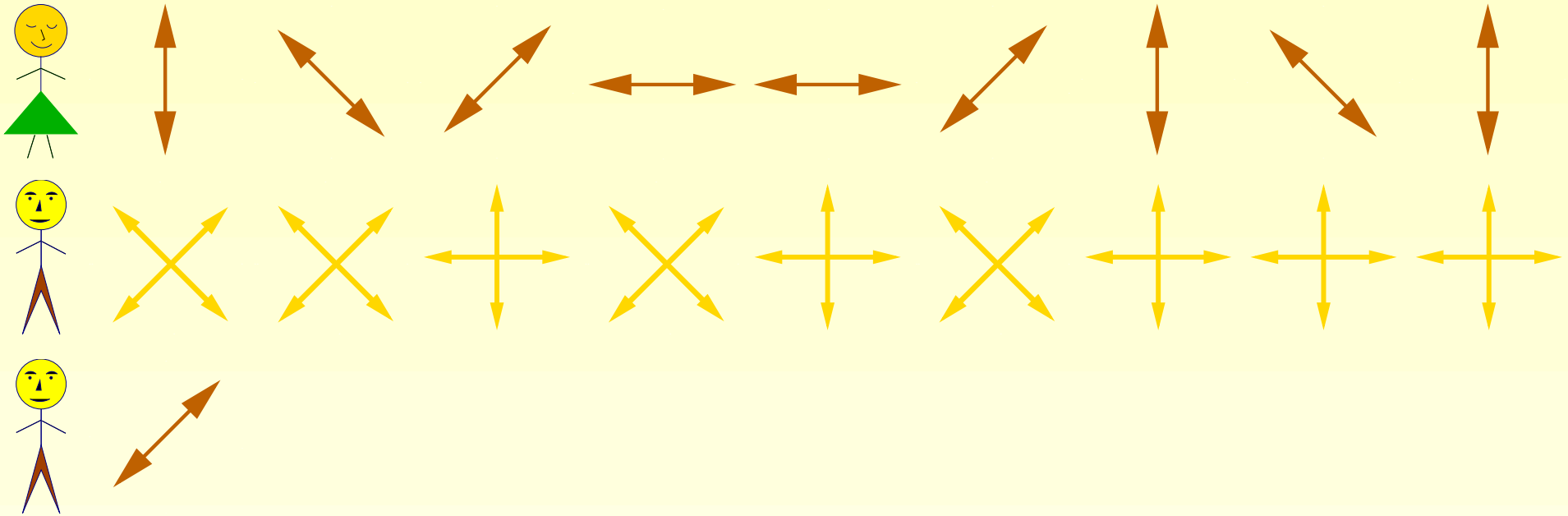


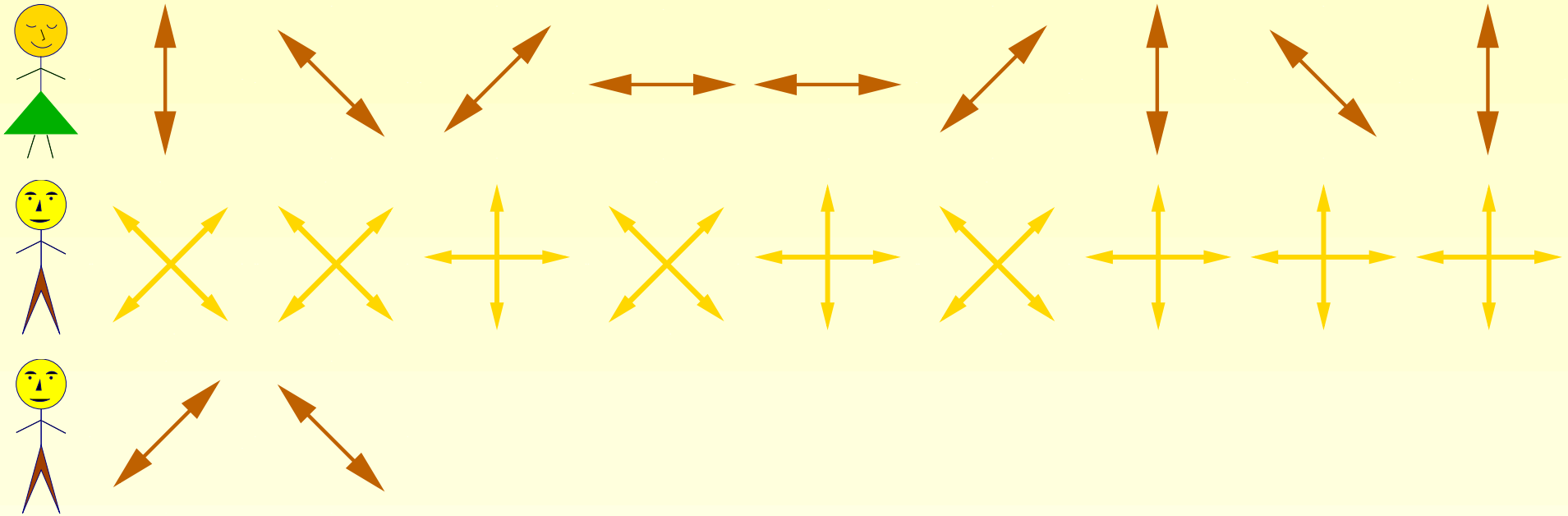


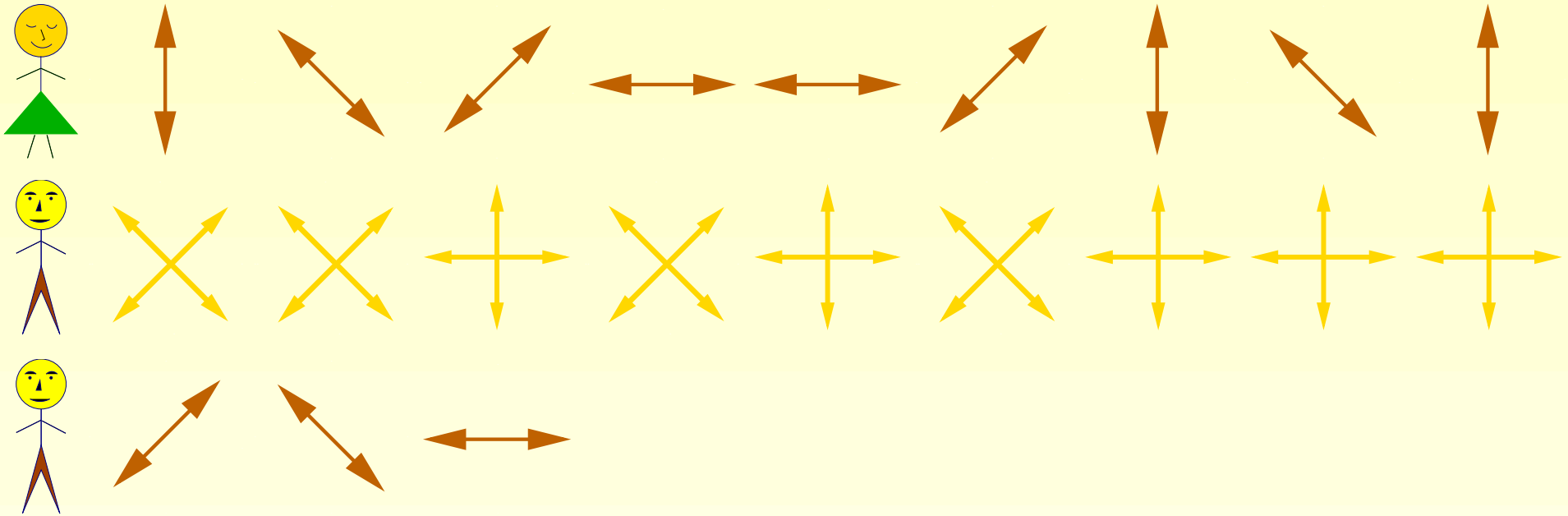


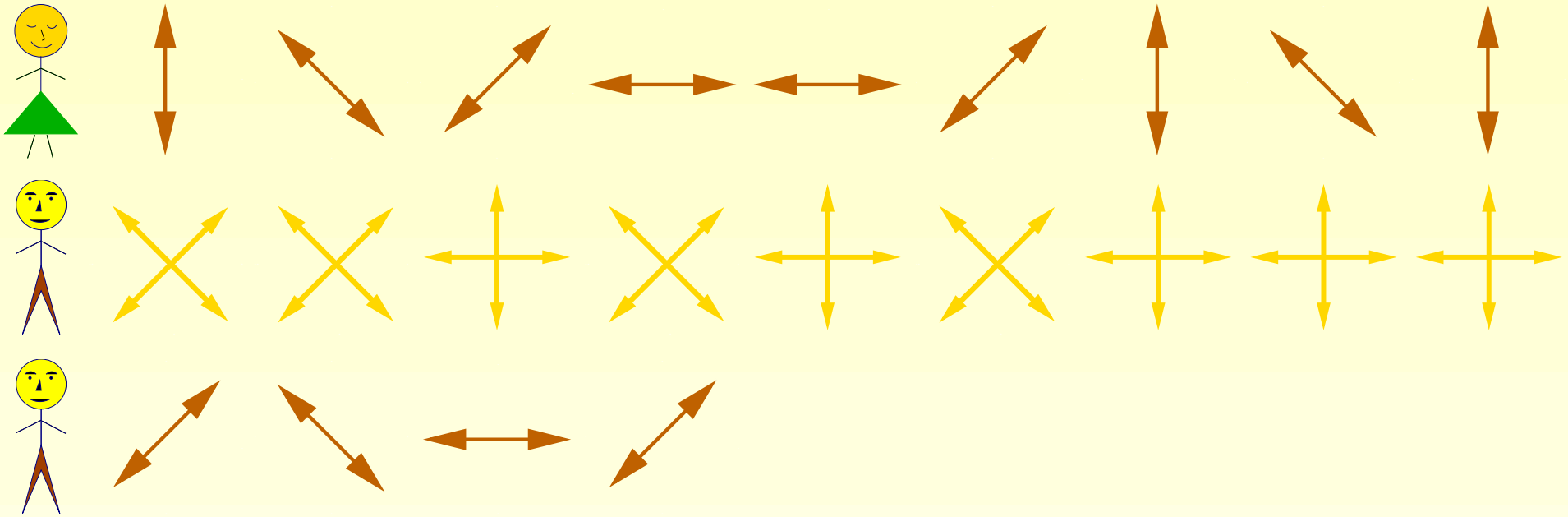


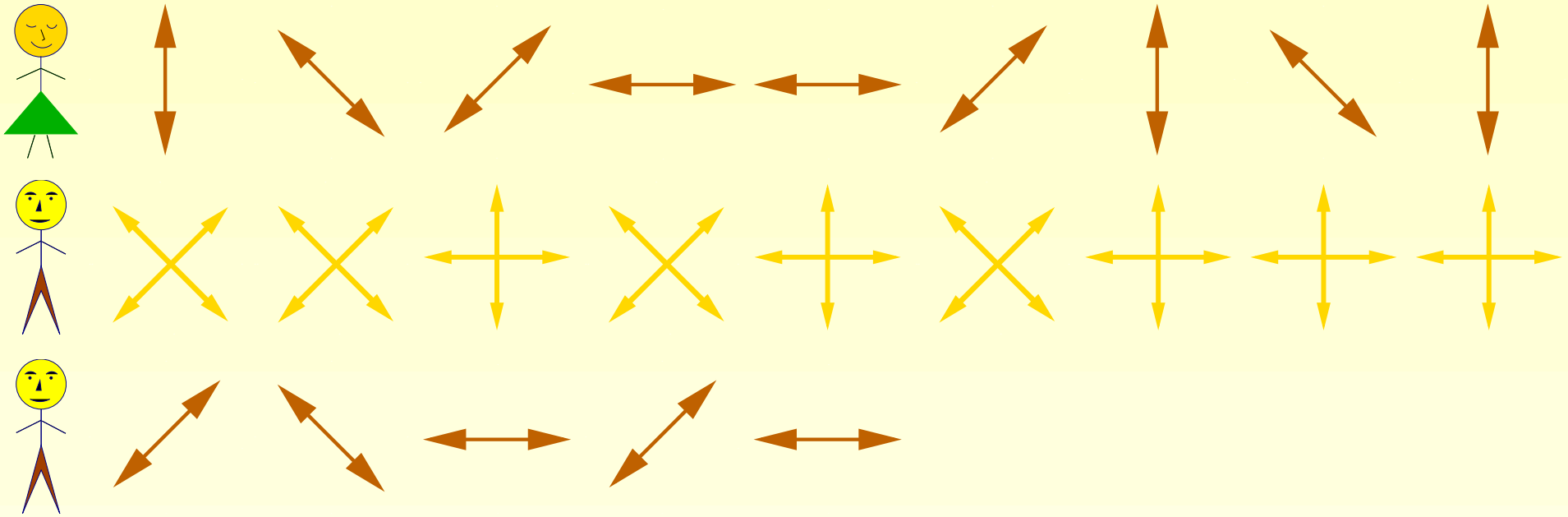


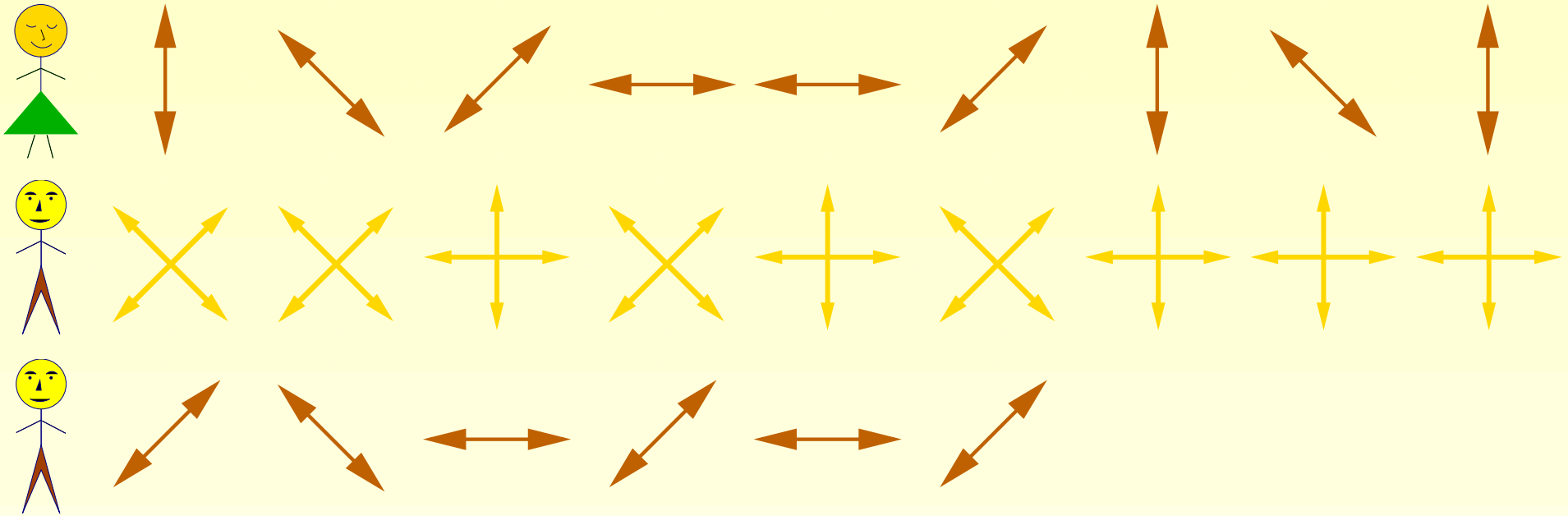


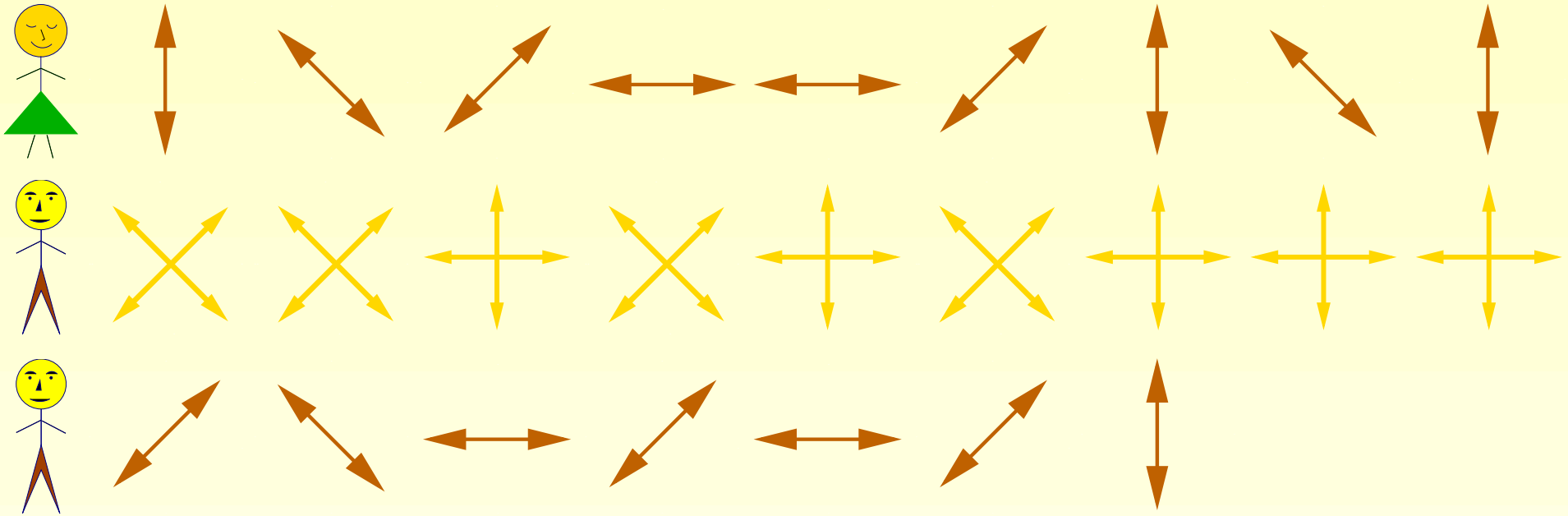


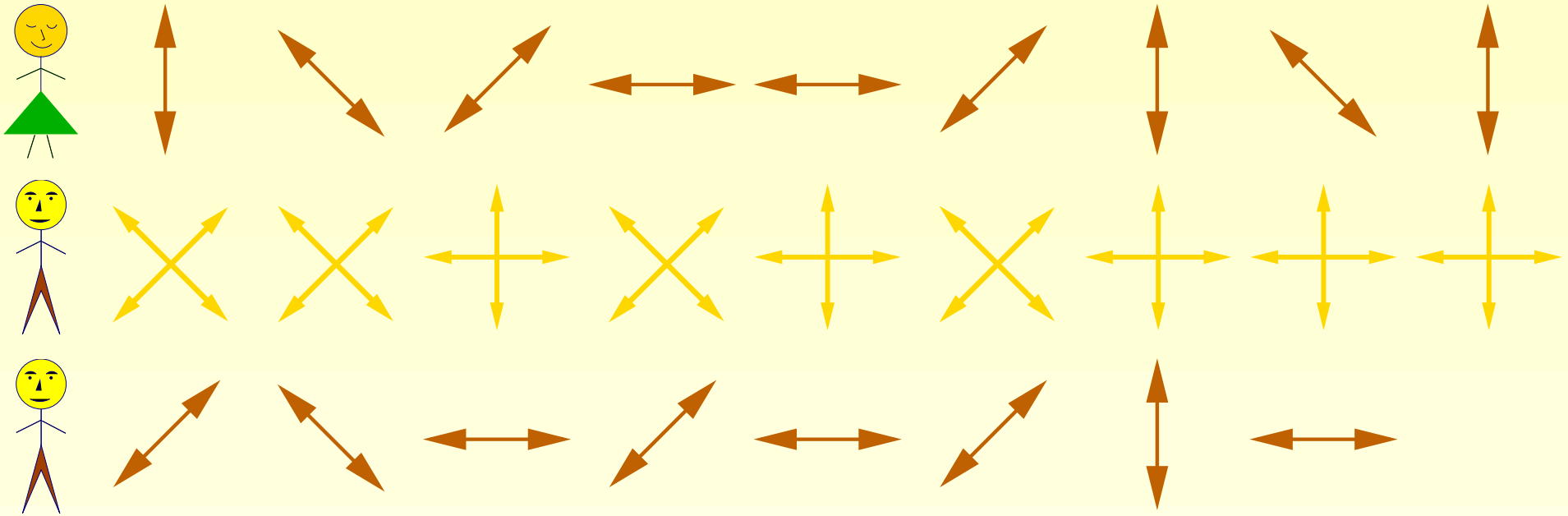


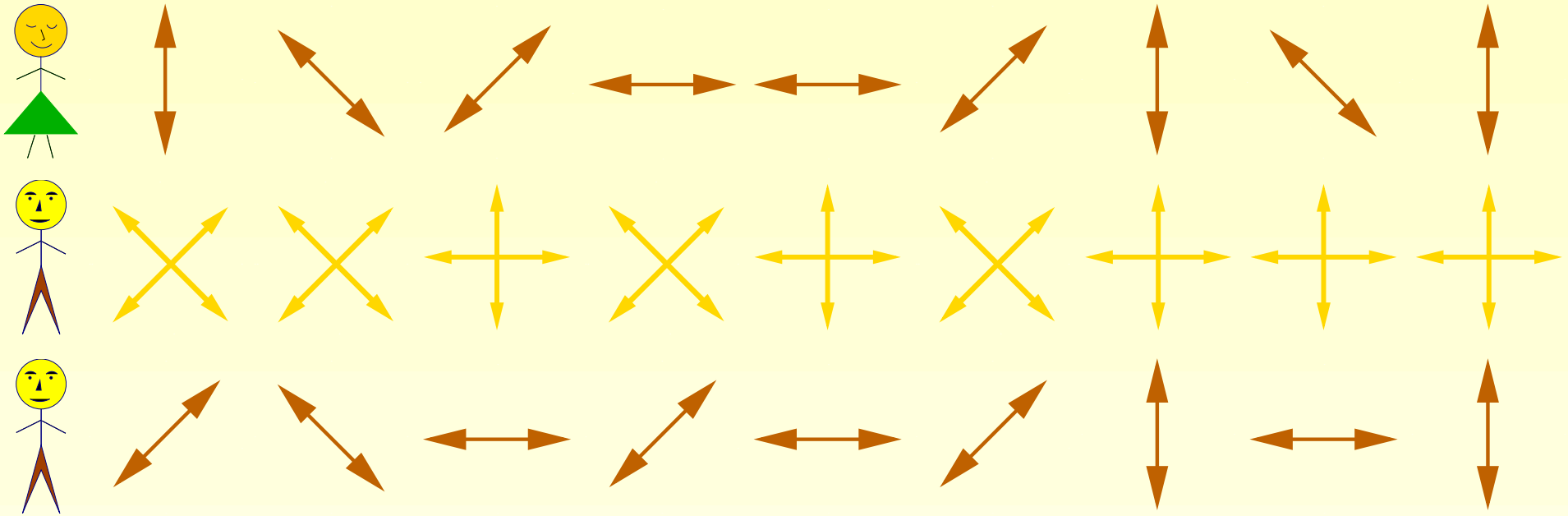


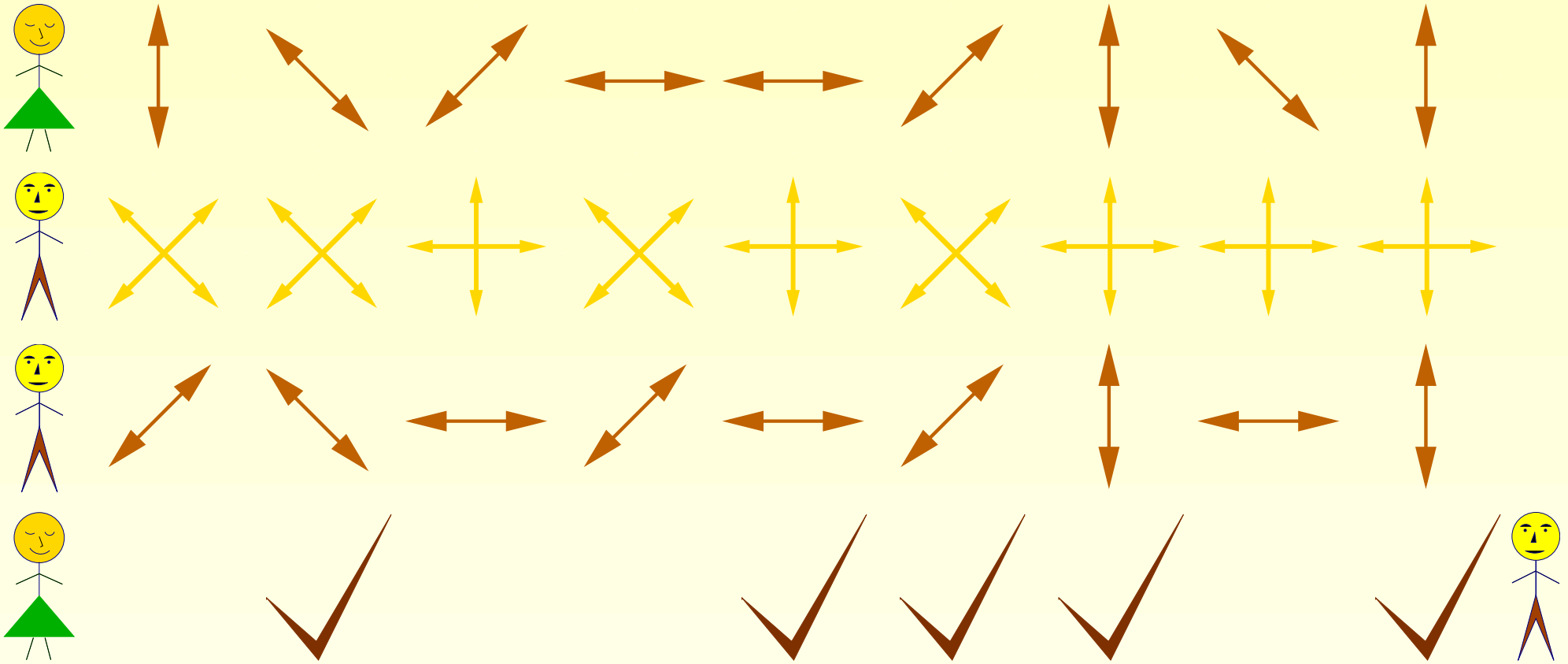


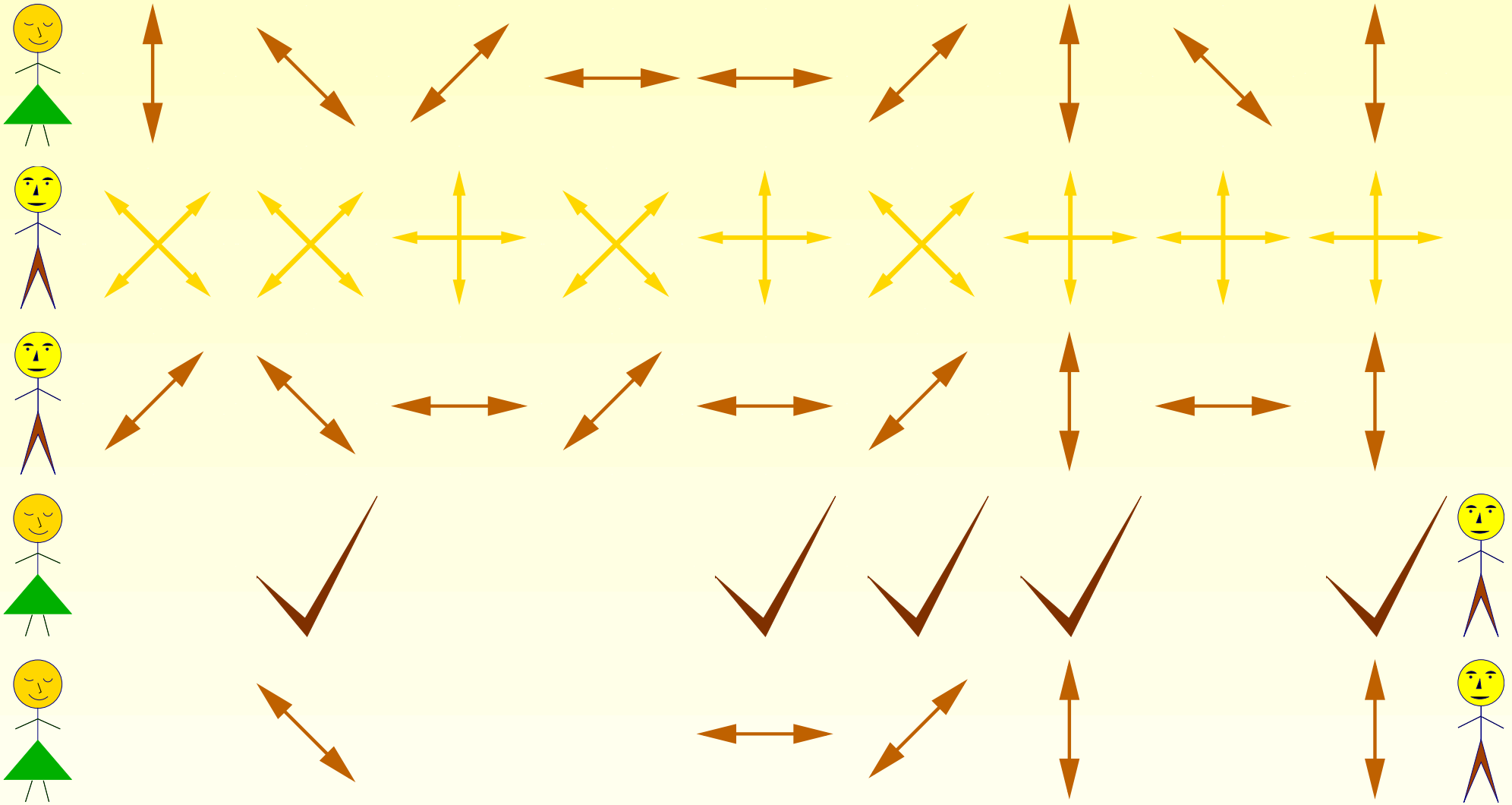


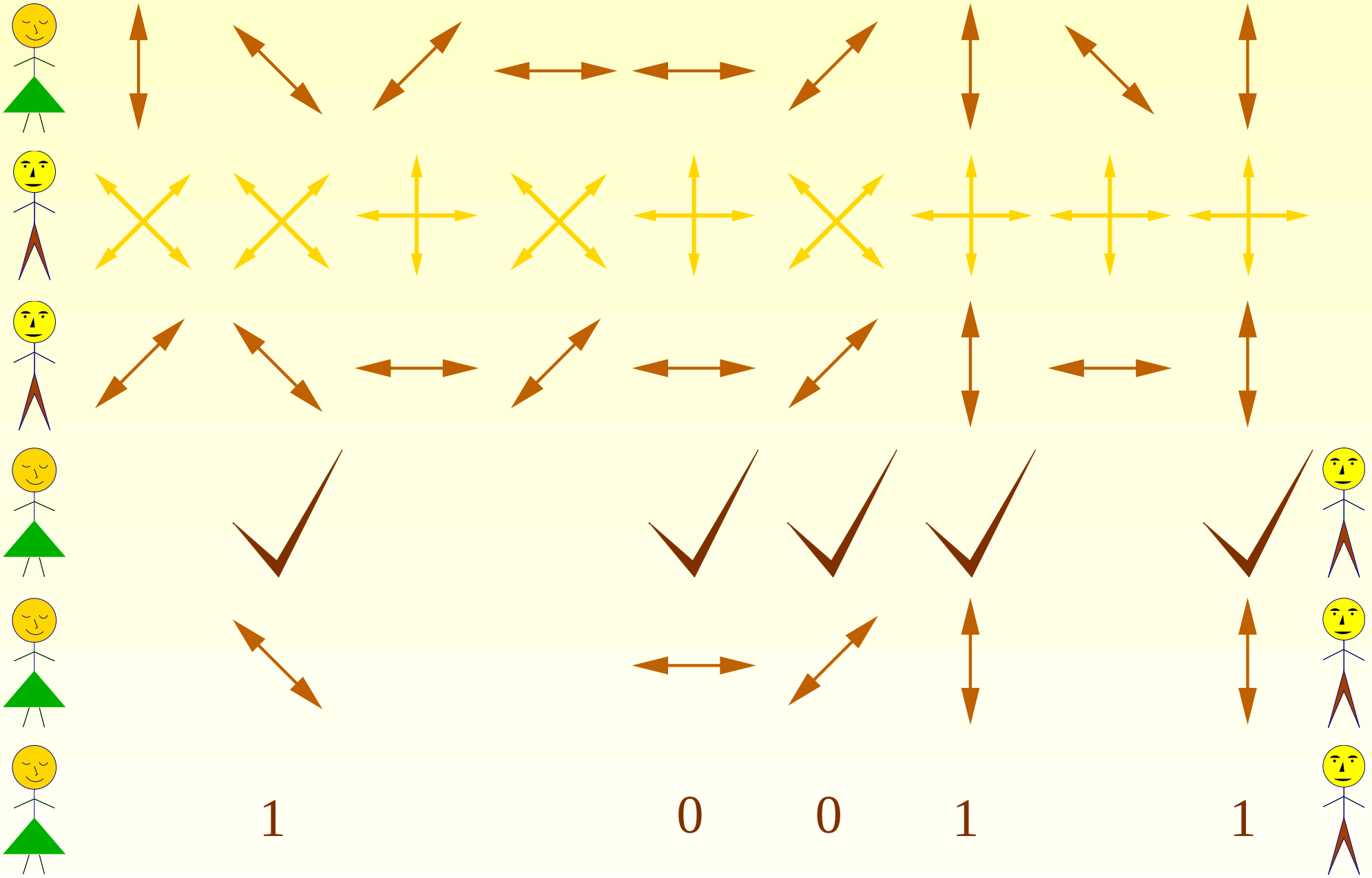




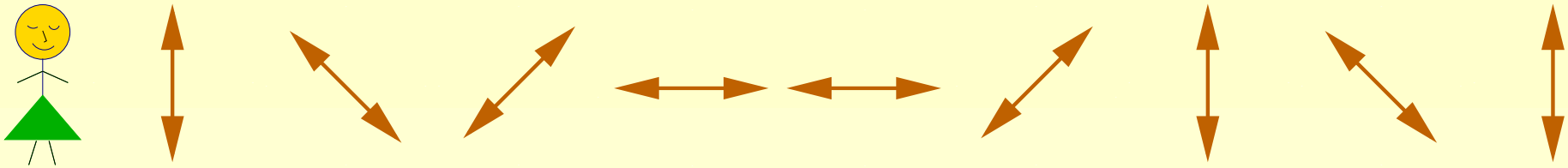


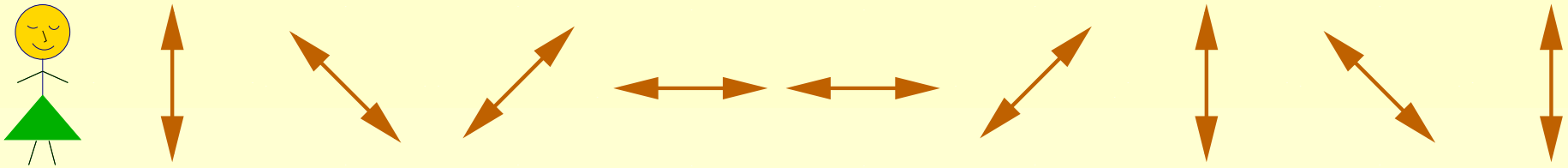




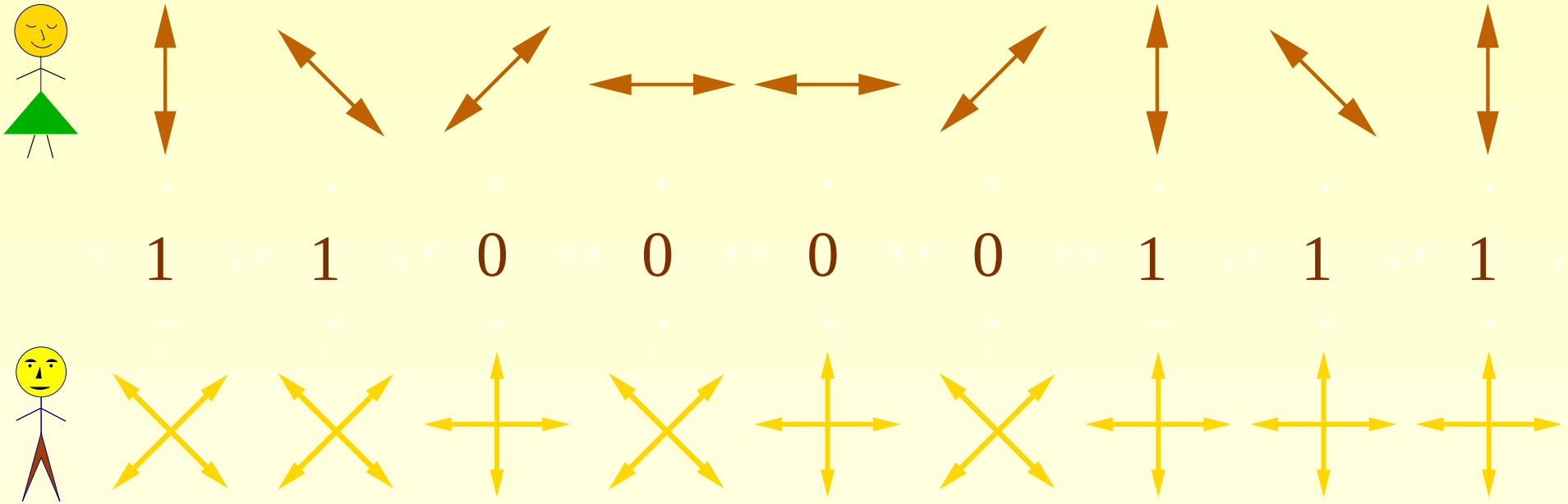

1
0
0
1
1

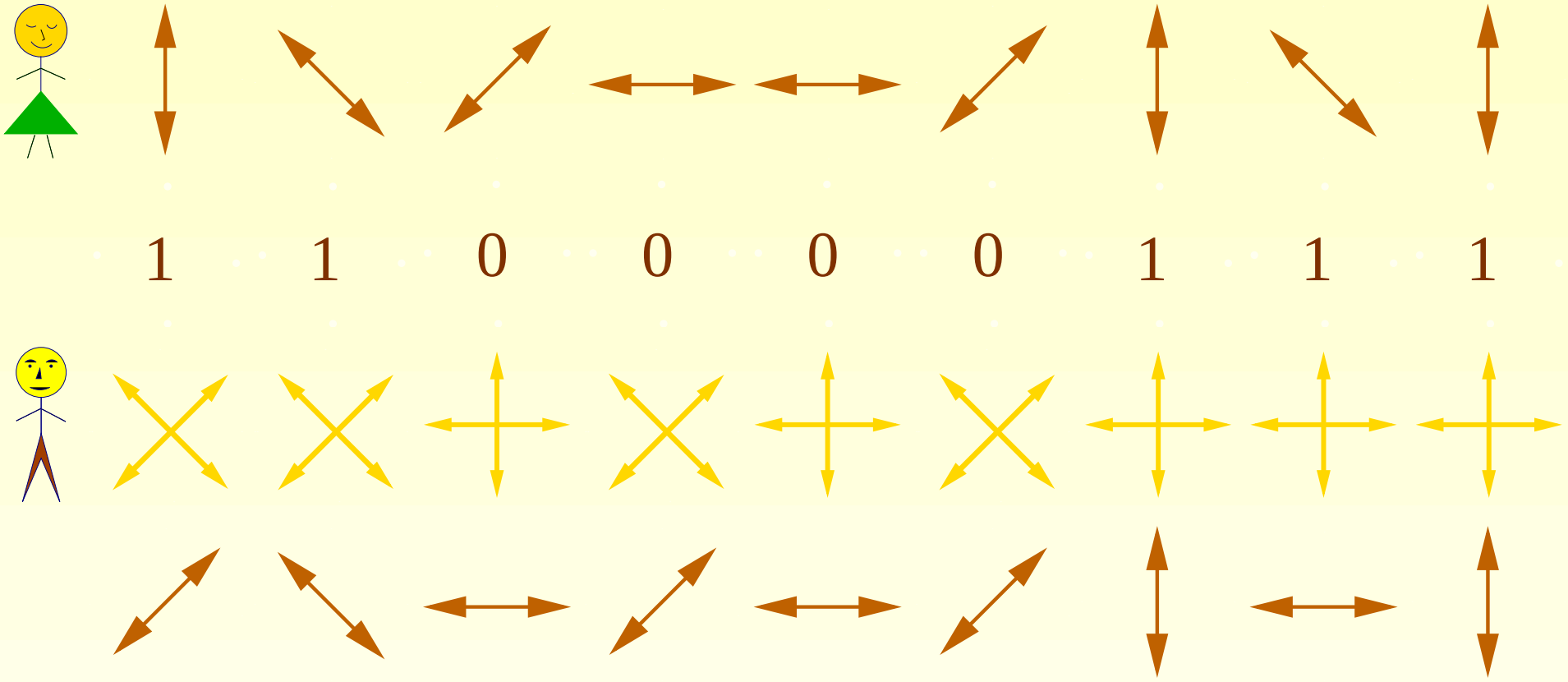
2.5 Błędne bity

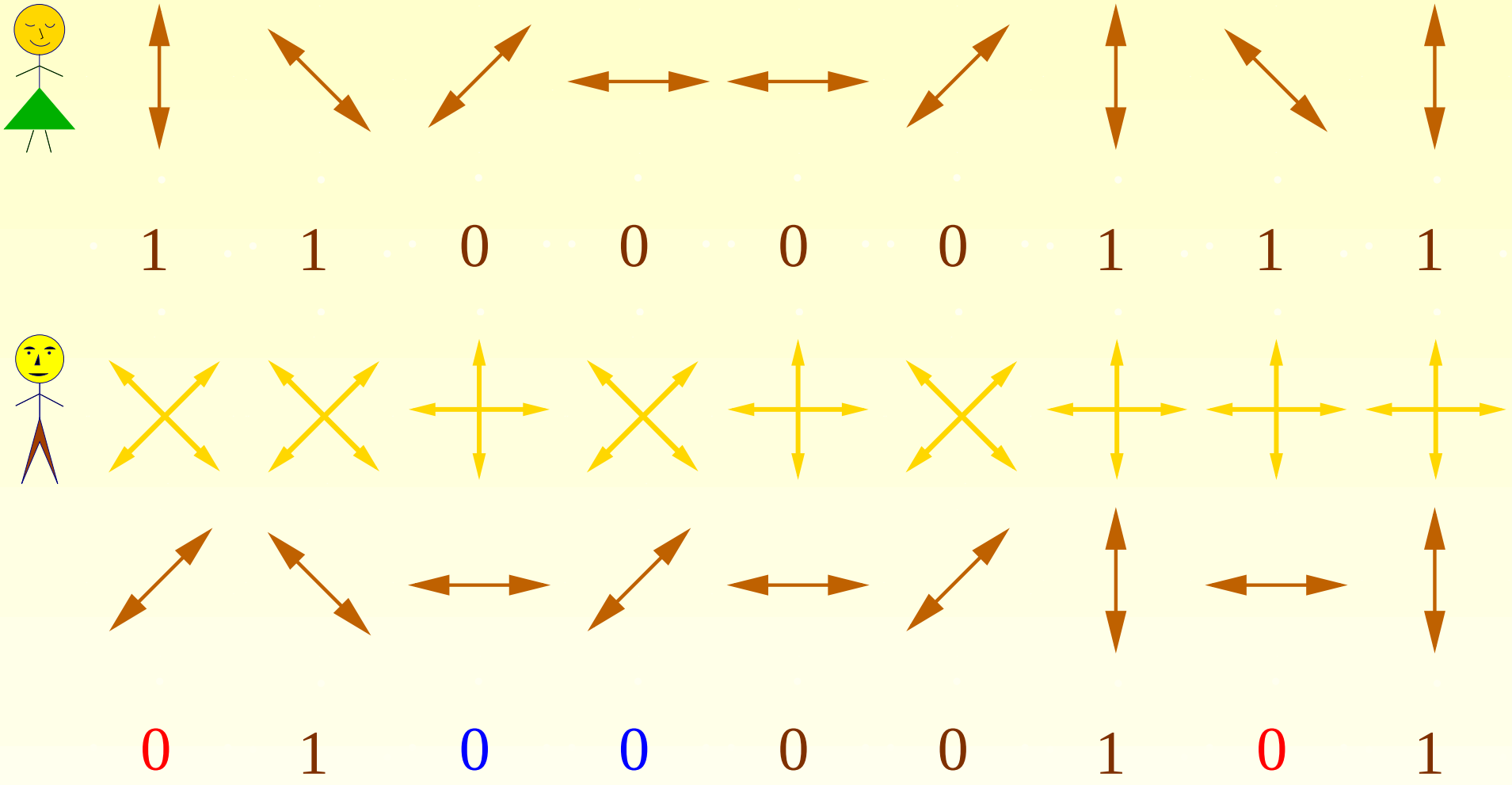


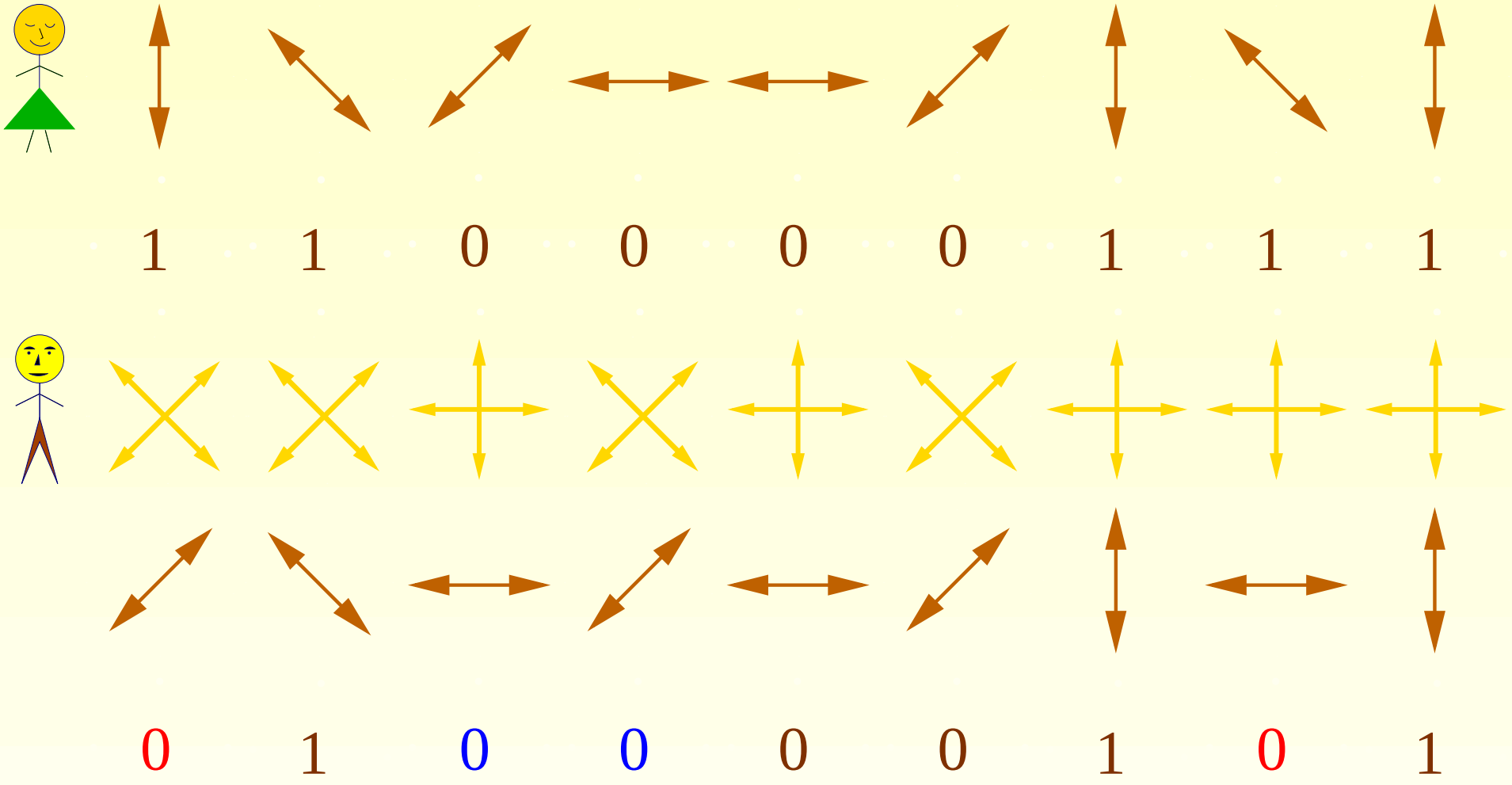


1 1 0 0 0 0 1 1 1


1 1 0 0 0 0 1 1 1


1 1 0 0 0 0 1 1 1


1 1 0 0 0 0 1 1 1
0 1 0 0 0 0 1 0 1



Średnio 50% bitów zarejestrowanych przez Bolka to bity pewne (brązowe), 25% bitów to bity prawidłowe mimo złego wyboru bazy (niebieskie) i 25% to bity nieprawidłowe (czerwone).

- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $\frac{1}{2}$

- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $\frac{1}{2}$
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy prawidłowym wyborze bazy wynosi 1

- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $\frac{1}{2}$
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy prawidłowym wyborze bazy wynosi 1
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy nieprawidłowo wybranej bazie wynosi $\frac{1}{2}$.

- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $\frac{1}{2}$
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy prawidłowym wyborze bazy wynosi 1
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy nieprawidłowo wybranej bazie wynosi $\frac{1}{2}$.
- Prawdopodobieństwo zarejestrowania prawidłowego bitu wynosi:

- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $\frac{1}{2}$
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy prawidłowym wyborze bazy wynosi 1
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy nieprawidłowo wybranej bazie wynosi $\frac{1}{2}$.
- Prawdopodobieństwo zarejestrowania prawidłowego bitu wynosi:

$$\frac{1}{2}.$$

- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $\frac{1}{2}$
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy prawidłowym wyborze bazy wynosi 1
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy nieprawidłowo wybranej bazie wynosi $\frac{1}{2}$.
- Prawdopodobieństwo zarejestrowania prawidłowego bitu wynosi:

$$\frac{1}{2} \cdot 1$$

- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $\frac{1}{2}$
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy prawidłowym wyborze bazy wynosi 1
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy nieprawidłowo wybranej bazie wynosi $\frac{1}{2}$.
- Prawdopodobieństwo zarejestrowania prawidłowego bitu wynosi:

$$\frac{1}{2} \cdot 1 +$$

- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $\frac{1}{2}$
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy prawidłowym wyborze bazy wynosi 1
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy nieprawidłowo wybranej bazie wynosi $\frac{1}{2}$.
- Prawdopodobieństwo zarejestrowania prawidłowego bitu wynosi:

$$\frac{1}{2} \cdot 1 + \frac{1}{2}$$

- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $\frac{1}{2}$
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy prawidłowym wyborze bazy wynosi 1
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy nieprawidłowo wybranej bazie wynosi $\frac{1}{2}$.
- Prawdopodobieństwo zarejestrowania prawidłowego bitu wynosi:

$$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2}$$

- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $\frac{1}{2}$
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy prawidłowym wyborze bazy wynosi 1
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy nieprawidłowo wybranej bazie wynosi $\frac{1}{2}$.
- Prawdopodobieństwo zarejestrowania prawidłowego bitu wynosi:

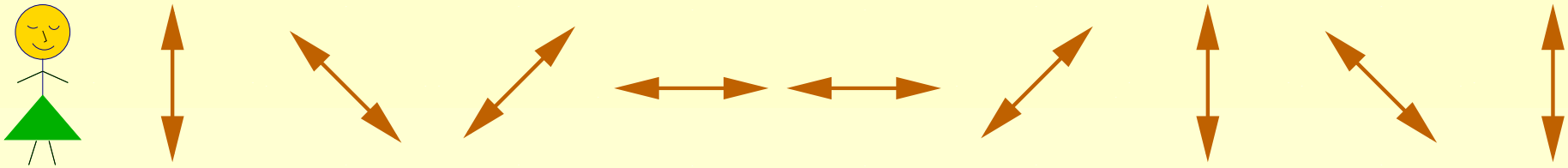
$$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$$

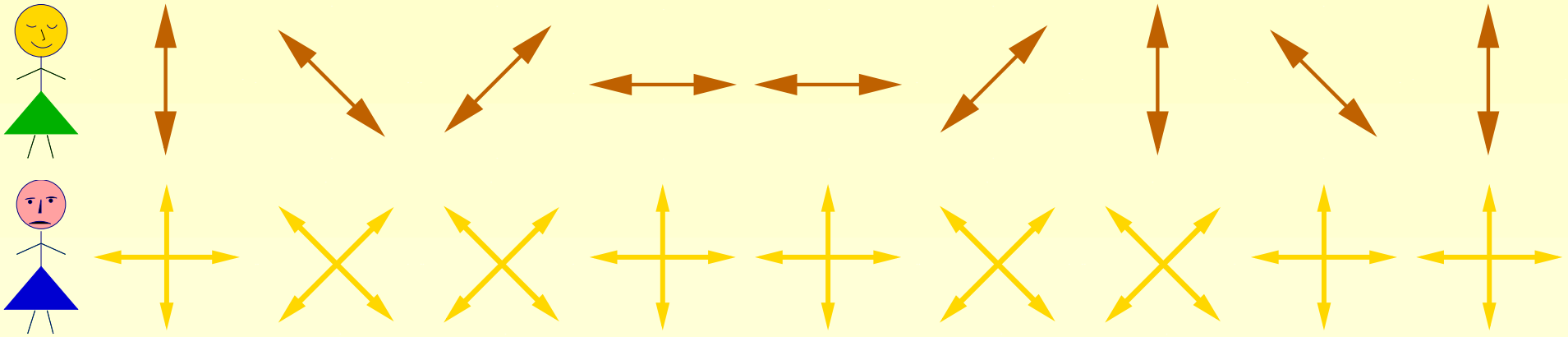
- Prawdopodobieństwo wyboru jednej z dwóch możliwych baz wynosi $\frac{1}{2}$
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy prawidłowym wyborze bazy wynosi 1
- Prawdopodobieństwo pomiaru prawidłowej polaryzacji przy nieprawidłowo wybranej bazie wynosi $\frac{1}{2}$.
- Prawdopodobieństwo zarejestrowania prawidłowego bitu wynosi:

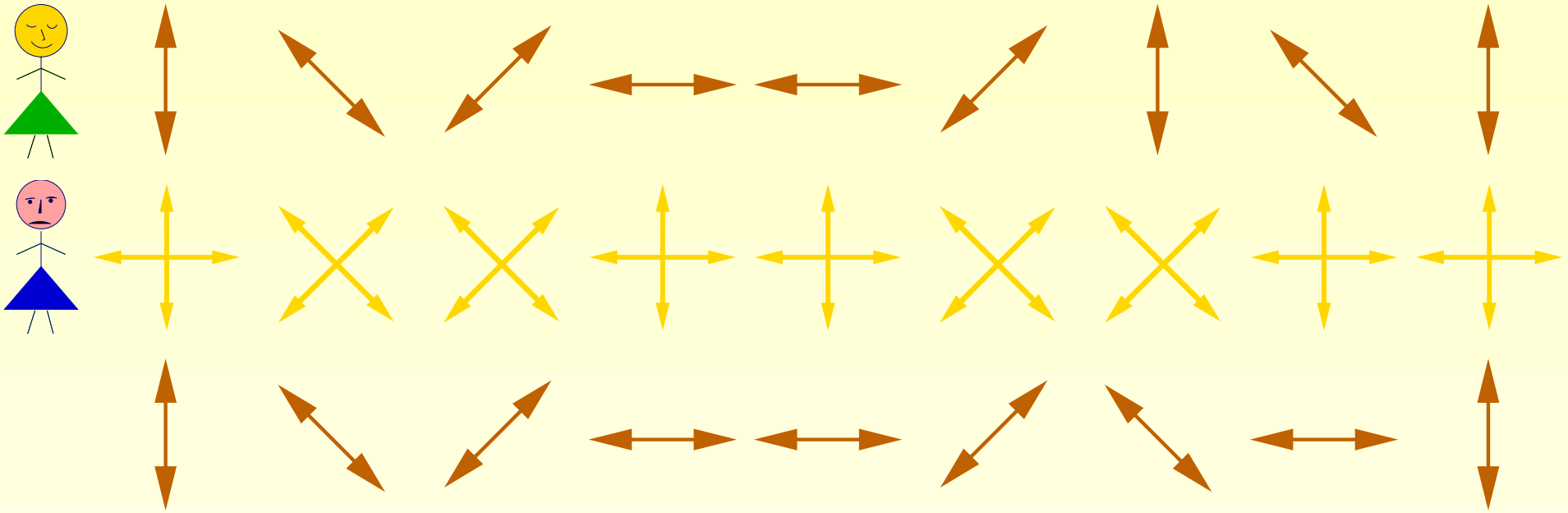
$$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$$

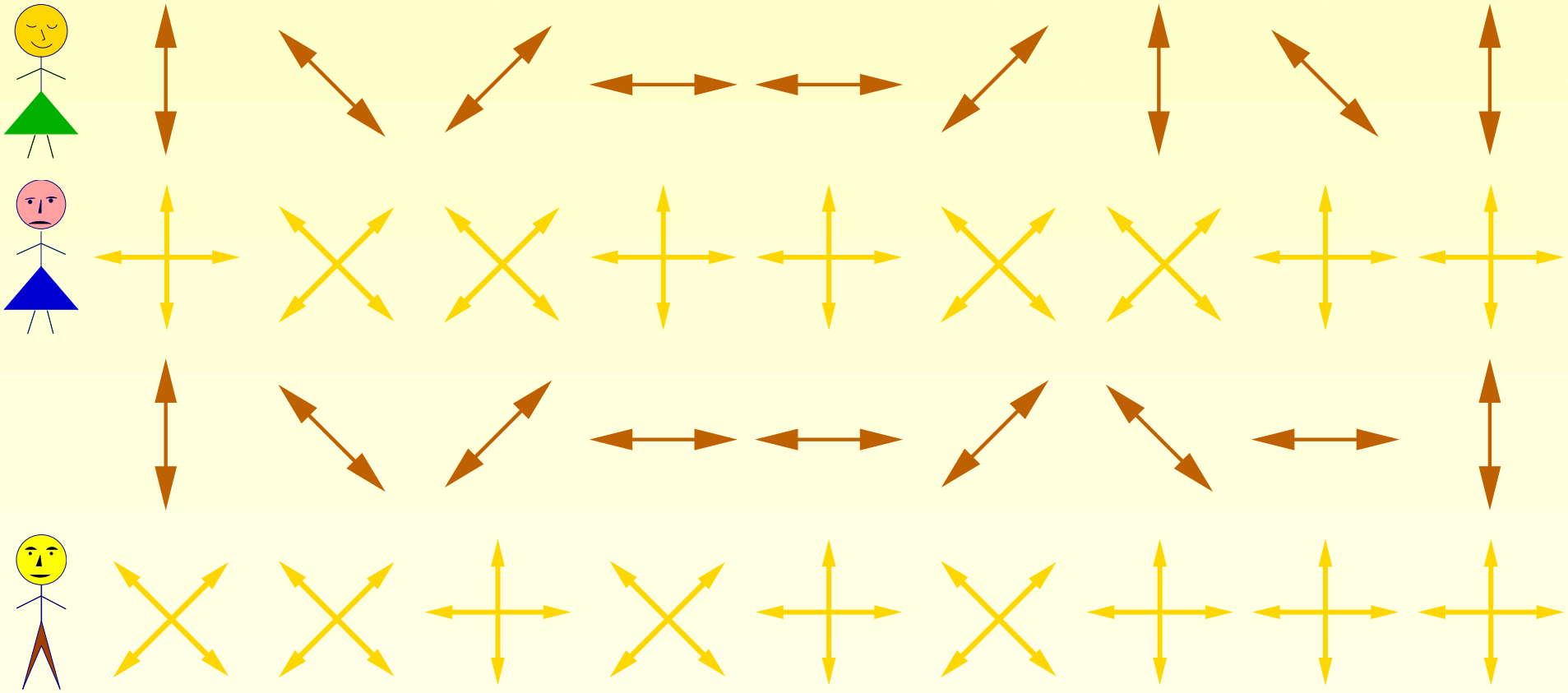
- Prawdopodobieństwo zarejestrowania błędnego bitu wynosi $\frac{1}{4}$.

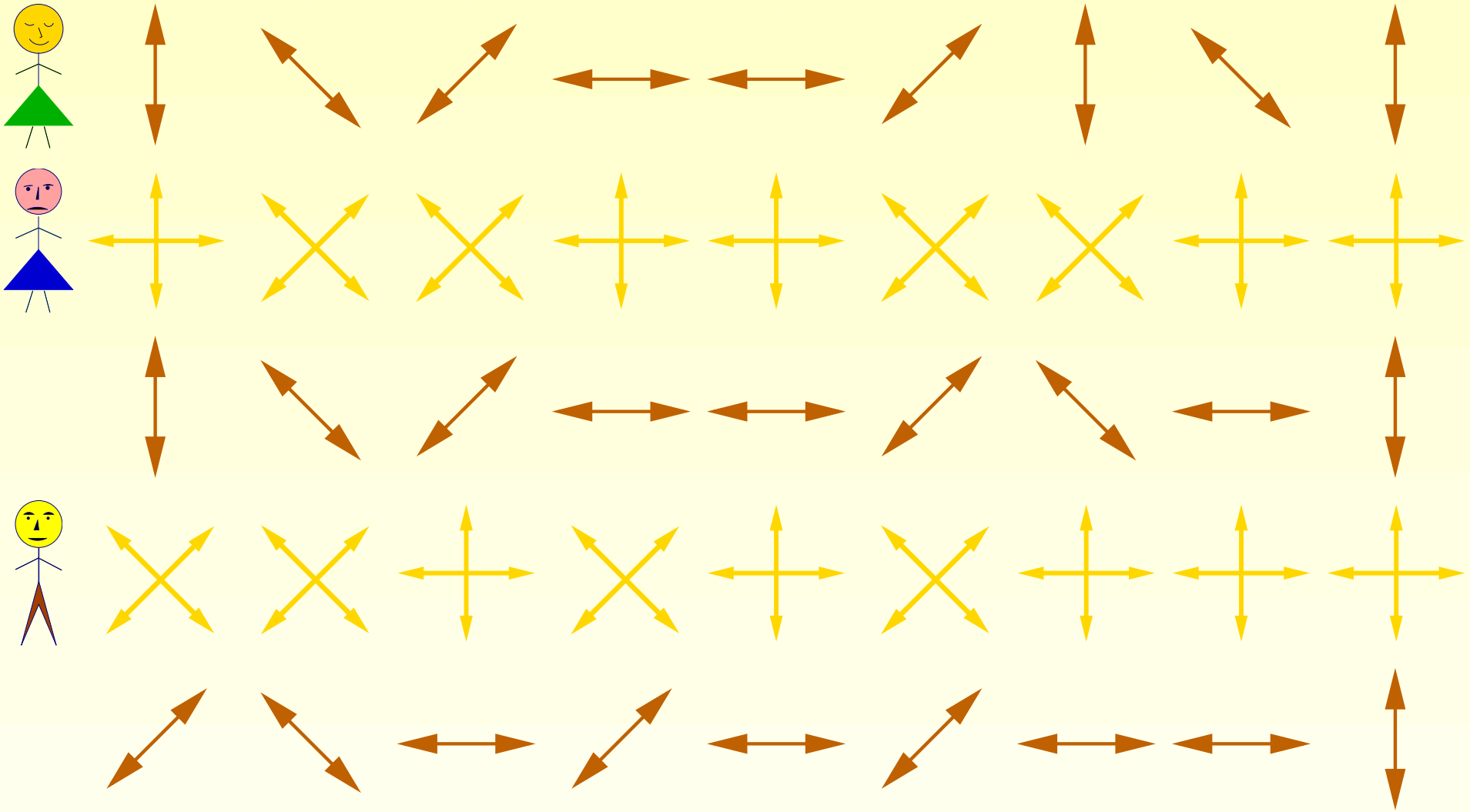
2.6 Ewa podsłuchuje

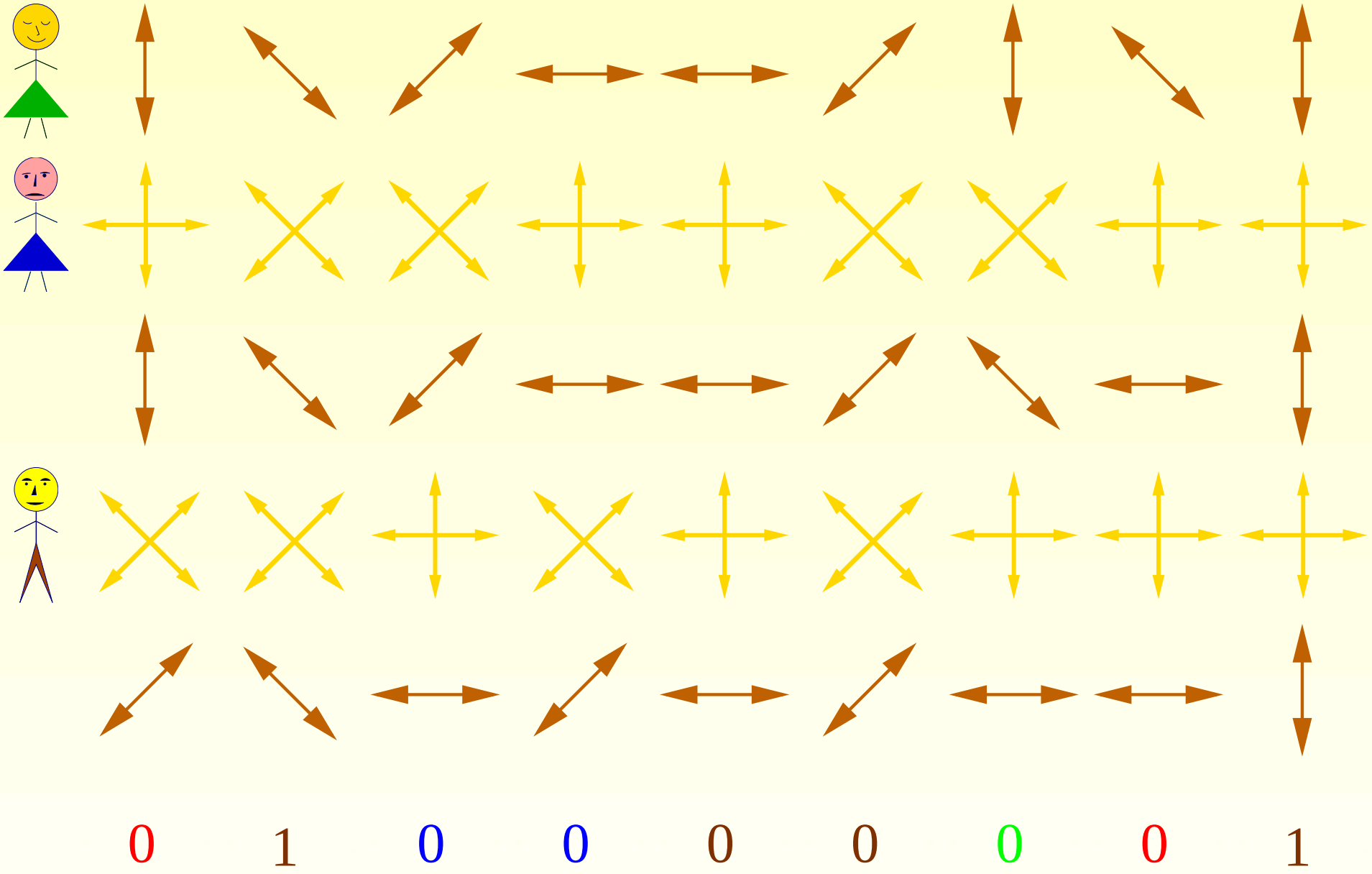


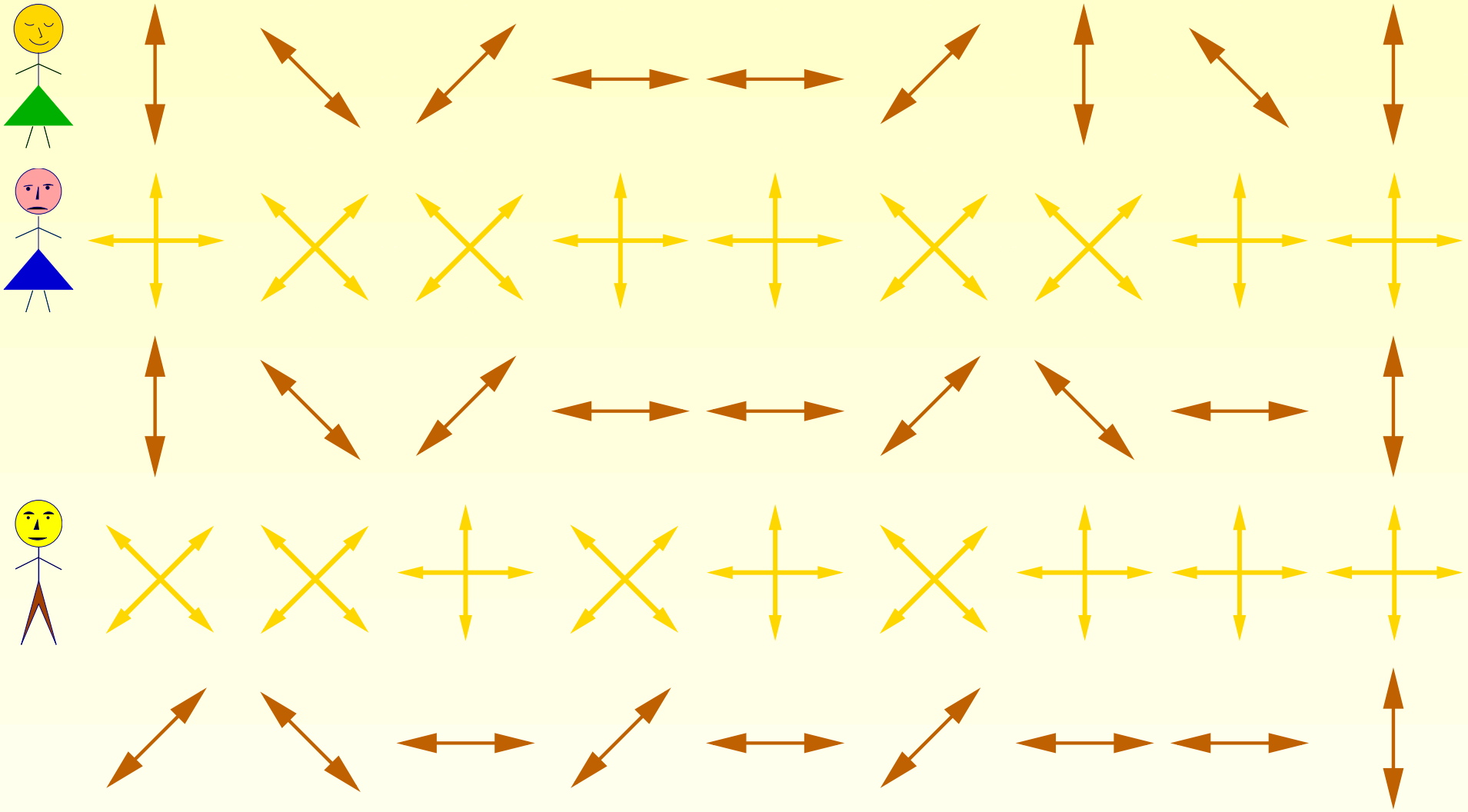









0 1 0 0 0 0 0 0 1



0 1 0 0 0 0 0 0 1

0 1 0 0 0 0 1 0 1

- Ewa podsłuchuje dokonując pomiaru w losowo wybranej bazie i po zarejestrowaniu polaryzacji przesyła foton o takiej samej polaryzacji do Bolka.

- Ewa podsłuchuje dokonując pomiaru w losowo wybranej bazie i po zarejestrowaniu polaryzacji przesyła foton o takiej samej polaryzacji do Bolka.
- W ten sposób Ewa zmienia niektóre bity, czyli wprowadza błędy w przekazie (zielone bity).

- Ewa podsłuchuje dokonując pomiaru w losowo wybranej bazie i po zarejestrowaniu polaryzacji przesyła foton o takiej samej polaryzacji do Bolka.
- W ten sposób Ewa zmienia niektóre bity, czyli wprowadza błędy w przekazie (zielone bity).
- Alicja i Bolek mogą wykryć obecność Ewy porównując losowo wybraną część bitów z uzgodnionego już klucza (bity te następnie usuwają).

- Ewa podsłuchuje dokonując pomiaru w losowo wybranej bazie i po zarejestrowaniu polaryzacji przesyła foton o takiej samej polaryzacji do Bolka.
- W ten sposób Ewa zmienia niektóre bity, czyli wprowadza błędy w przekazie (zielone bity).
- Alicja i Bolek mogą wykryć obecność Ewy porównując losowo wybraną część bitów z uzgodnionego już klucza (bity te następnie usuwają).
- Jeśli okaże się, że bity zostały zmienione, to oznacza że Ewa podsłuchiwała.

- Ewa podsłuchuje dokonując pomiaru w losowo wybranej bazie i po zarejestrowaniu polaryzacji przesyła foton o takiej samej polaryzacji do Bolka.
- W ten sposób Ewa zmienia niektóre bity, czyli wprowadza błędy w przekazie (zielone bity).
- Alicja i Bolek mogą wykryć obecność Ewy porównując losowo wybraną część bitów z uzgodnionego już klucza (bity te następnie usuwają).
- Jeśli okaże się, że bity zostały zmienione, to oznacza że Ewa podsłuchiwała.

  Wtedy uzgadnianie klucza zaczyna się od nowa!

- Na poziomie kwantowym nie ma możliwości pasywnego podsłuchu. Każdy podsłuch zaburza przekaz.

- Na poziomie kwantowym nie ma możliwości pasywnego podsłuchu. Każdy podsłuch zaburza przekaz.
- Prawa mechaniki kwantowej gwarantują bezpieczeństwo przy uzgadnianiu klucza kryptograficznego.

- Na poziomie kwantowym nie ma możliwości pasywnego podsłuchu. Każdy podsłuch zaburza przekaz.
- Prawa mechaniki kwantowej gwarantują bezpieczeństwo przy uzgadnianiu klucza kryptograficznego.
- Kwantowa dystrybucja klucza + klasyczny szyfr Vernama = całkowicie bezpieczny kanał łączności!

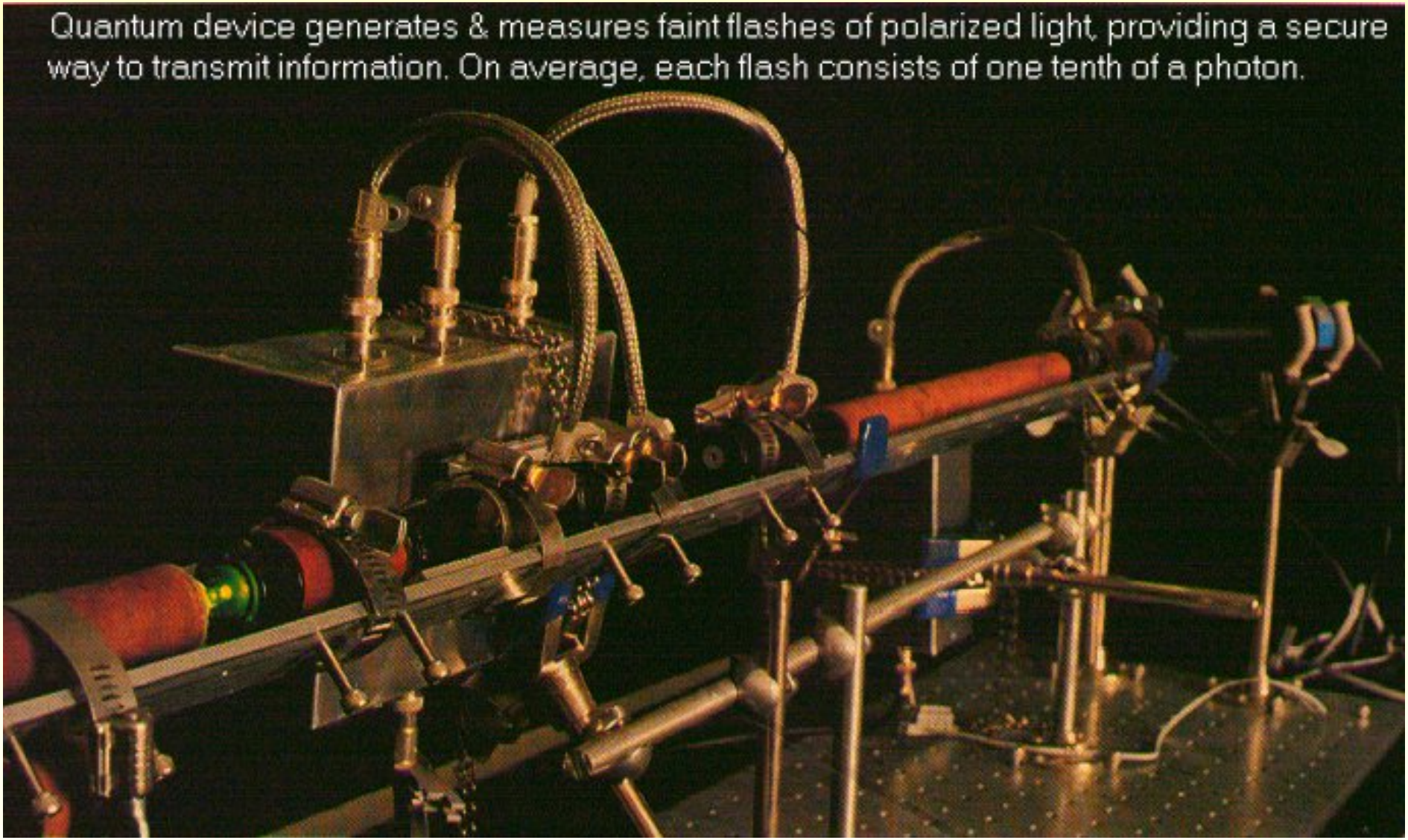
- Istnieją inne protokoły kwantowe, np.
  - Artur Ekert, 1991, protokół oparty na EPR

- Istnieją inne protokoły kwantowe, np.
  - Artur Ekert, 1991, protokół oparty na EPR
  - B92 (Charles Bennett, 1992), baza nieortogonalna

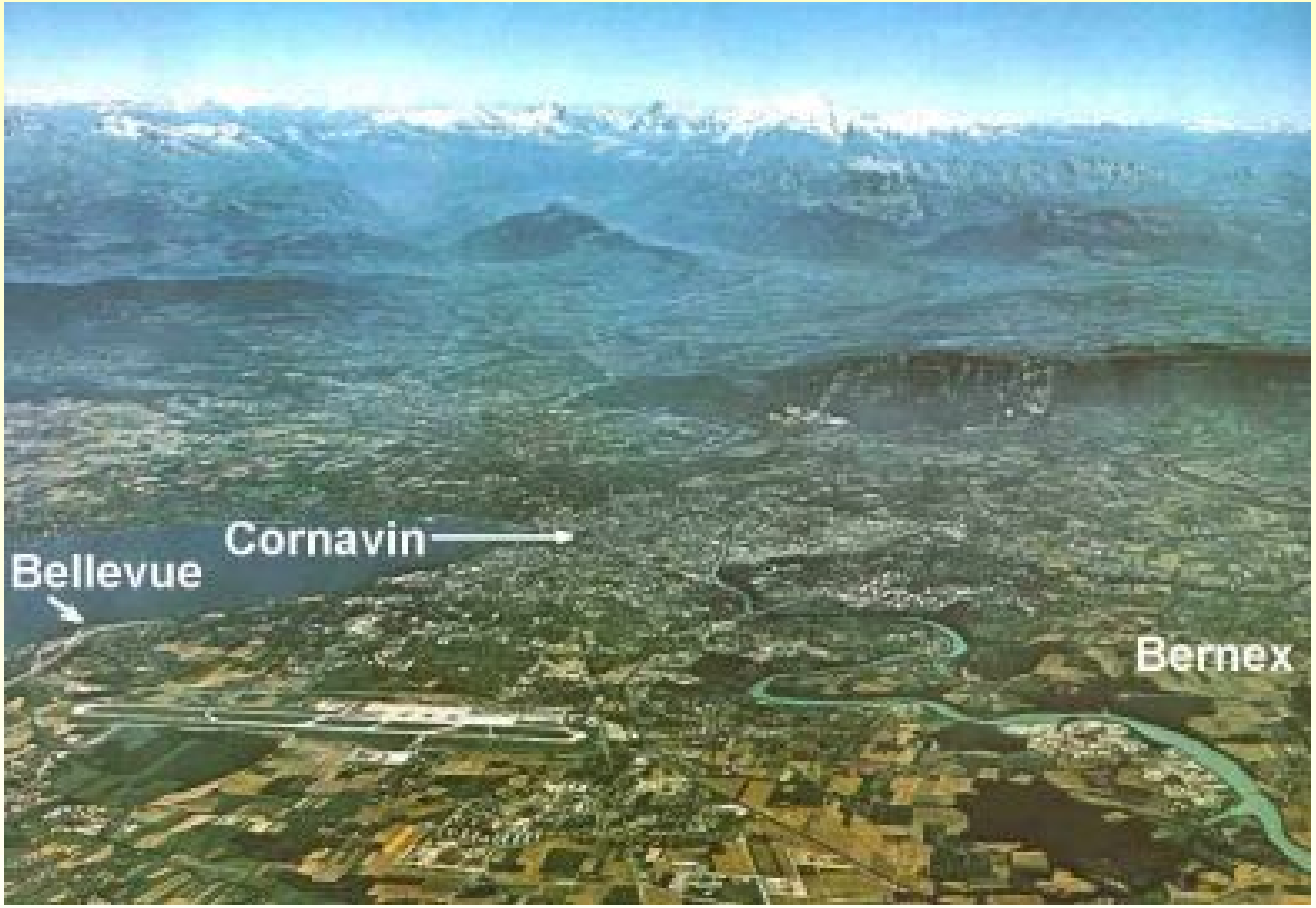
- Istnieją inne protokoły kwantowe, np.
  - Artur Ekert, 1991, protokół oparty na EPR
  - B92 (Charles Bennett, 1992), baza nieortogonalna
- Zamiast polaryzacji można używać fazy fotonów jako qubitów

- Istnieją inne protokoły kwantowe, np.
  - Artur Ekert, 1991, protokół oparty na EPR
  - B92 (Charles Bennett, 1992), baza nieortogonalna
- Zamiast polaryzacji można używać fazy fotonów jako qubitów
- Ciągle pojawiają się nowe propozycje!

2.7 Kryptografia kwantowa w praktyce



Pierwsze urządzenie do kwantowej kryptografii zbudowane w laboratoriach IBM (odległość 32 cm, 10 bitów/sek), Ch. Bennett i inni, 1992



Genewa — miejsce eksperymentów kwantowych na odległościach kilkudziesięciu kilometrów w światłowodach, N. Gisin, W. Tittel i inni, 2000, 2001

Kryptografia kwantowa jest już faktem!

Kryptografia kwantowa jest już faktem!

- Przy połączeniach światłowodowych uzyskuje się odległości kilkudziesięciu kilometrów (Genewa 23 km, Los Alamos 48 km)
- Prowadzi się intensywne badania nad połączeniami kwantowymi w powietrzu (Los Alamos, Hughes i inni, 2000, 1,6 km w świetle dziennym; Malvern, Gorman, Tapster, Rarity, 2001, 1,9 km w nocy)
- Plotka (prawdopodobna) głosi, że istnieje już połączenie kwantowe pomiędzy Białym Domem i Pentagonem.

Kryptografia kwantowa jest już faktem!

- Przy połączeniach światłowodowych uzyskuje się odległości kilkudziesięciu kilometrów (Genewa 23 km, Los Alamos 48 km)
- Prowadzi się intensywne badania nad połączeniami kwantowymi w powietrzu (Los Alamos, Hughes i inni, 2000, 1,6 km w świetle dziennym; Malvern, Gorman, Tapster, Rarity, 2001, 1,9 km w nocy)
- Plotka (prawdopodobna) głosi, że istnieje już połączenie kwantowe pomiędzy Białym Domem i Pentagonem.

Kryptografia kwantowa jest już faktem!

- Przy połączeniach światłowodowych uzyskuje się odległości kilkudziesięciu kilometrów (Genewa 23 km, Los Alamos 48 km)
- Prowadzi się intensywne badania nad połączeniami kwantowymi w powietrzu (Los Alamos, Hughes i inni, 2000, 1,6 km w świetle dziennym; Malvern, Gorman, Tapster, Rarity, 2001, 1,9 km w nocy)
- Plotka (prawdopodobna) głosi, że istnieje już połączenie kwantowe pomiędzy Białym Domem i Pentagonem.

Kryptografia kwantowa jest już faktem!

- Przy połączeniach światłowodowych uzyskuje się odległości kilkudziesięciu kilometrów (Genewa 23 km, Los Alamos 48 km)
- Prowadzi się intensywne badania nad połączeniami kwantowymi w powietrzu (Los Alamos, Hughes i inni, 2000, 1,6 km w świetle dziennym; Malvern, Gorman, Tapster, Rarity, 2001, 1,9 km w nocy)
- Plotka (prawdopodobna) głosi, że istnieje już połączenie kwantowe pomiędzy Białym Domem i Pentagonem.

Uczcie się optyki kwantowej!

Uczcie się optyki kwantowej!

Będziecie potrzebni!

Uczcie się optyki kwantowej!

Będziecie potrzebni!

Powodzenia!