VIII Festiwal Nauki i Sztuki

na

Wydziale Fizyki UAM

VIII Festiwal Nauki i Sztuki

na

Wydziale Fizyki UAM

Kryptografia kwantowa raz jeszcze

Ryszard Tanaś

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

13 października 2005

Enigma

niemiecka maszyna szyfrująca

Marian Rejewski

Jerzy Różycki

Henryk Zygalski

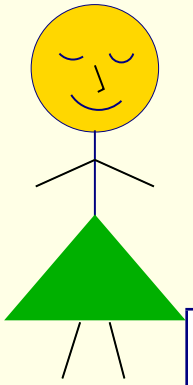
polscy matematycy, którzy

złamali szyfr enigmy

Plan wykładu

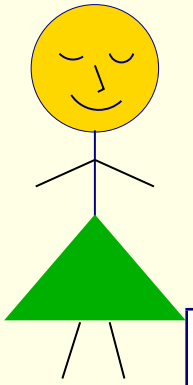
1 Główne postacie

1 Główne postacie

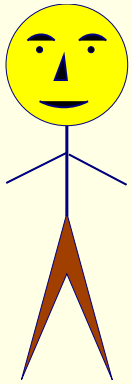


Alicja — nadawca informacji

1 Główne postacie

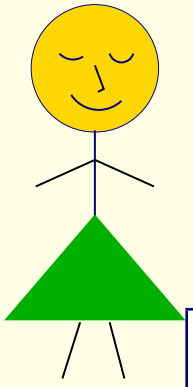


Alicja — nadawca informacji

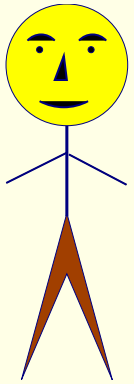


Bolek — odbiorca (adresat) informacji

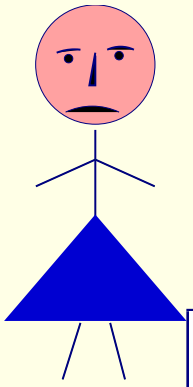
1 Główne postacie



Alicja — nadawca informacji

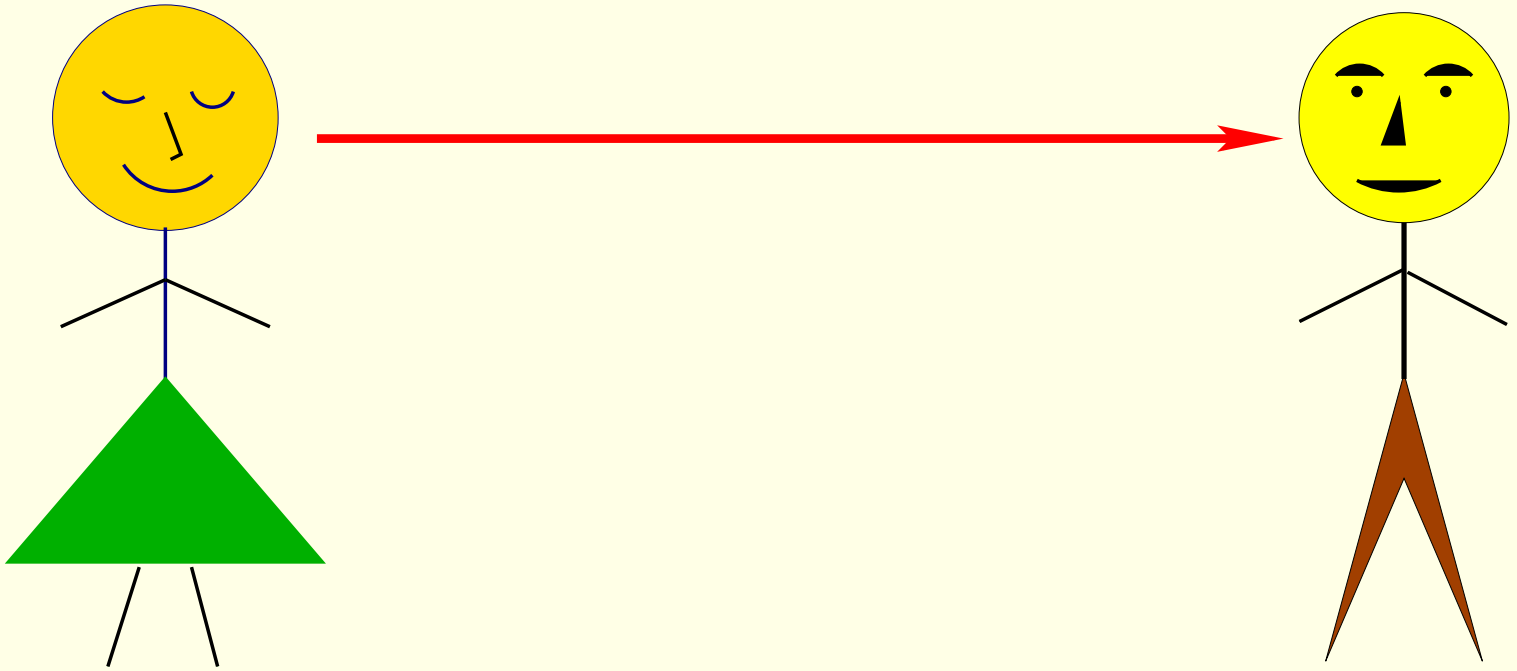


Bolek — odbiorca (adresat) informacji

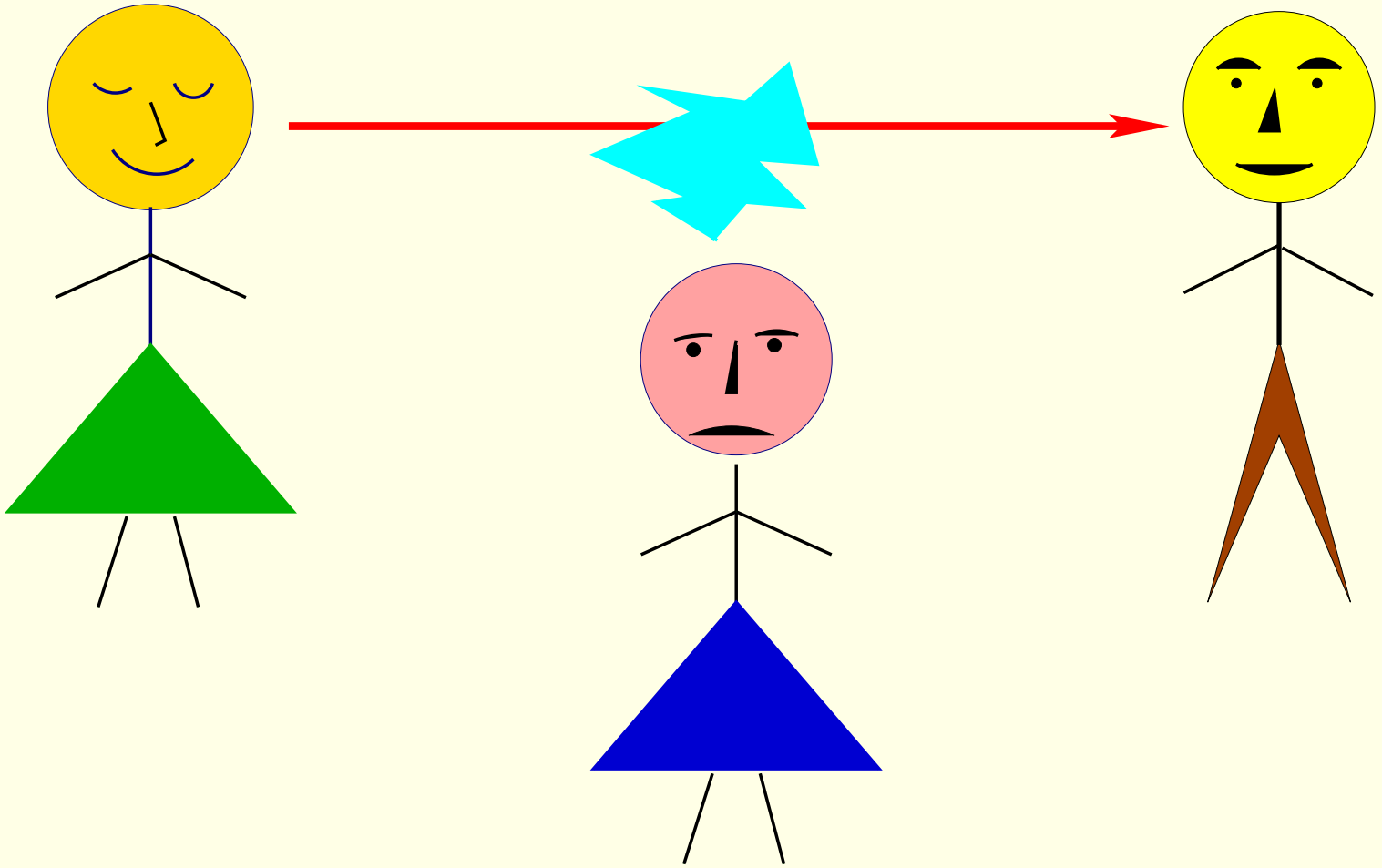


Ewa — usiłująca przechwycić informację

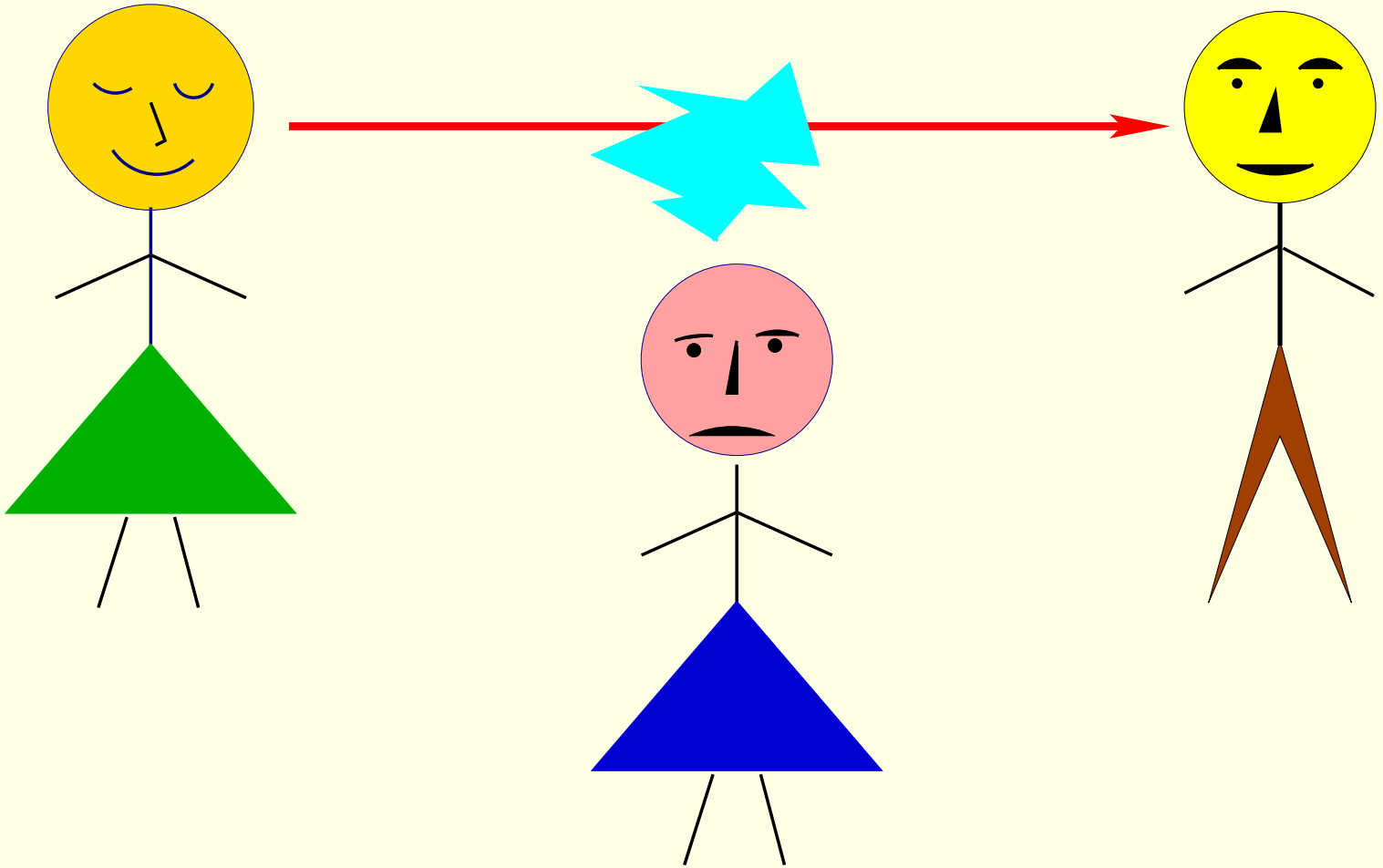
2 Kanał łączności



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

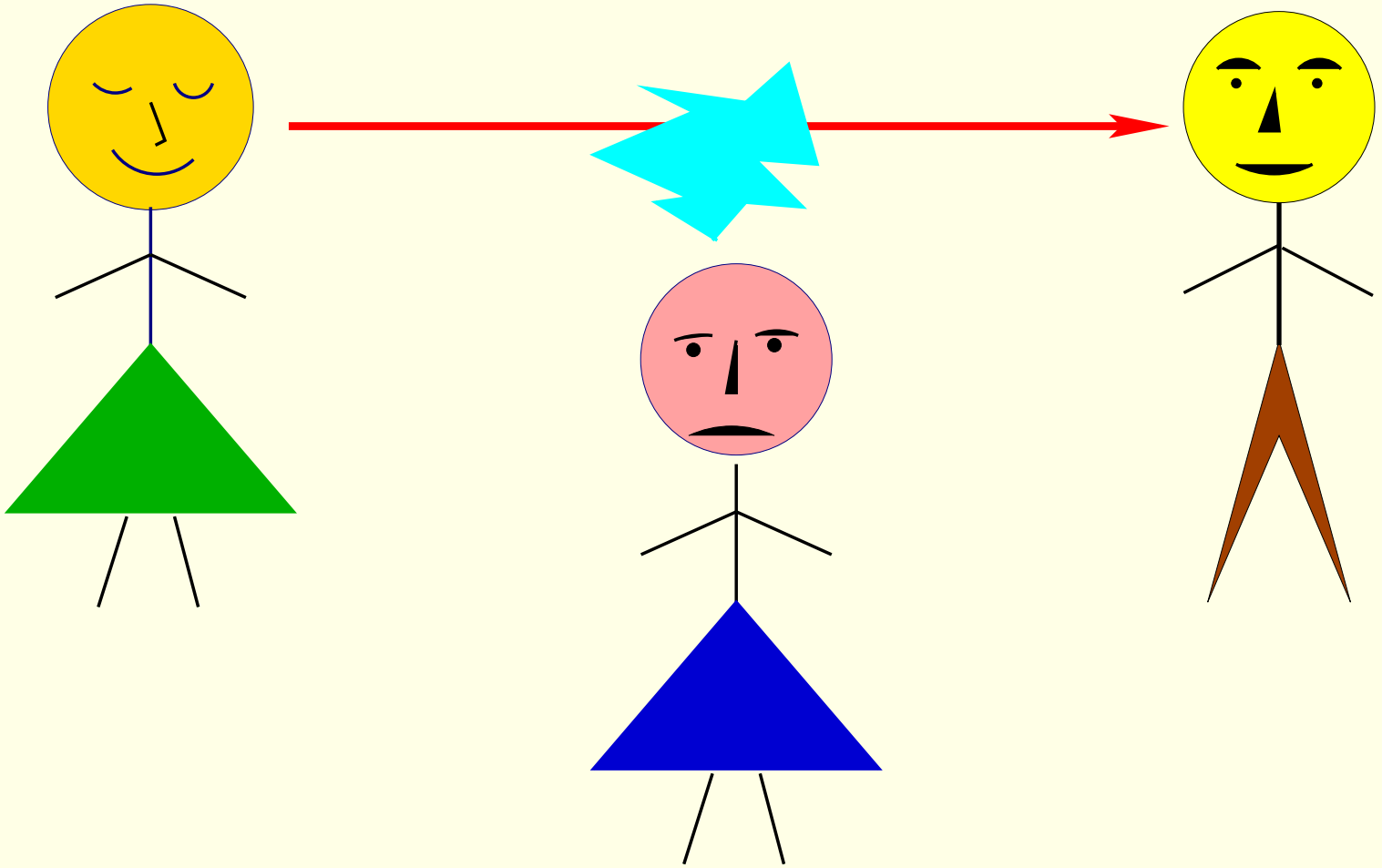


Ewa podsłuchuje usiłując dowiedzieć się co Alicja przesyła do Bolka



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!

3 Szyfr Vernama (one-time pad) — nie do złamania

Szyfry Che Guevary

Przykład

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.

Przykład

tekst jawny	⟶	S	Z	Y	F	R
binarnie	⟶	01010011	01011010	01011001	01000110	01010010
klucz	⟶	01110010	01010101	11011100	10110011	00101011
kryptogram	⟶	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.

Przykład

tekst jawny	⟶	S	Z	Y	F	R
binarnie	⟶	01010011	01011010	01011001	01000110	01010010
klucz	⟶	01110010	01010101	11011100	10110011	00101011
kryptogram	⟶	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.

Przykład

tekst jawny	⟶	S	Z	Y	F	R
binarnie	⟶	01010011	01011010	01011001	01000110	01010010
klucz	⟶	01110010	01010101	11011100	10110011	00101011
kryptogram	⟶	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.

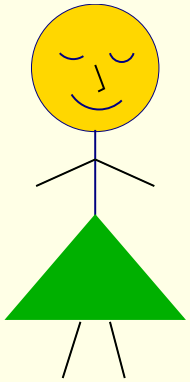
Przykład

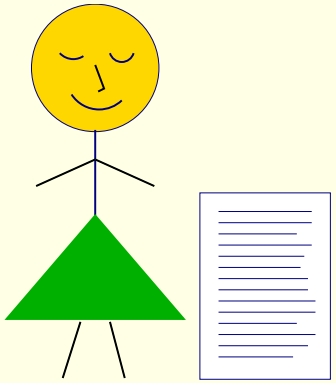
tekst jawny	⟶	S	Z	Y	F	R
binarnie	⟶	01010011	01011010	01011001	01000110	01010010
klucz	⟶	01110010	01010101	11011100	10110011	00101011
kryptogram	⟶	00100001	00001111	10000101	11110101	01111001

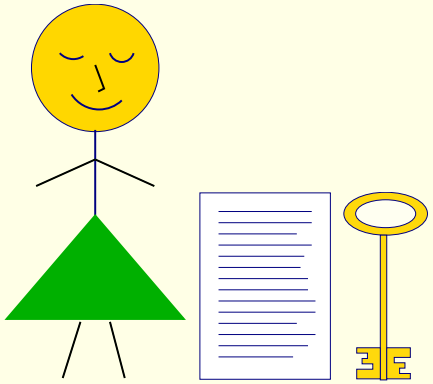
- Klucz jest losowym ciągiem bitów.
- Kryptogram jest także losowym ciągiem bitów i jeśli nie znamy klucza to nie dowiemy się niczego o tekście jawnym.
- Jeśli klucz jest tak długi jak wiadomość i użyty tylko raz, to szyfr ten gwarantuje bezpieczeństwo absolutne.
- Współczesne metody kryptograficzne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

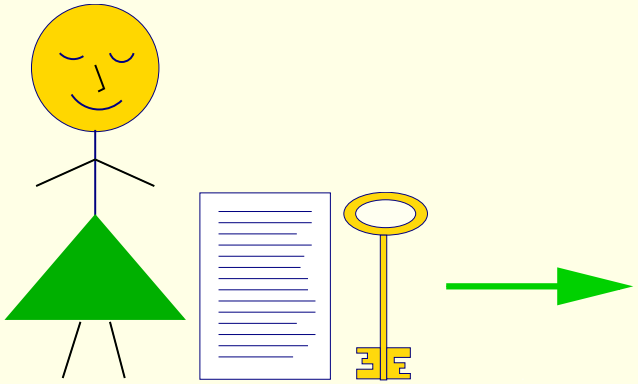
4 Klasyczne systemy kryptograficzne

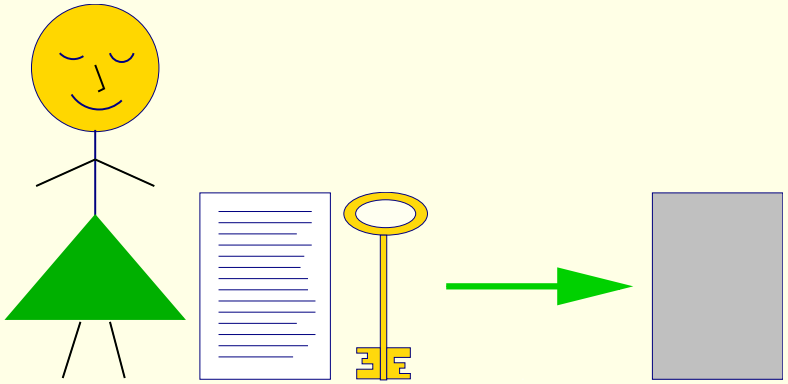
4.1 Systemy z kluczem tajnym

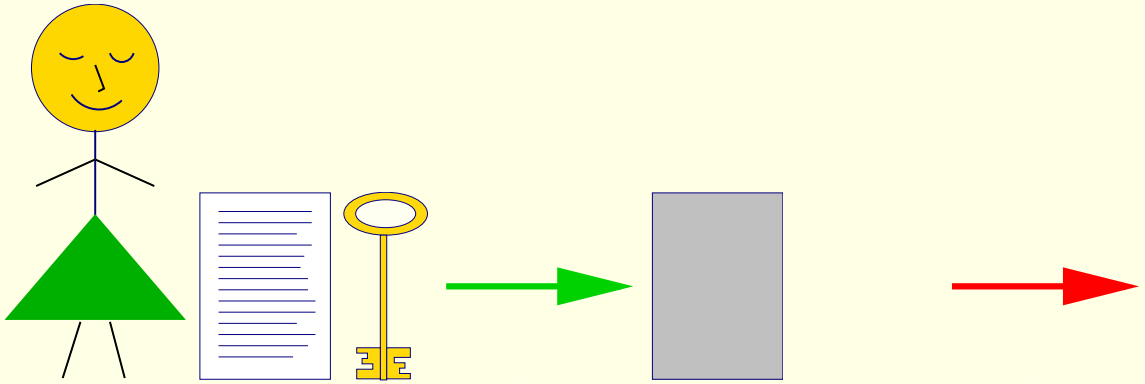


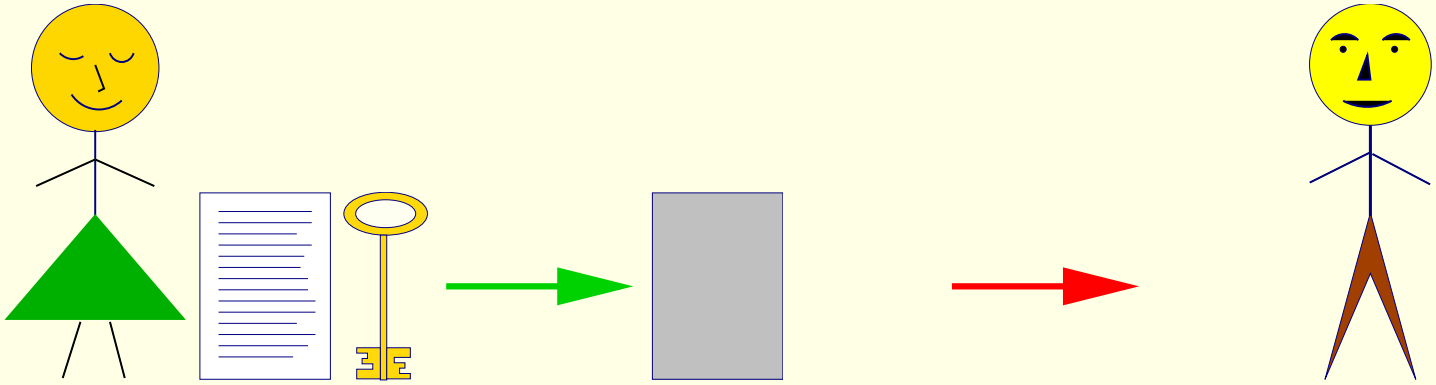


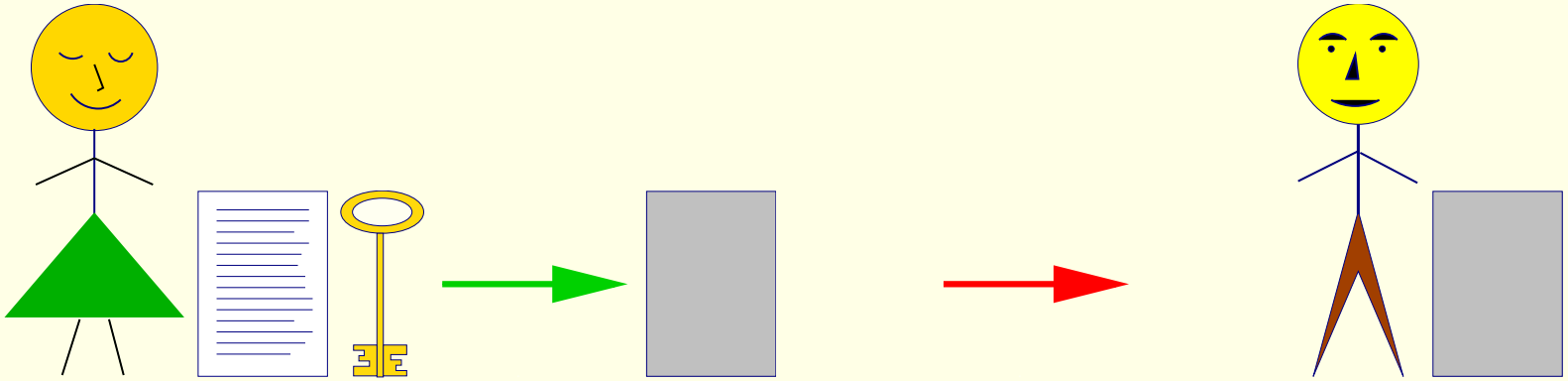


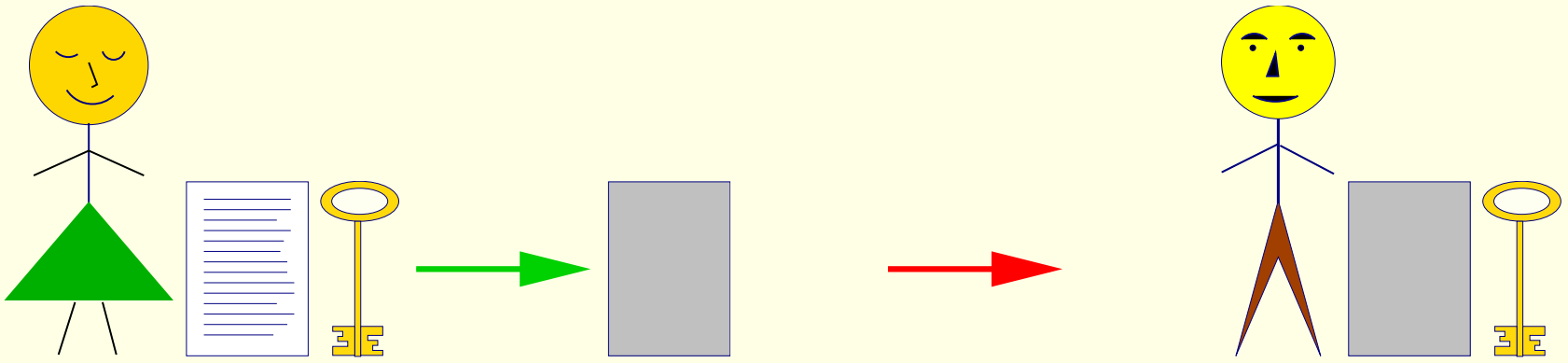


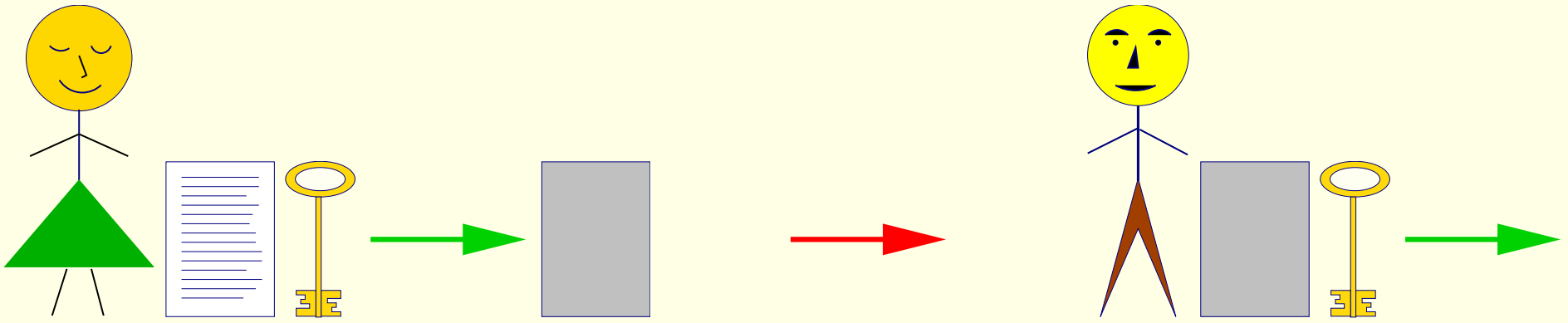


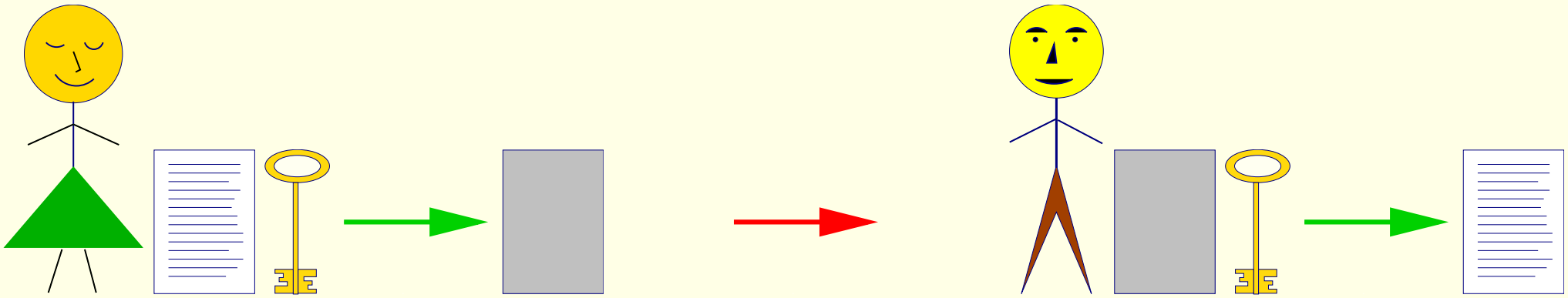


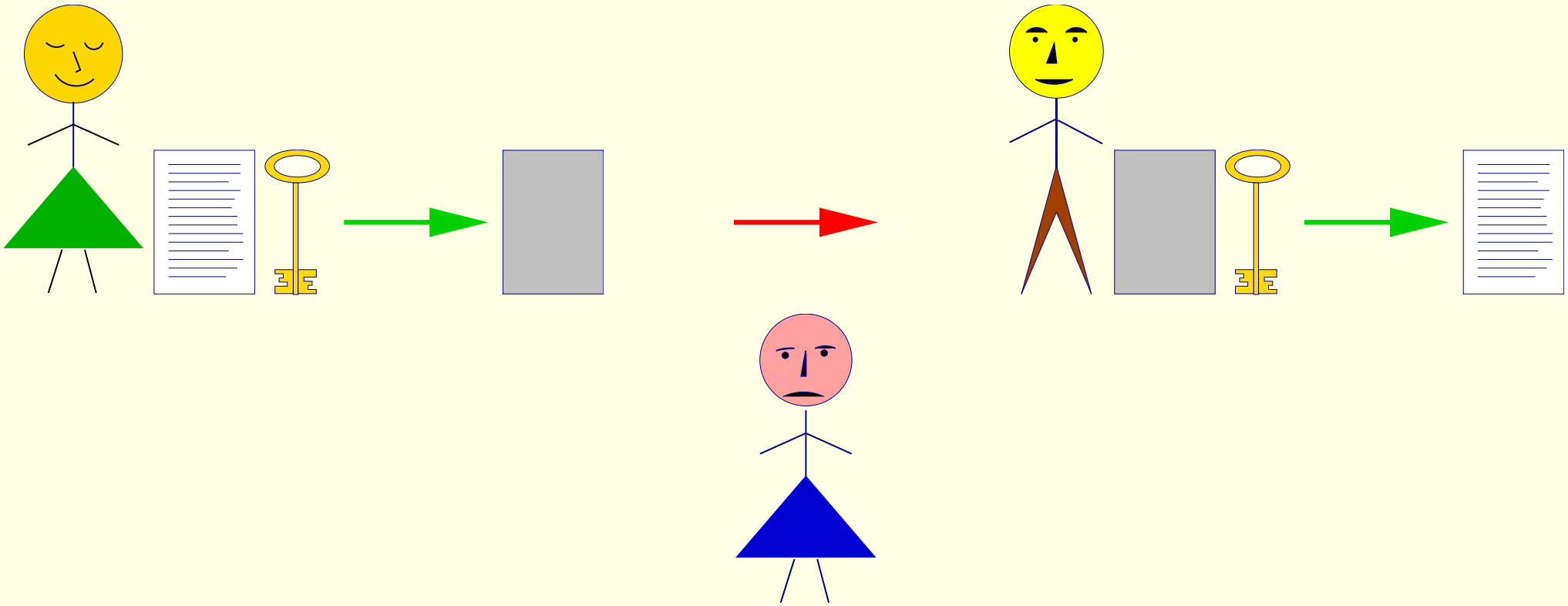


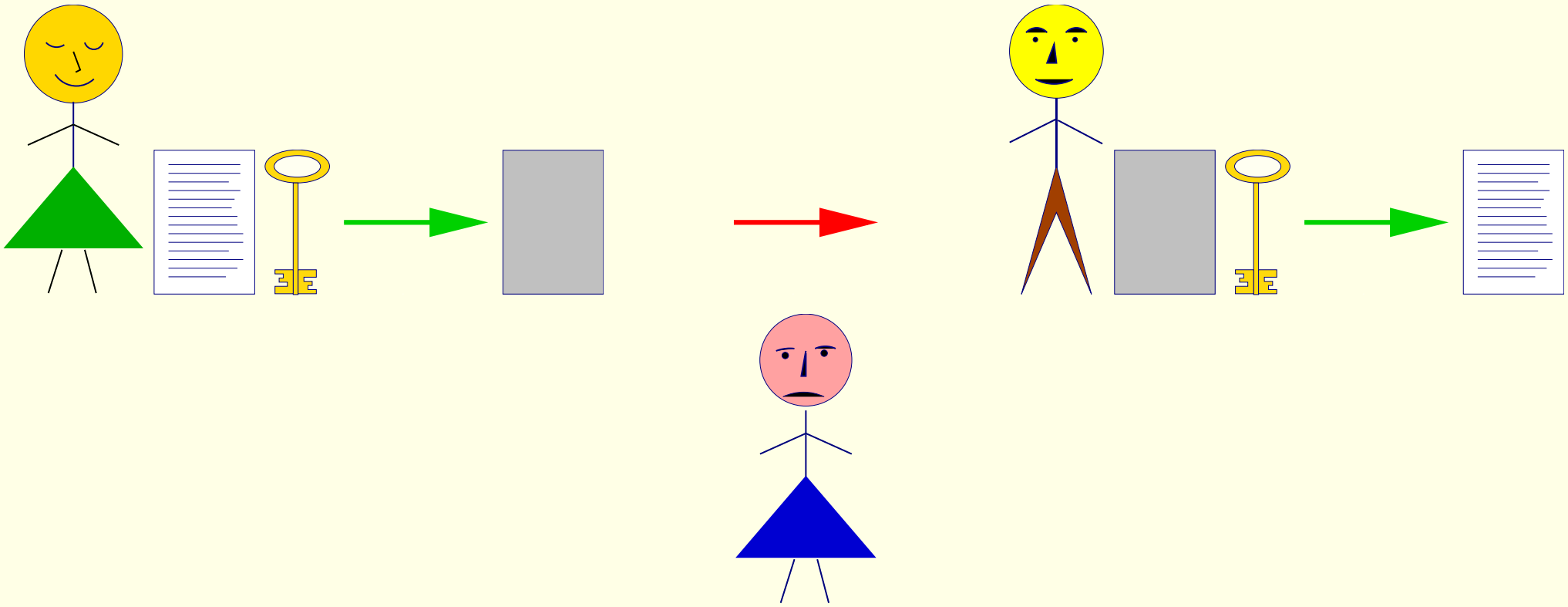


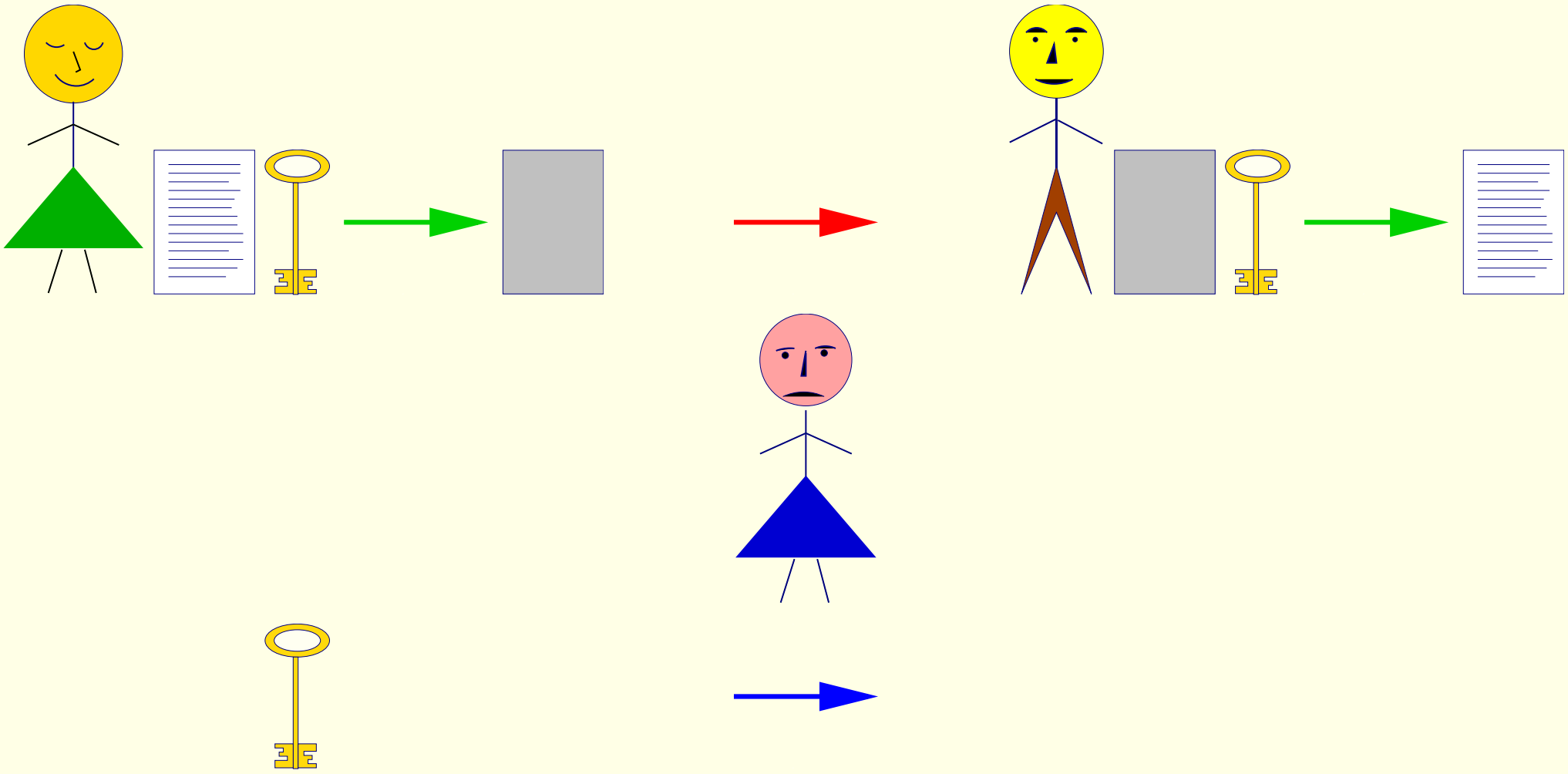


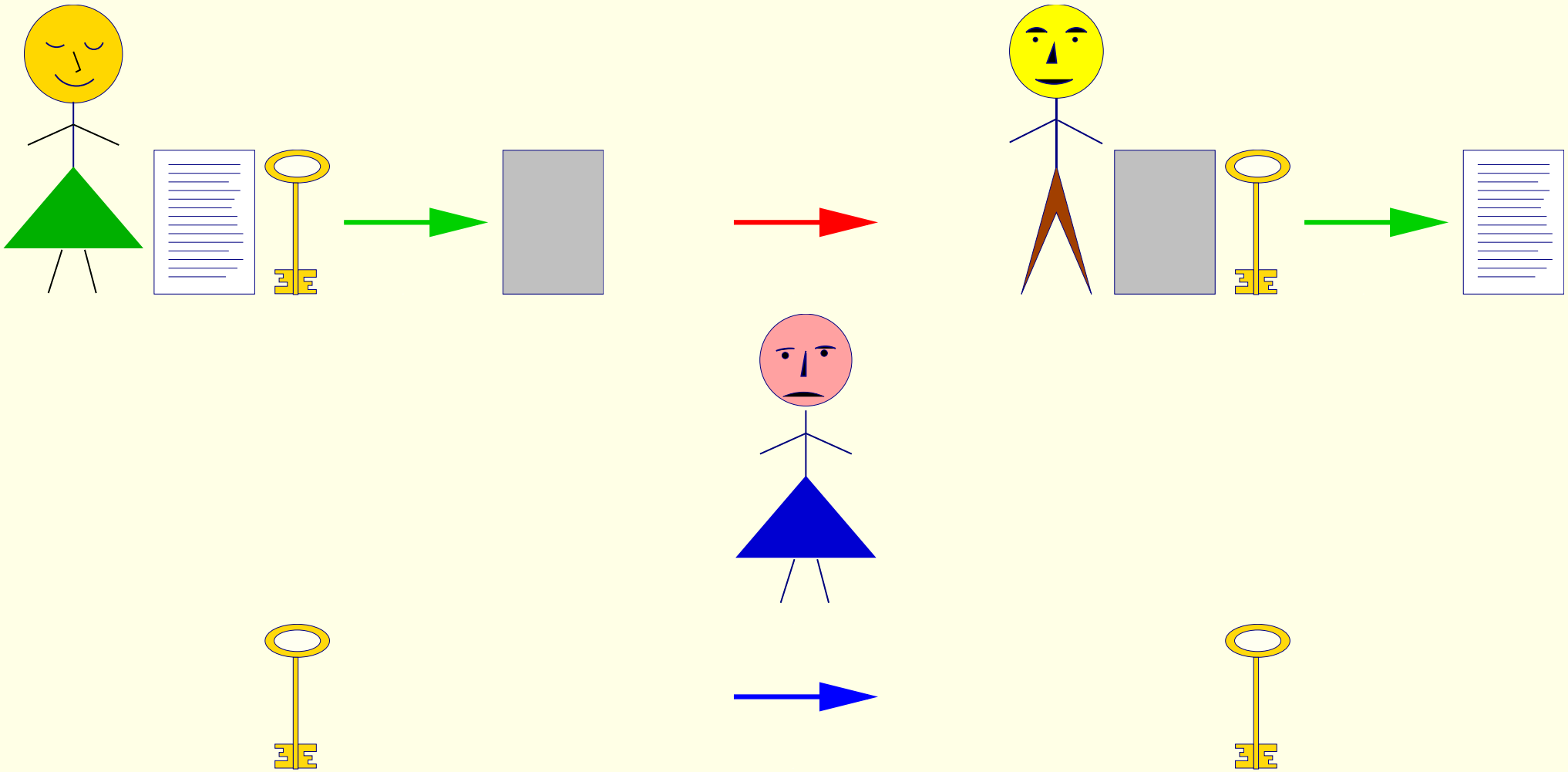


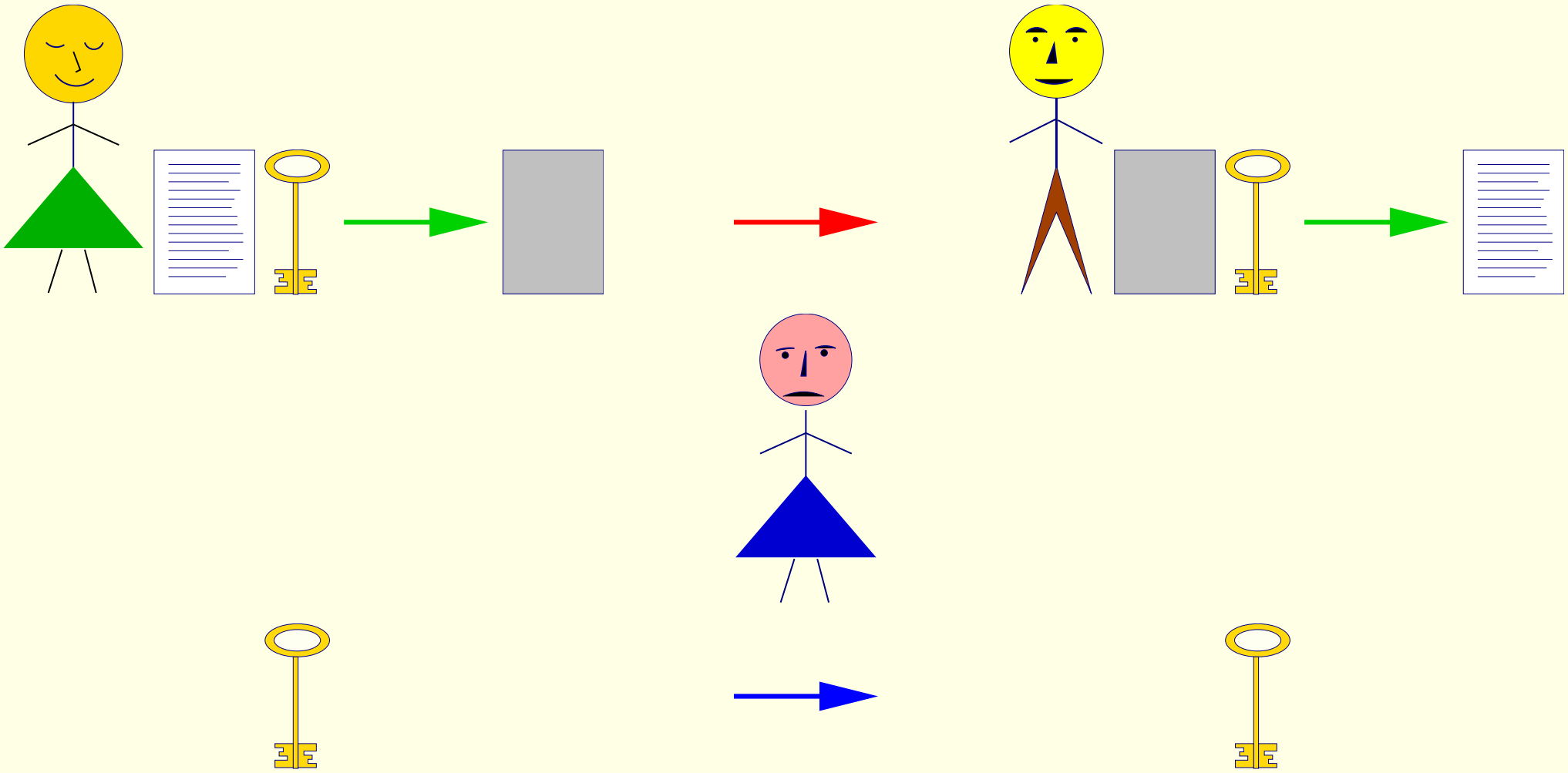




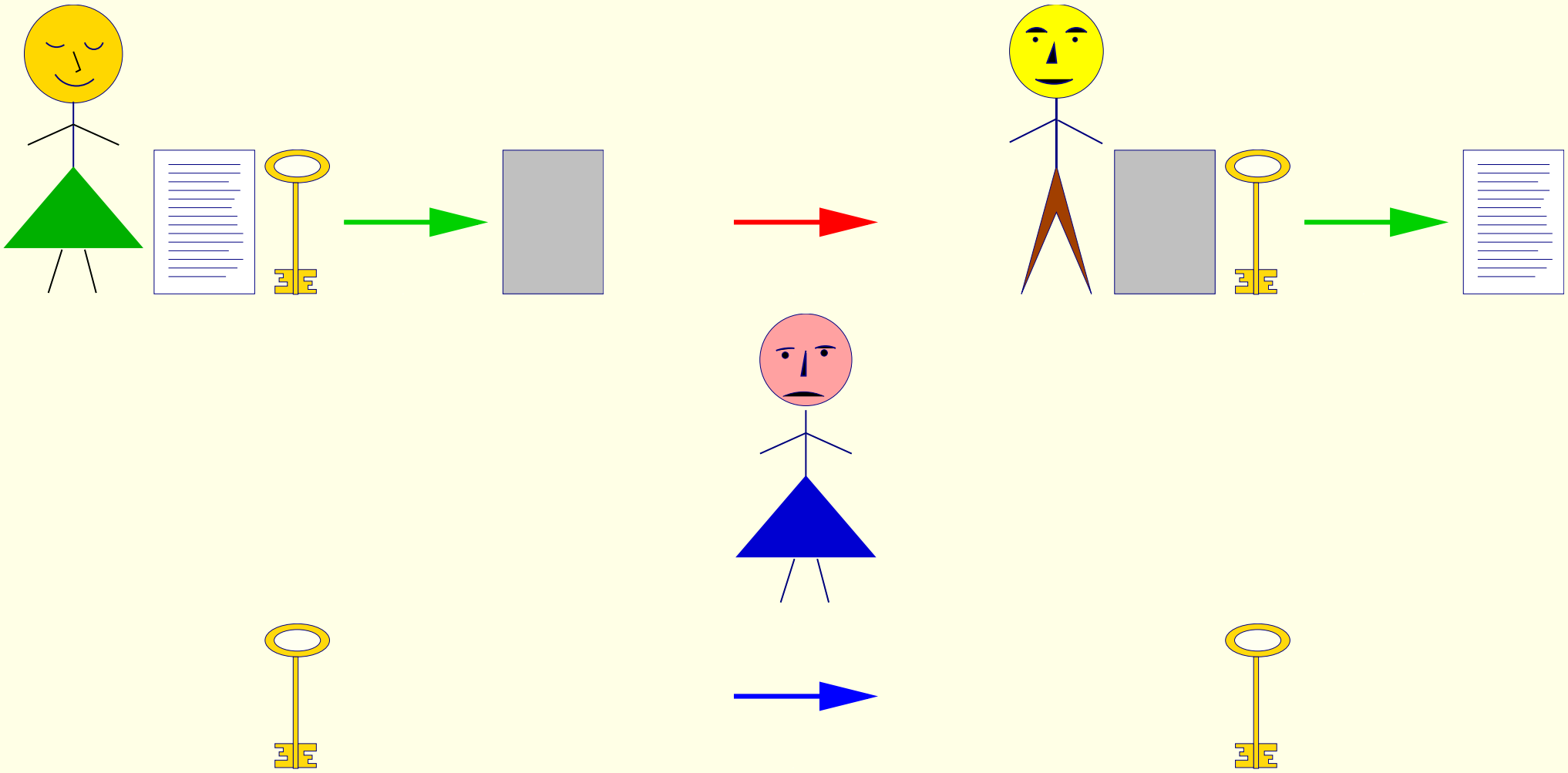






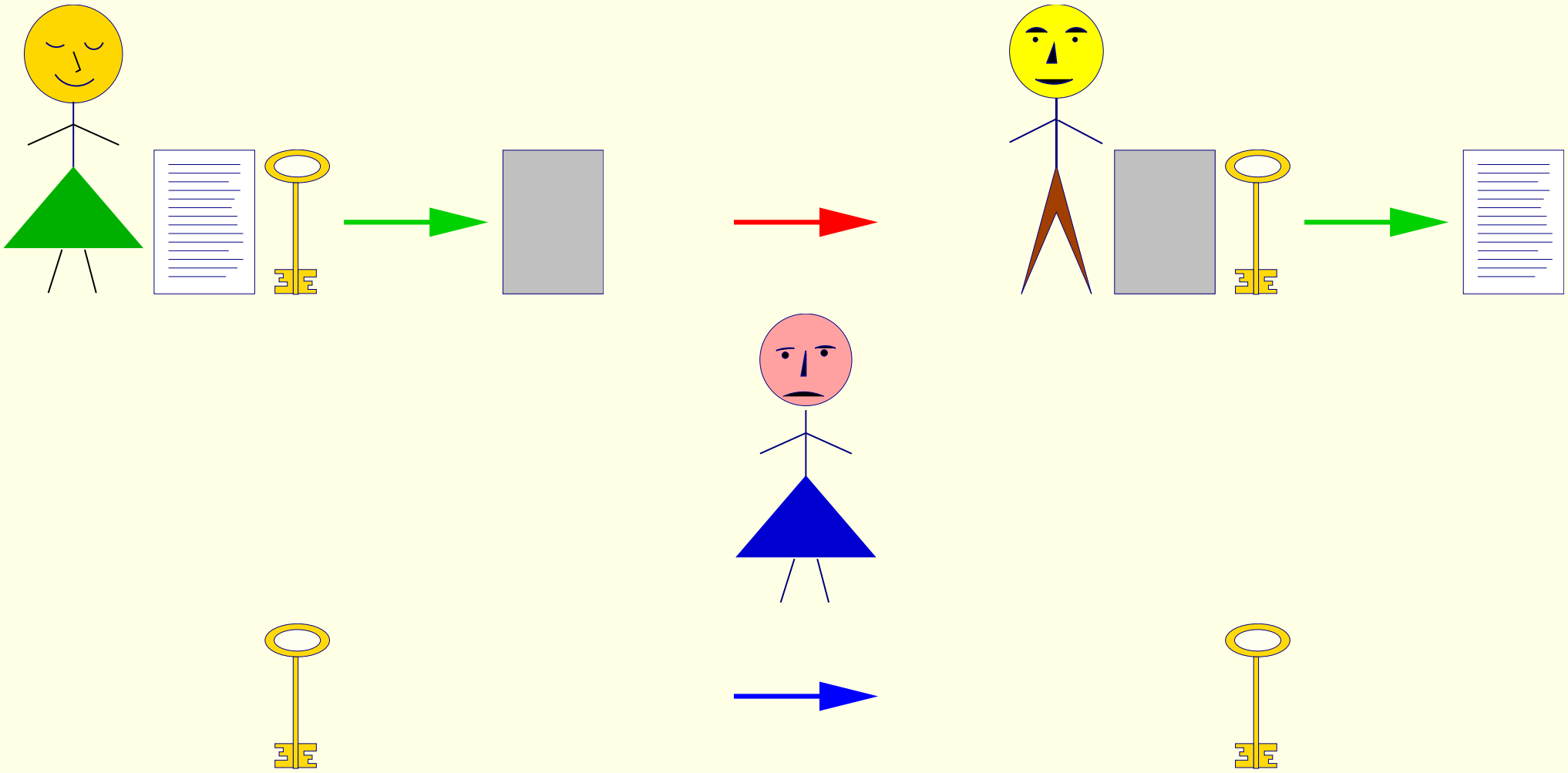


Pułapka



Pułapka

Aby zbudować bezpieczny kanał łączności . . .

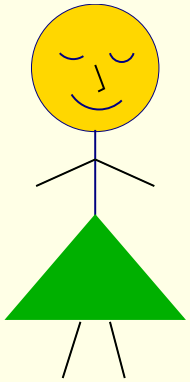


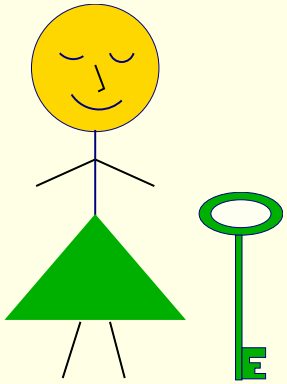
Pułapka

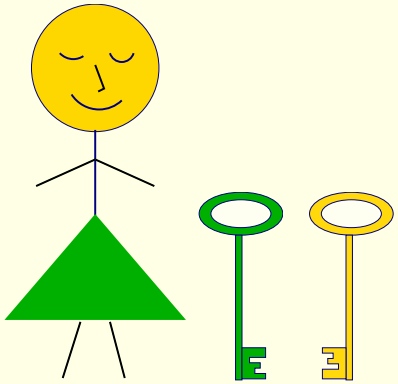
Aby zbudować bezpieczny kanał łączności . . .

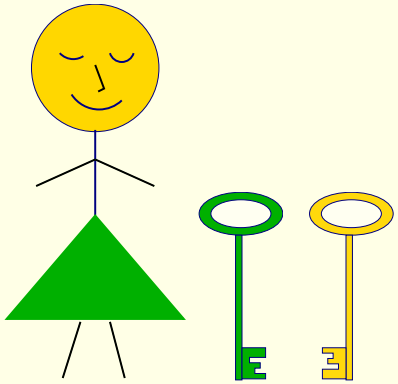
. . . trzeba mieć bezpieczny kanał łączności!

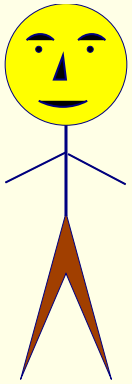
4.2 Systemy z kluczem publicznym

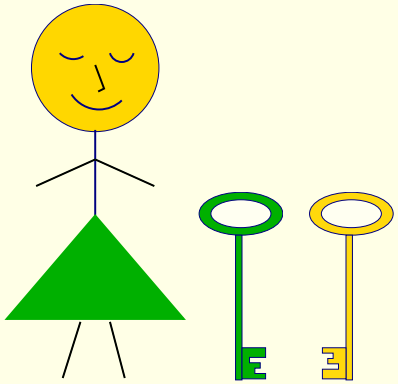


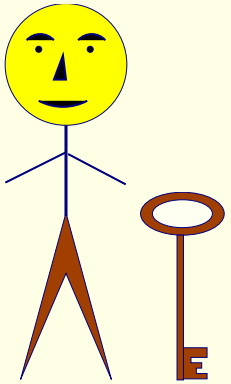


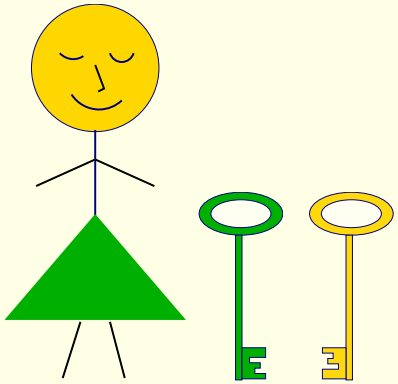


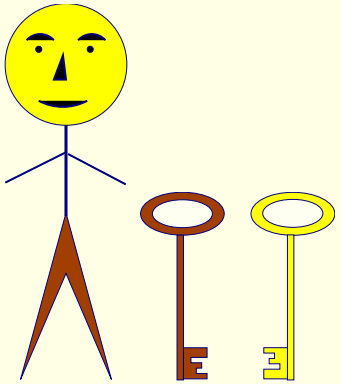


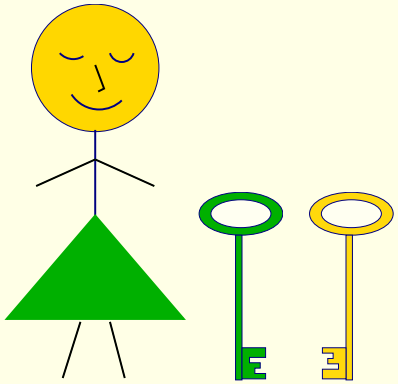




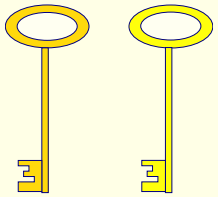




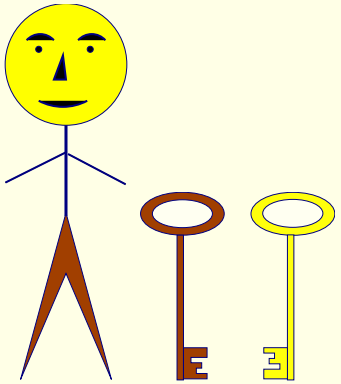


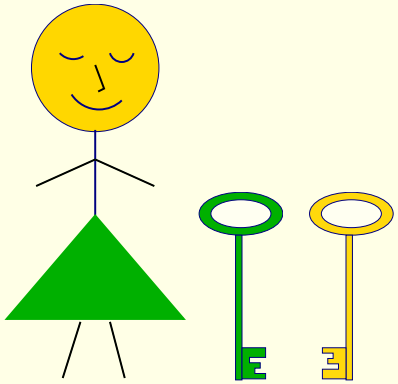


Klucze

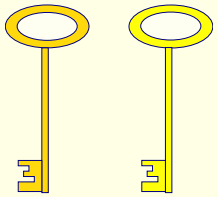


publiczne

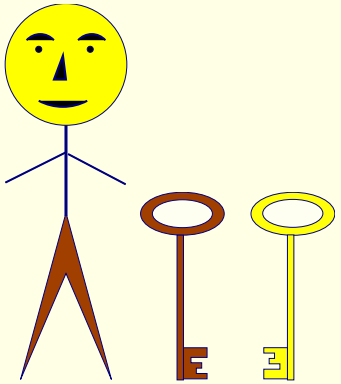


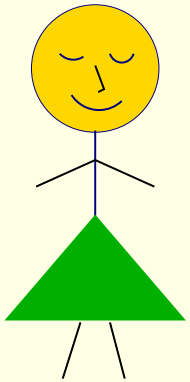


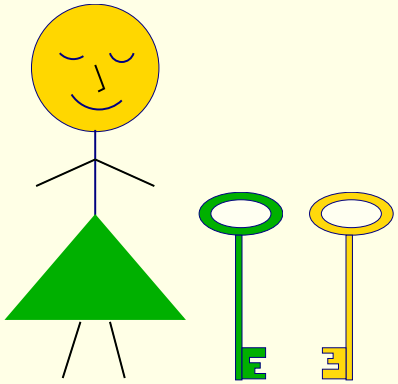
Klucze



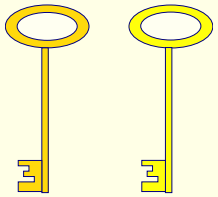
publiczne



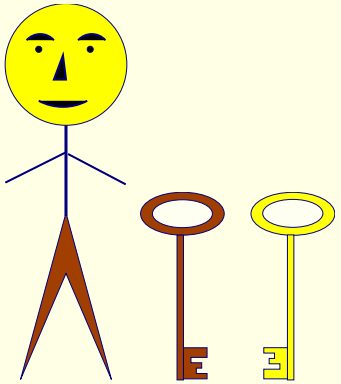


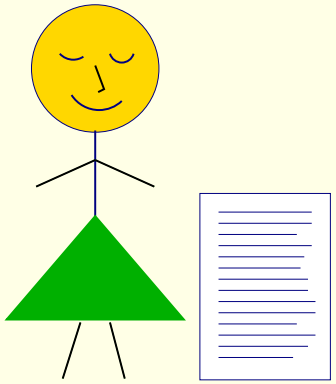


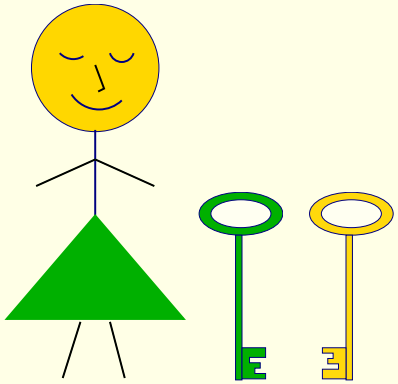
Klucze



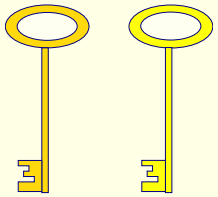
publiczne



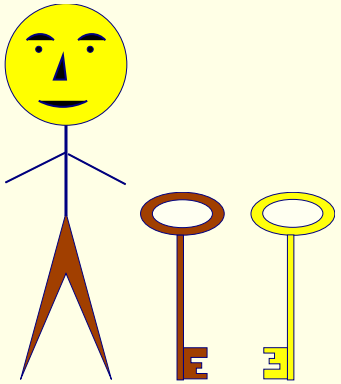


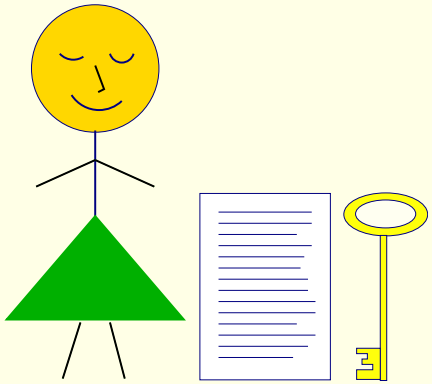


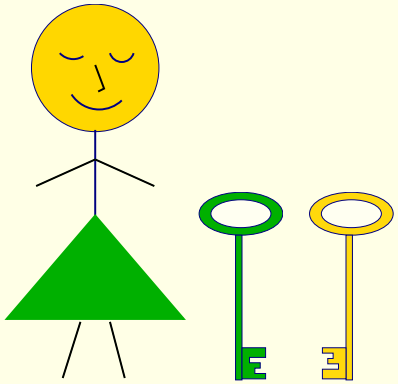
Klucze



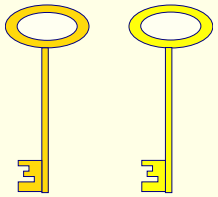
publiczne



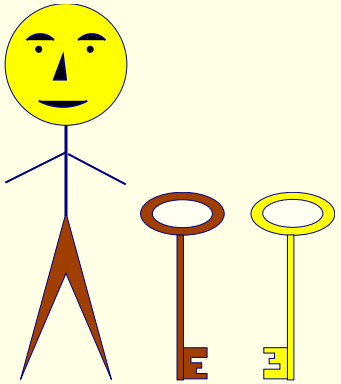


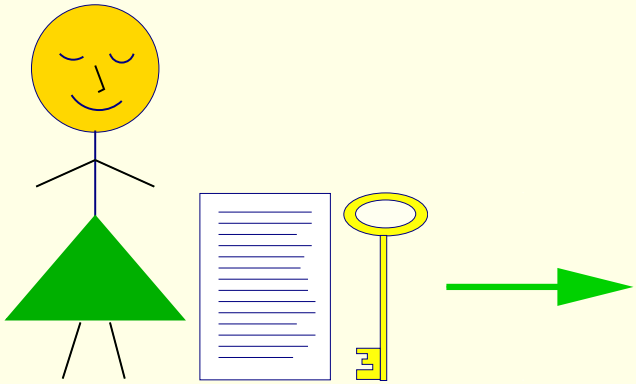


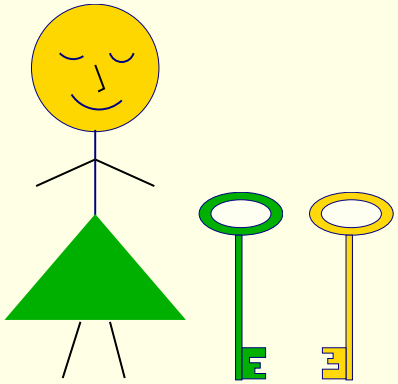
Klucze

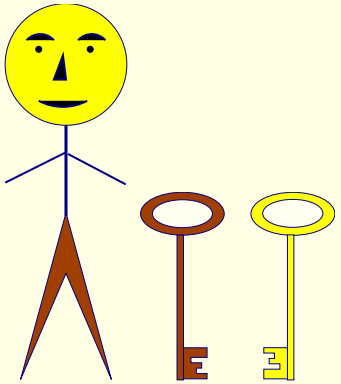


publiczne

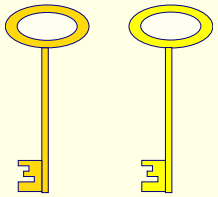




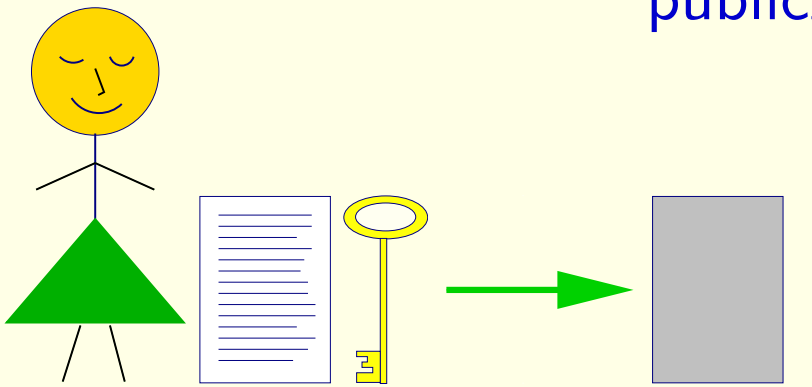


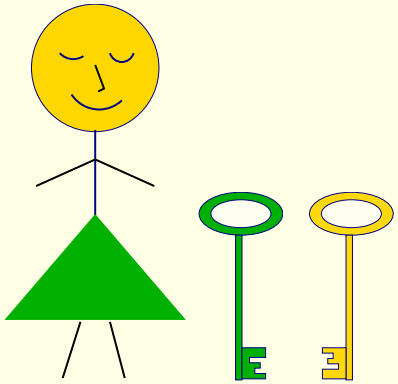


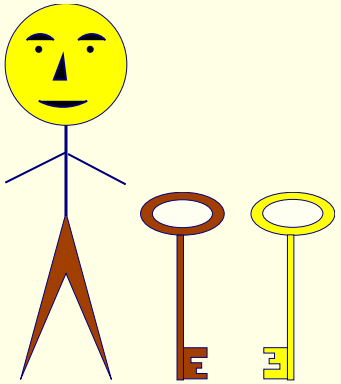
Klucze



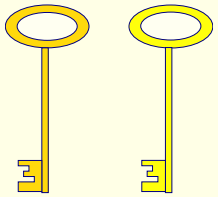
publiczne



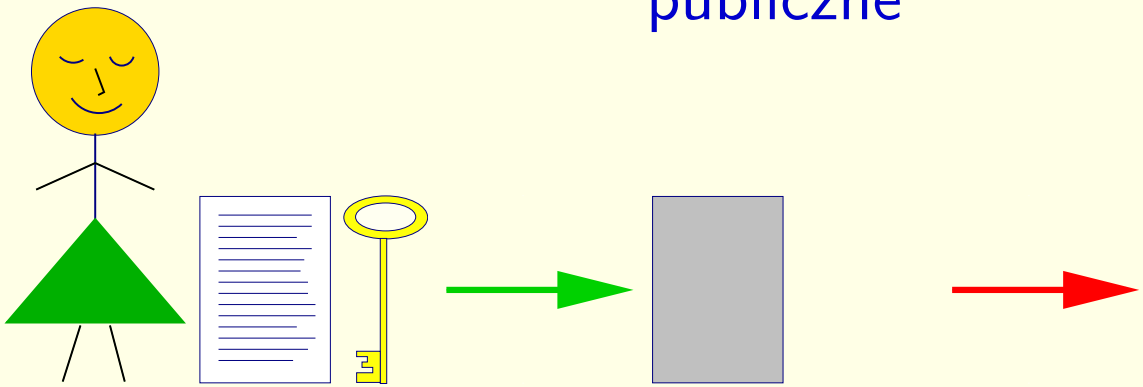


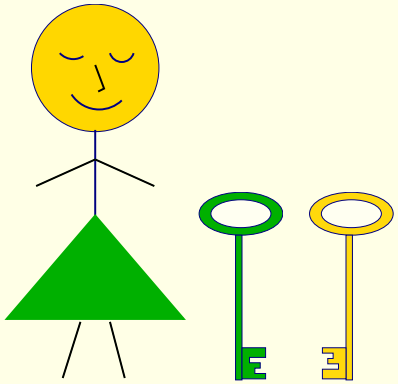


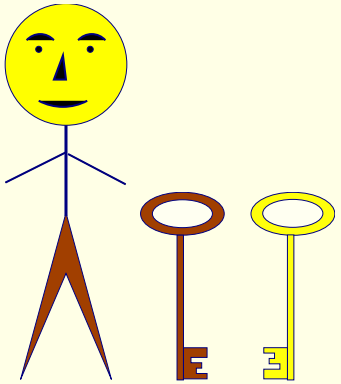
Klucze



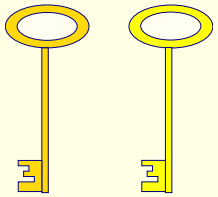
publiczne



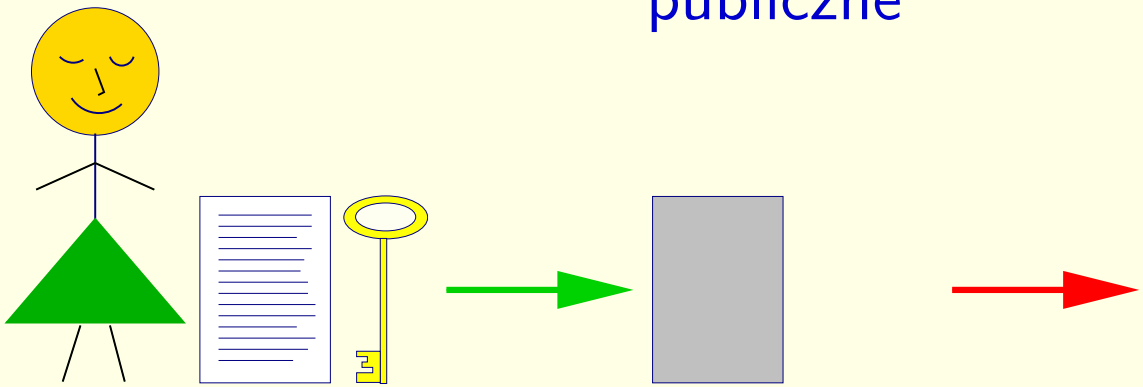


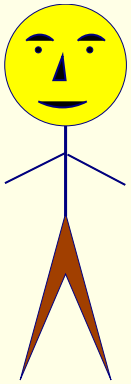


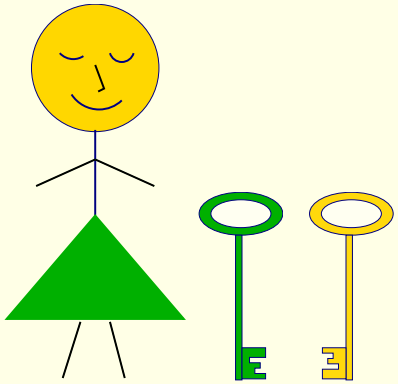
Klucze

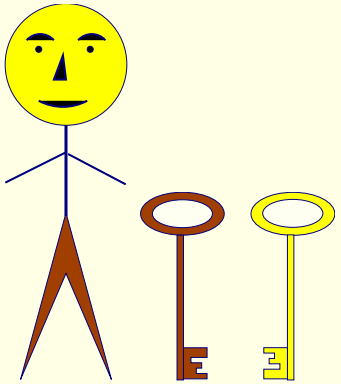


publiczne

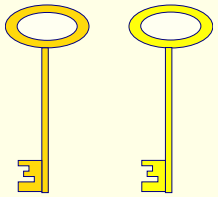




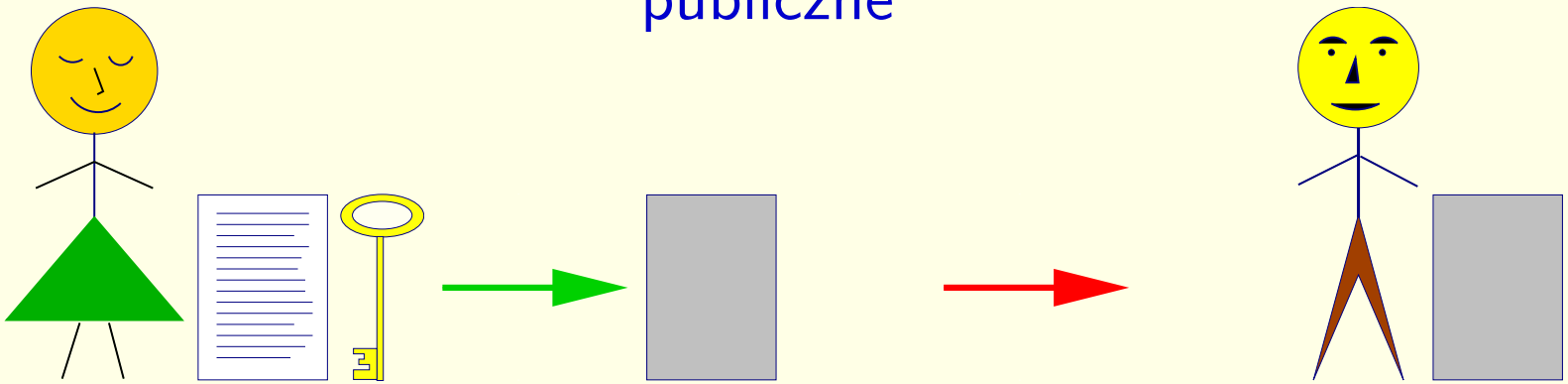


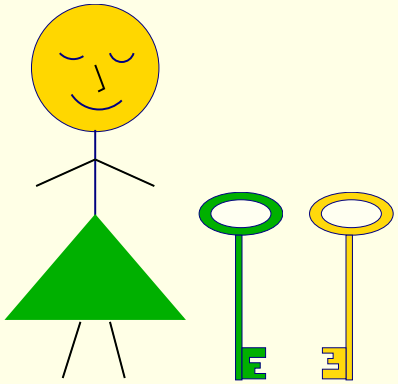


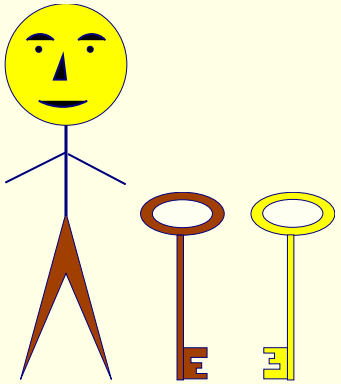
Klucze



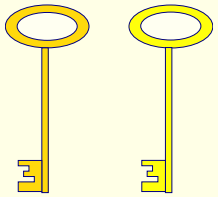
publiczne



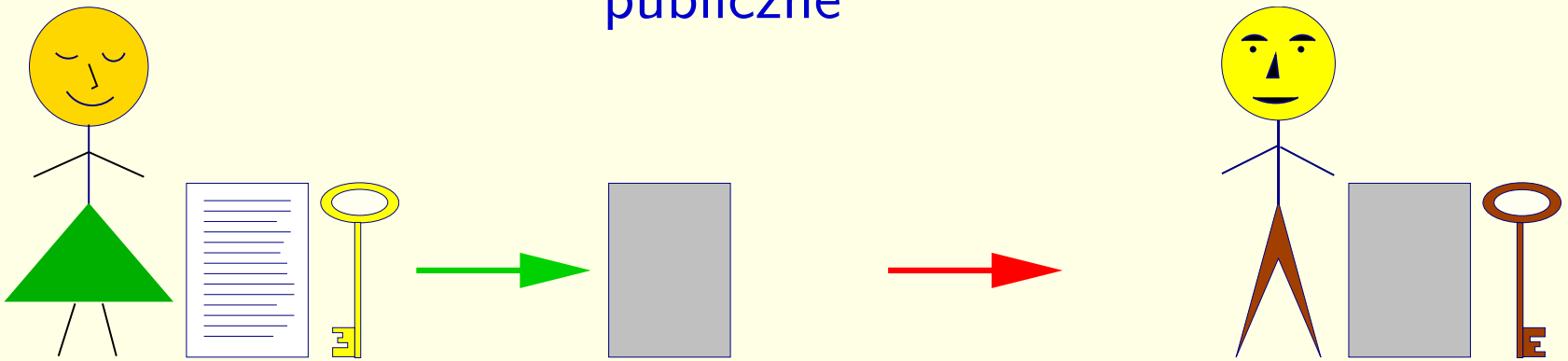


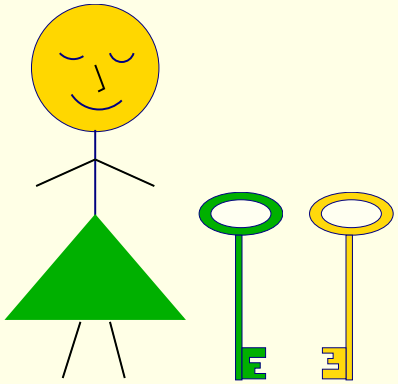


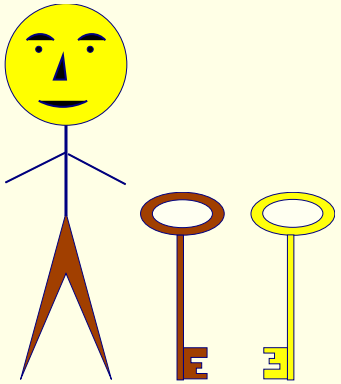
Klucze



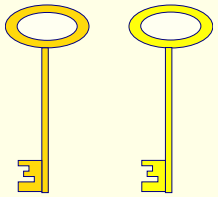
publiczne



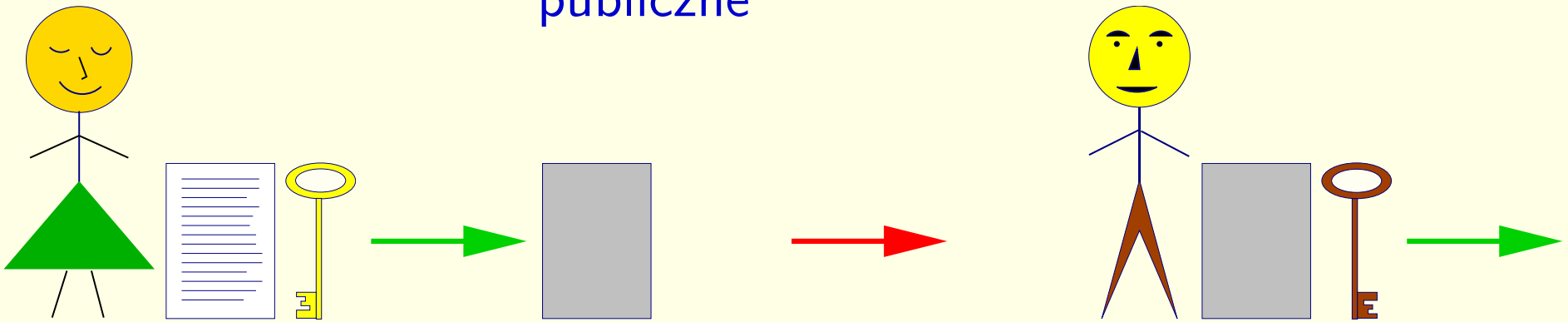


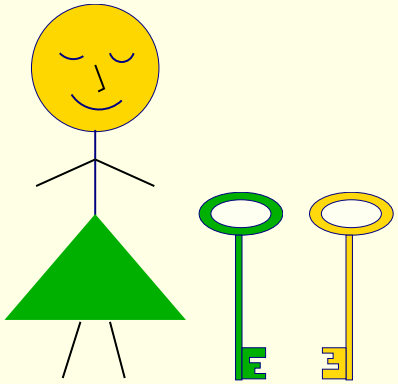


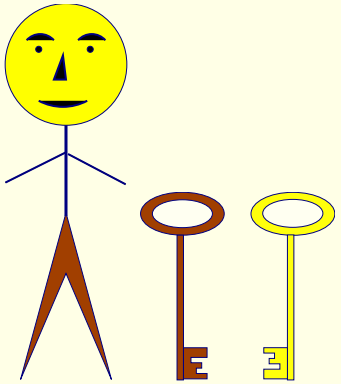
Klucze



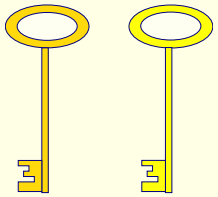
publiczne



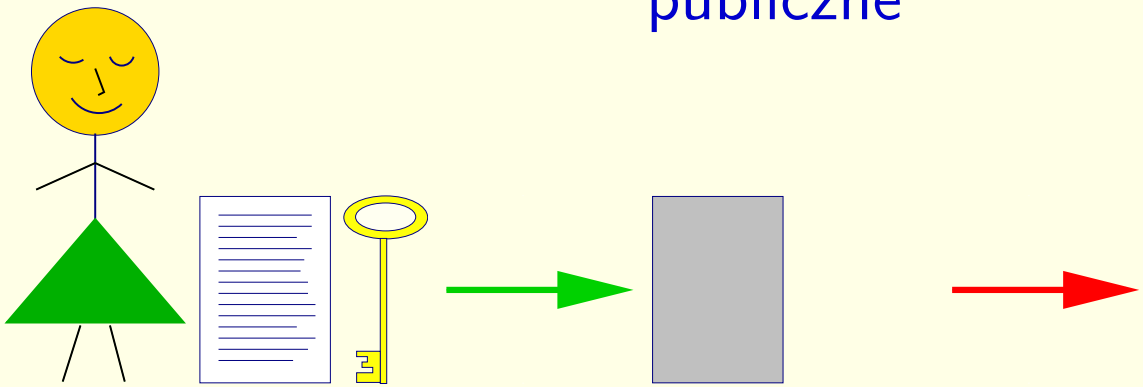


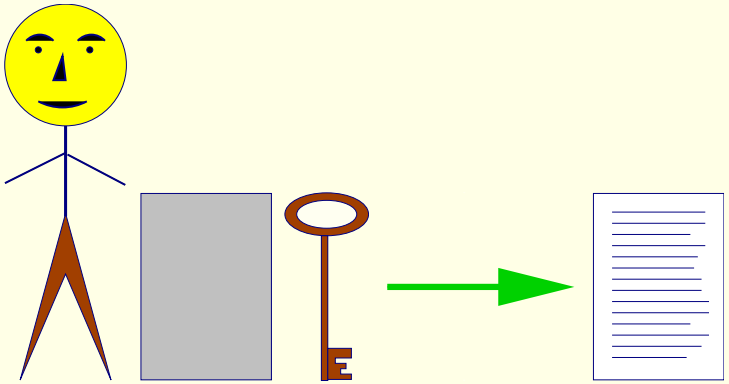


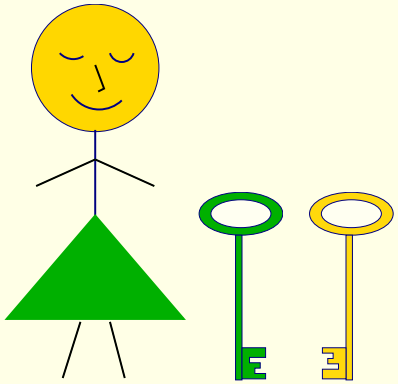
Klucze

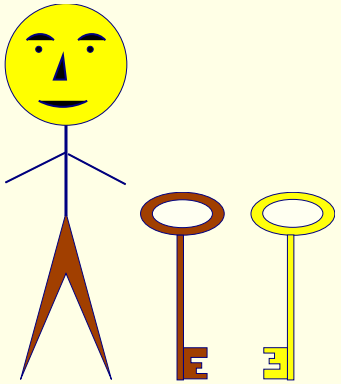


publiczne

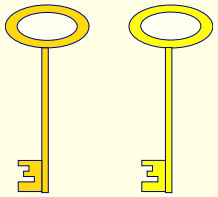




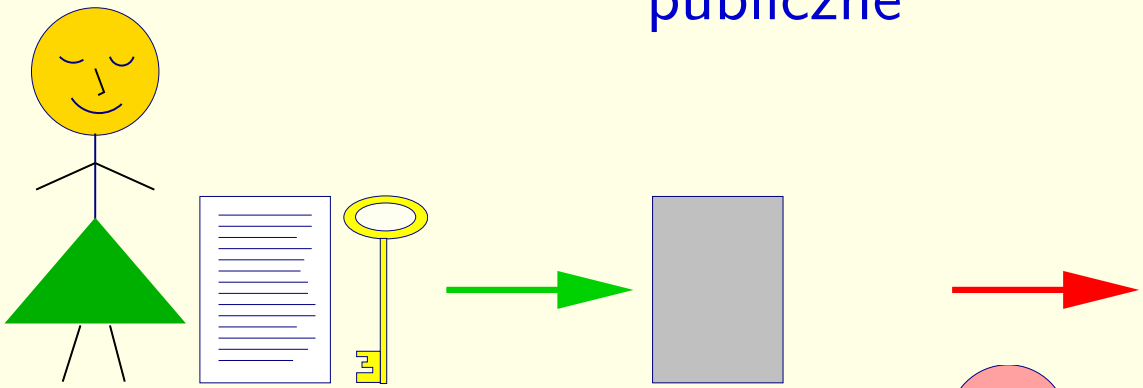


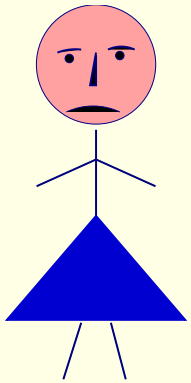


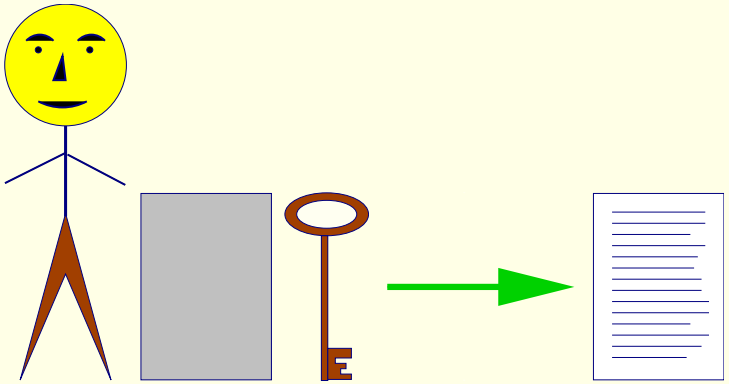
Klucze

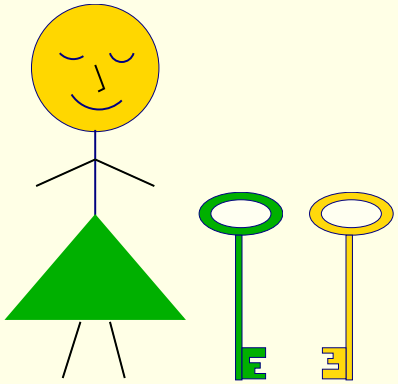


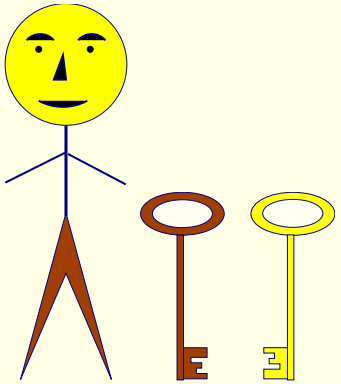
publiczne



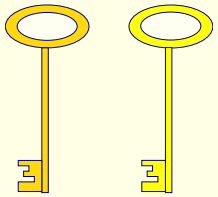




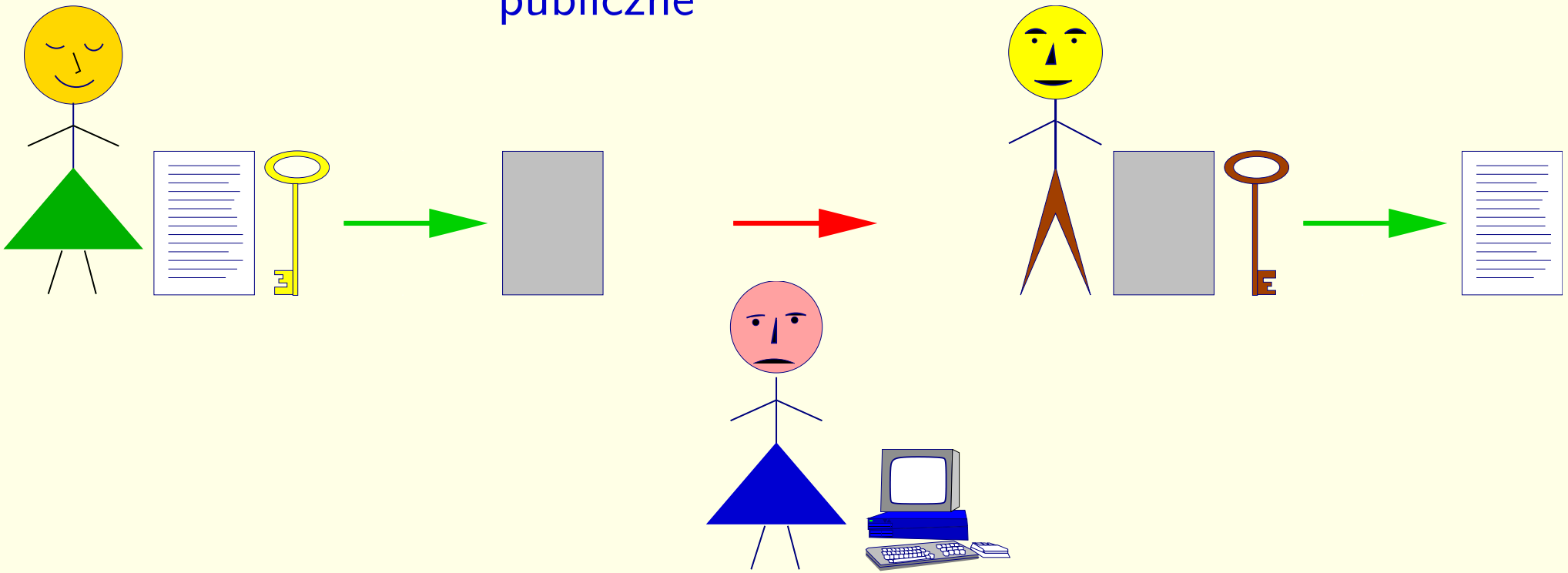




Klucze



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)
- Najbardziej znany kryptosystem z kluczem publicznym, RSA, opiera się na trudności z rozkładem liczby na czynniki (faktoryzacja)

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)

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)

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

$$425734521821081888851 \quad = \quad \square \cdot \square$$

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

$$425734521821081888 51 = \square \cdot \square$$

$$425734521821081888 51 =$$

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

$$425734521821081888 51 = \boxed{} \cdot \boxed{}$$

$$425734521821081888 51 = 4657537033 \cdot 9140765147$$

RSA Challenge Numbers

Do sfaktoryzowania: RSA-640, 193 cyfry dziesiętne

RSA Challenge Numbers

Do sfaktoryzowania: RSA-640, 193 cyfry dziesiętne

3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609

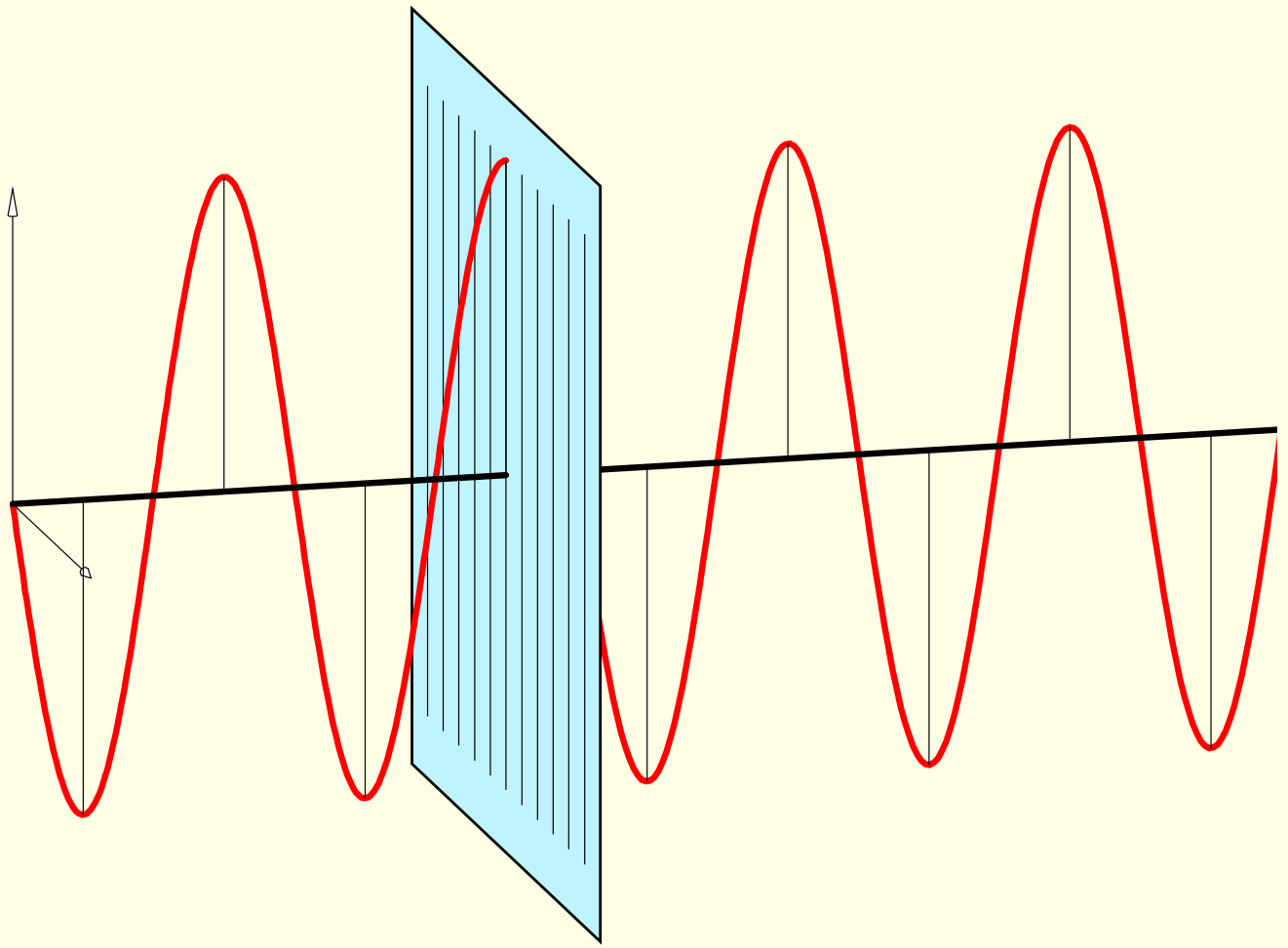
RSA Challenge Numbers

Do sfaktoryzowania: RSA-640, 193 cyfry dziesiętne

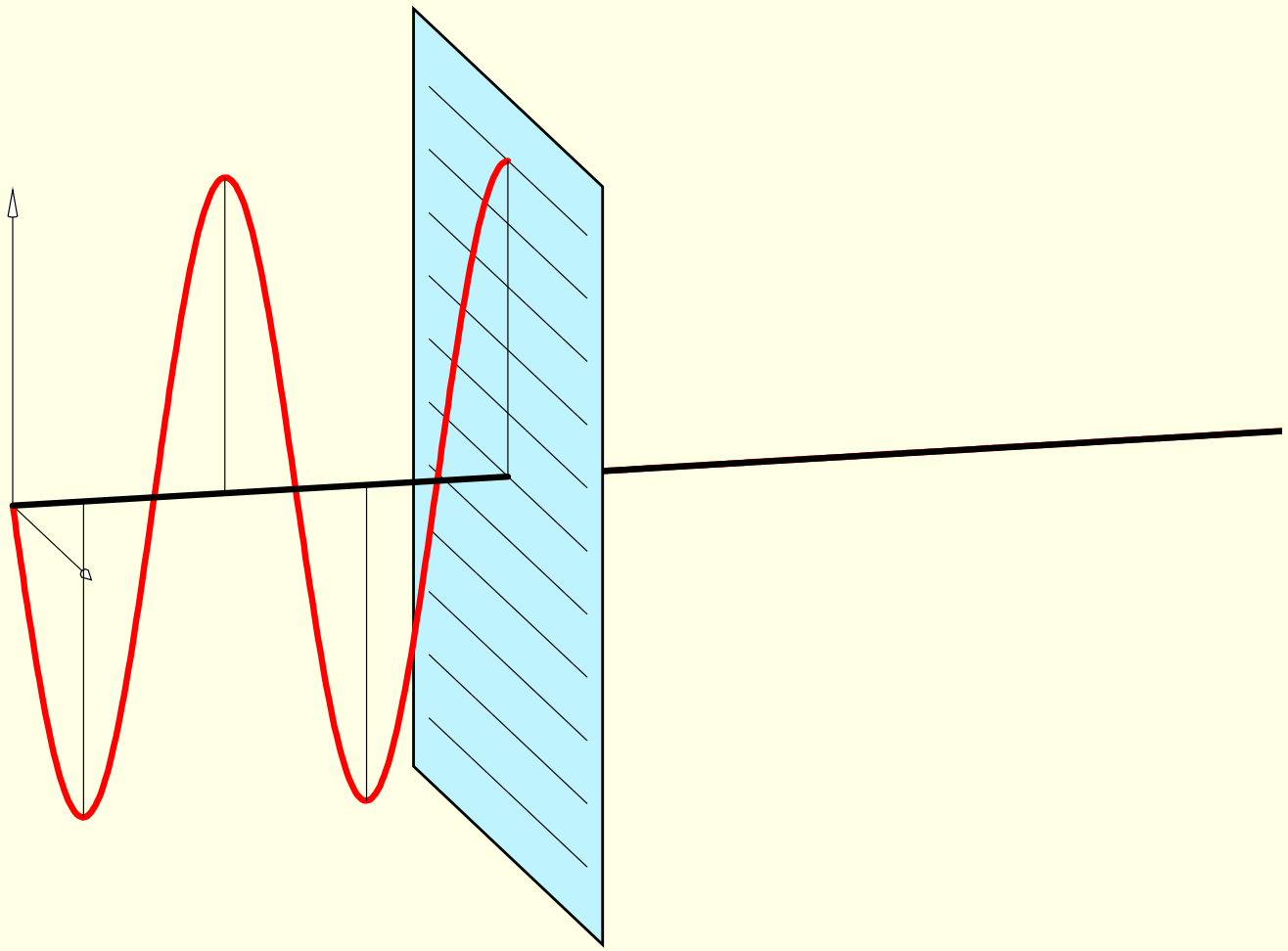
$$3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609$$

Nagroda 20000 $

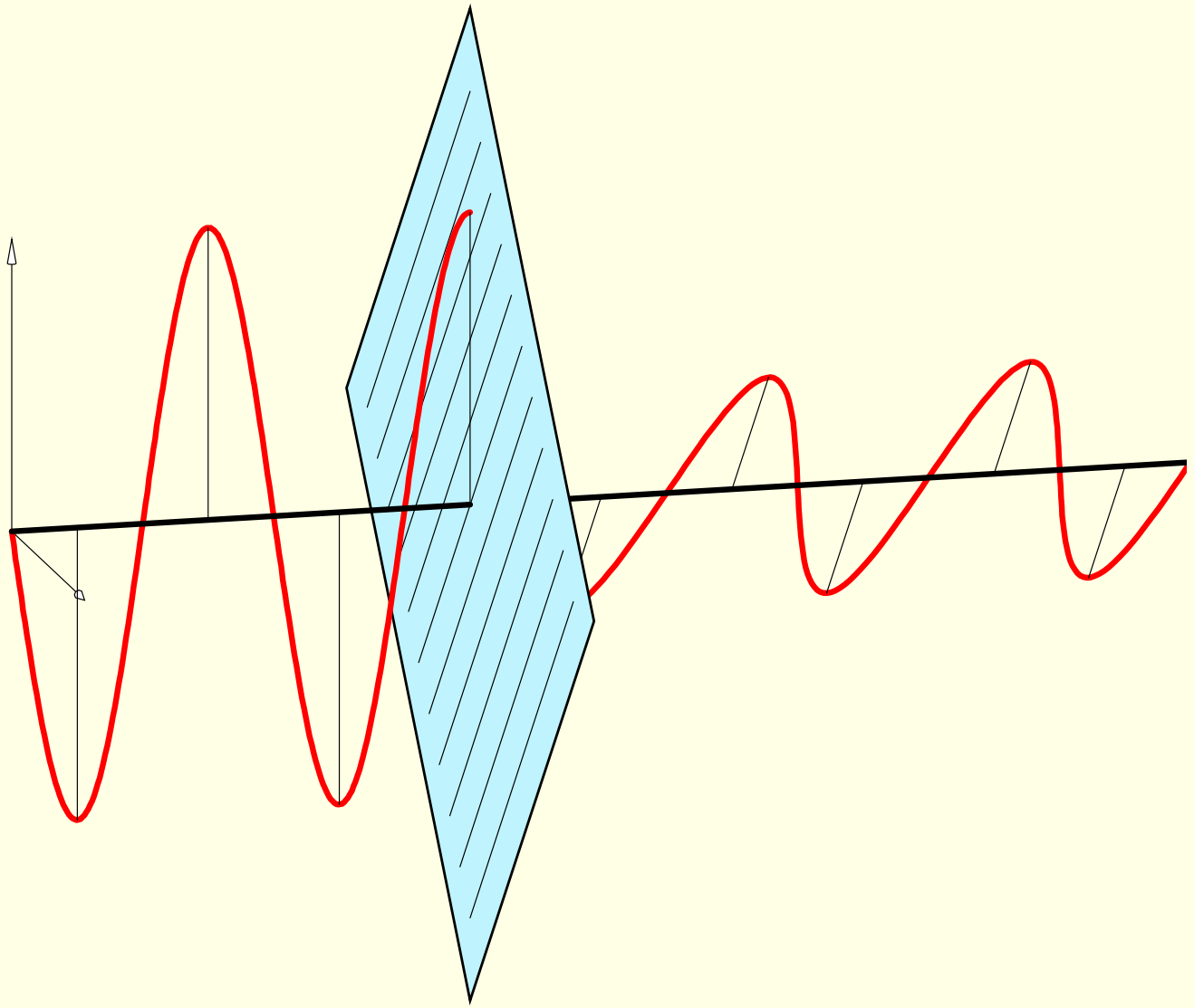
5 Fotony i ich polaryzacja



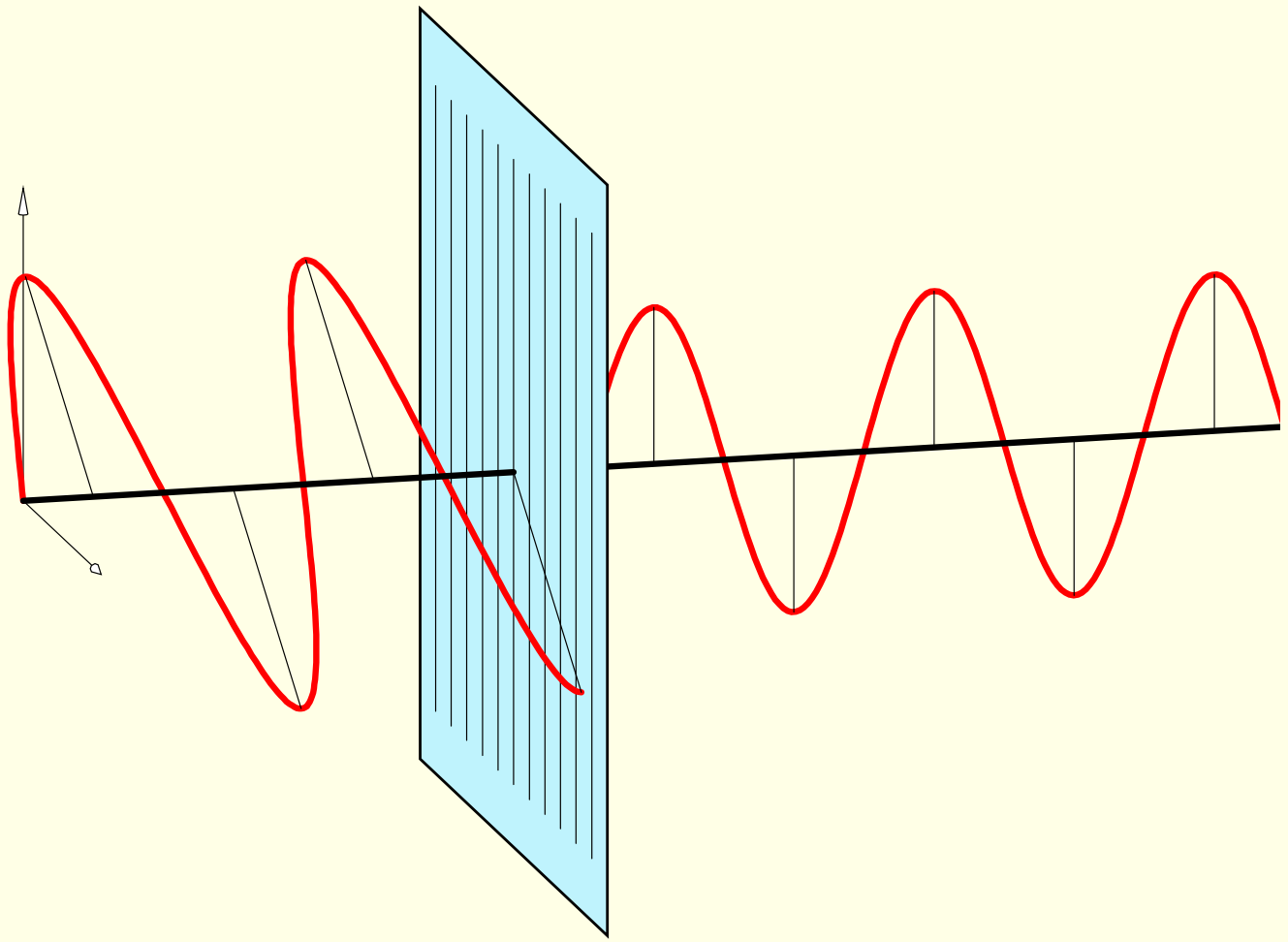
Polaryzator ustawiony pionowo przepuszcza światło spolaryzowane pionowo.



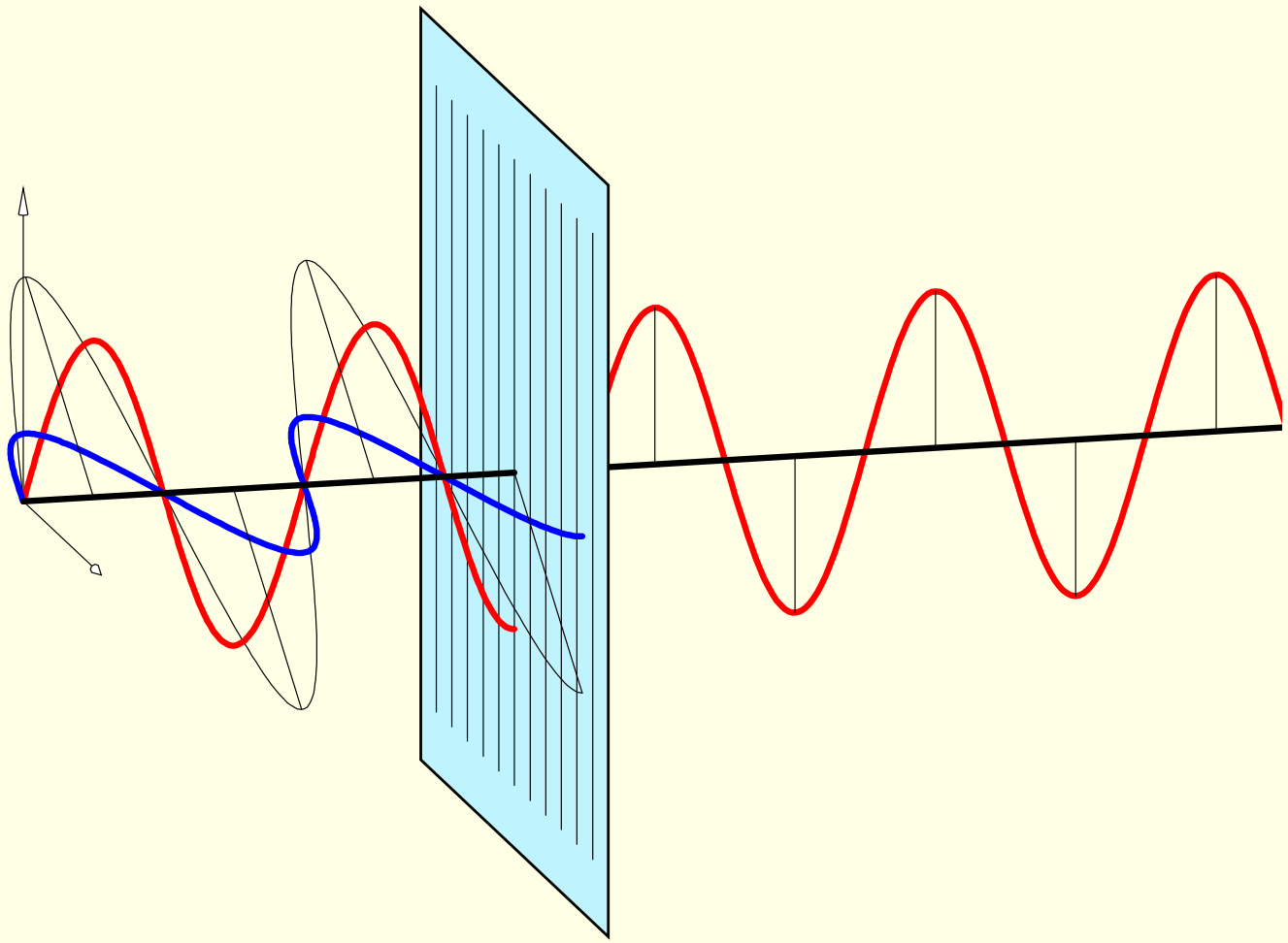
Polaryzator ustawiony poziomo zatrzymuje światło spolaryzowane pionowo.



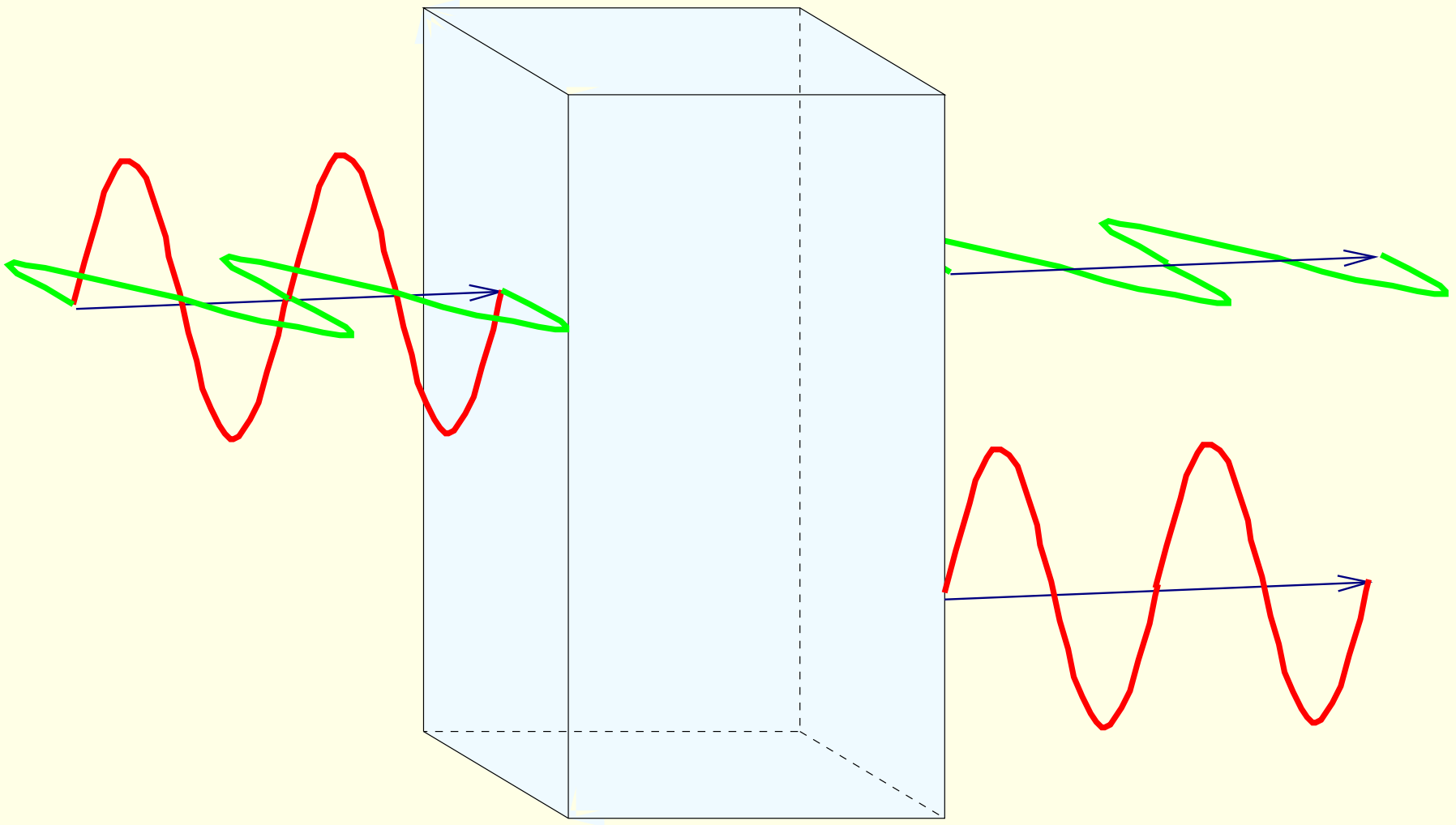
Polaryzator ustawiony ukośnie przepuszcza światło spolaryzowane ukośnie. Skąd się wzięło światło spolaryzowane ukośnie?



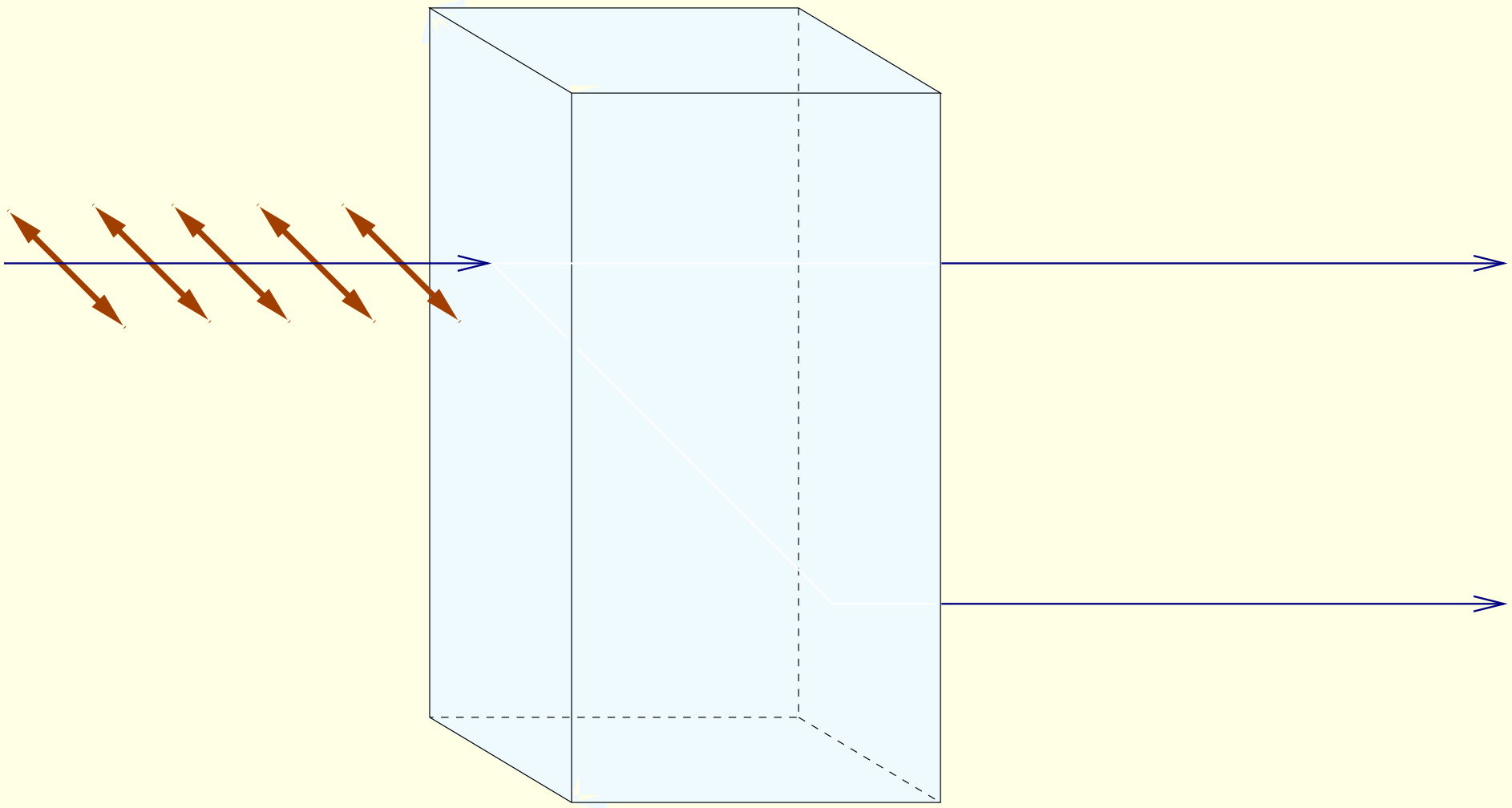
Pada światło spolaryzowane ukośnie, polaryzator ustawiony pionowo przepuszcza światło spolaryzowane pionowo.



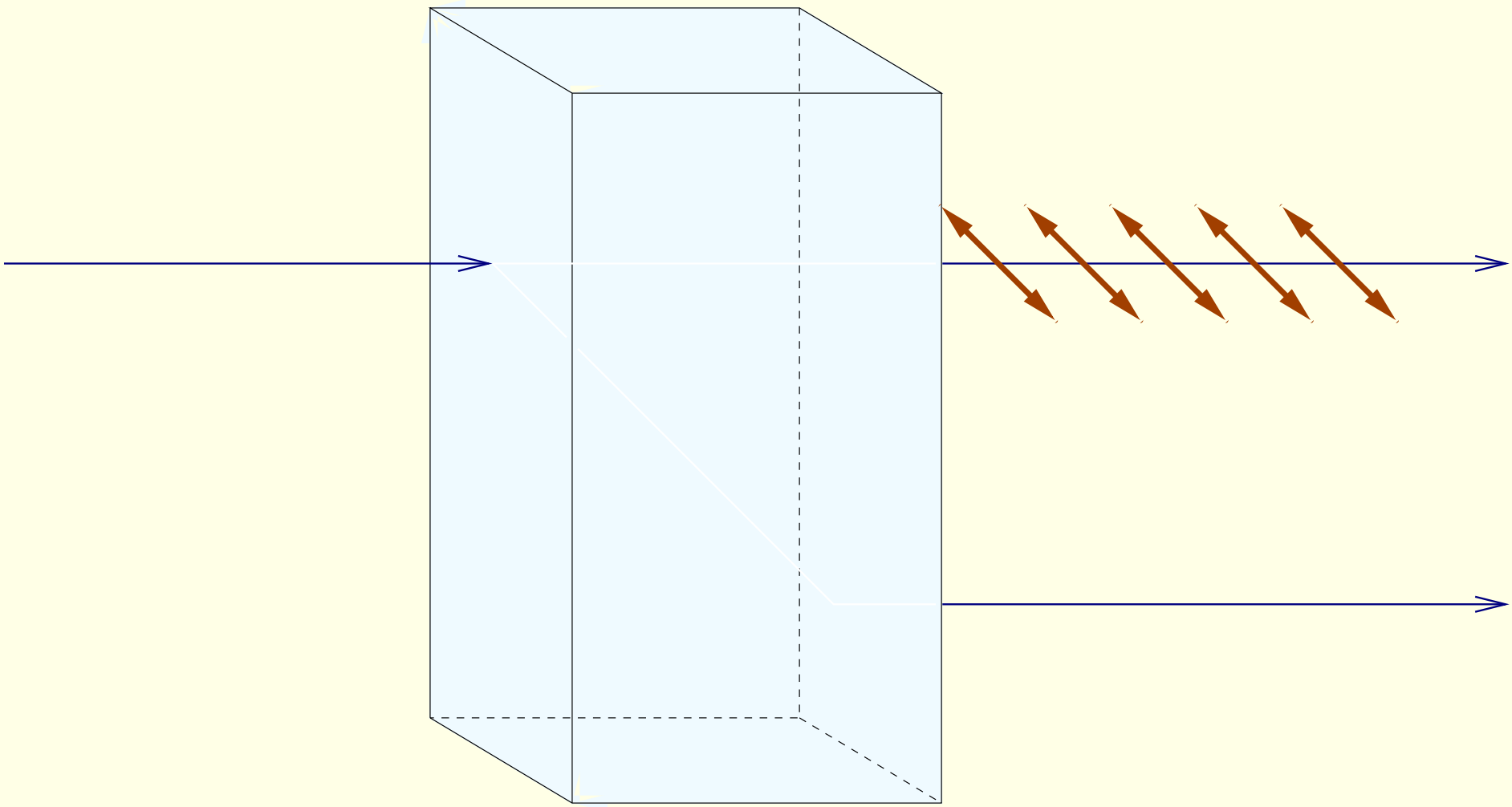
Polaryzacja ukośna jest superpozycją polaryzacji pionowej i poziomej. Polaryzator przepuszcza tylko składową pionową!



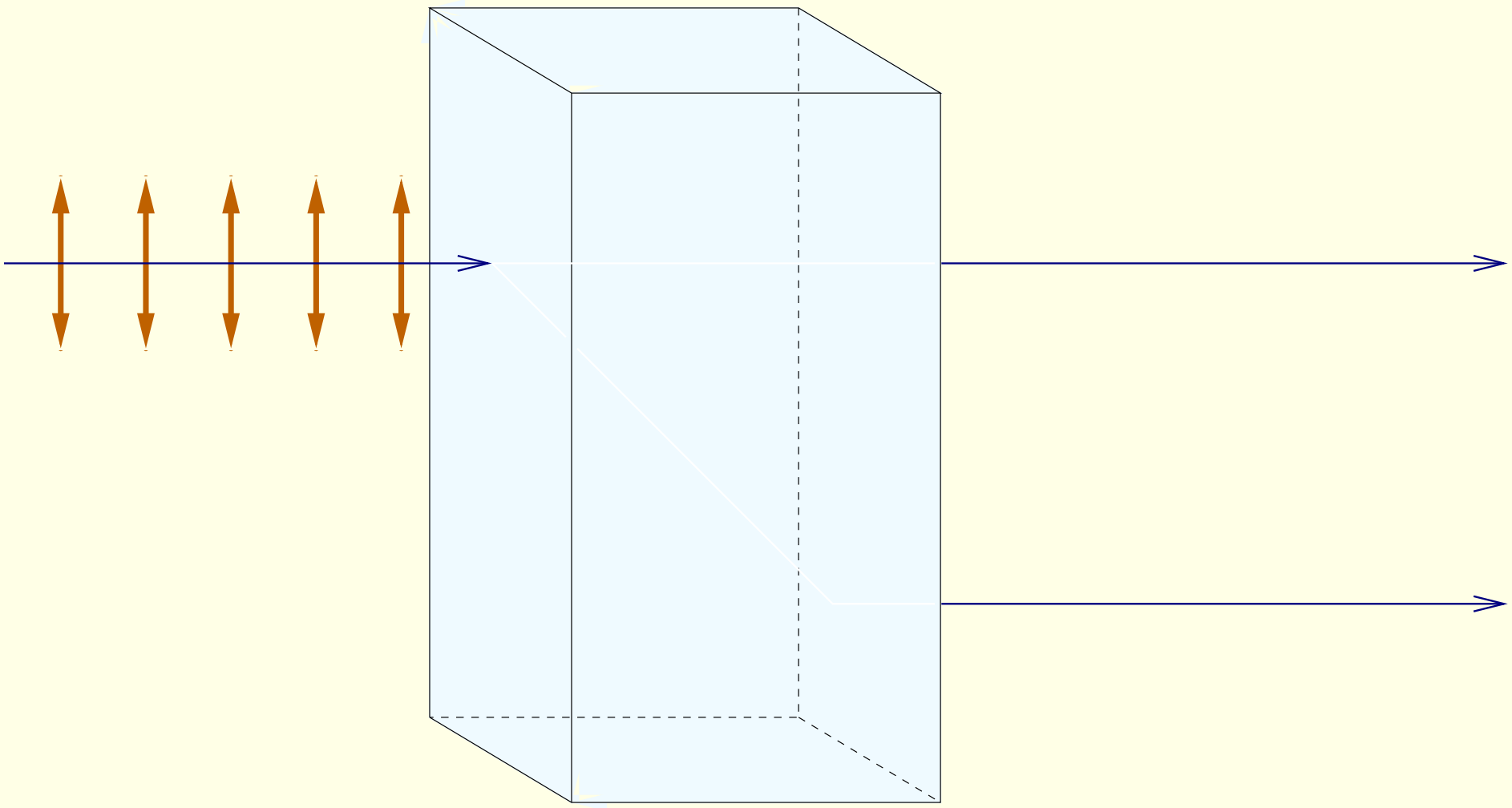
Dwójłomny kryształ kalcytu rozdziela falę świetlną na dwie składowe o wzajemnie prostopadłych polaryzacjach (promień zwyczajny i nadzwyczajny).



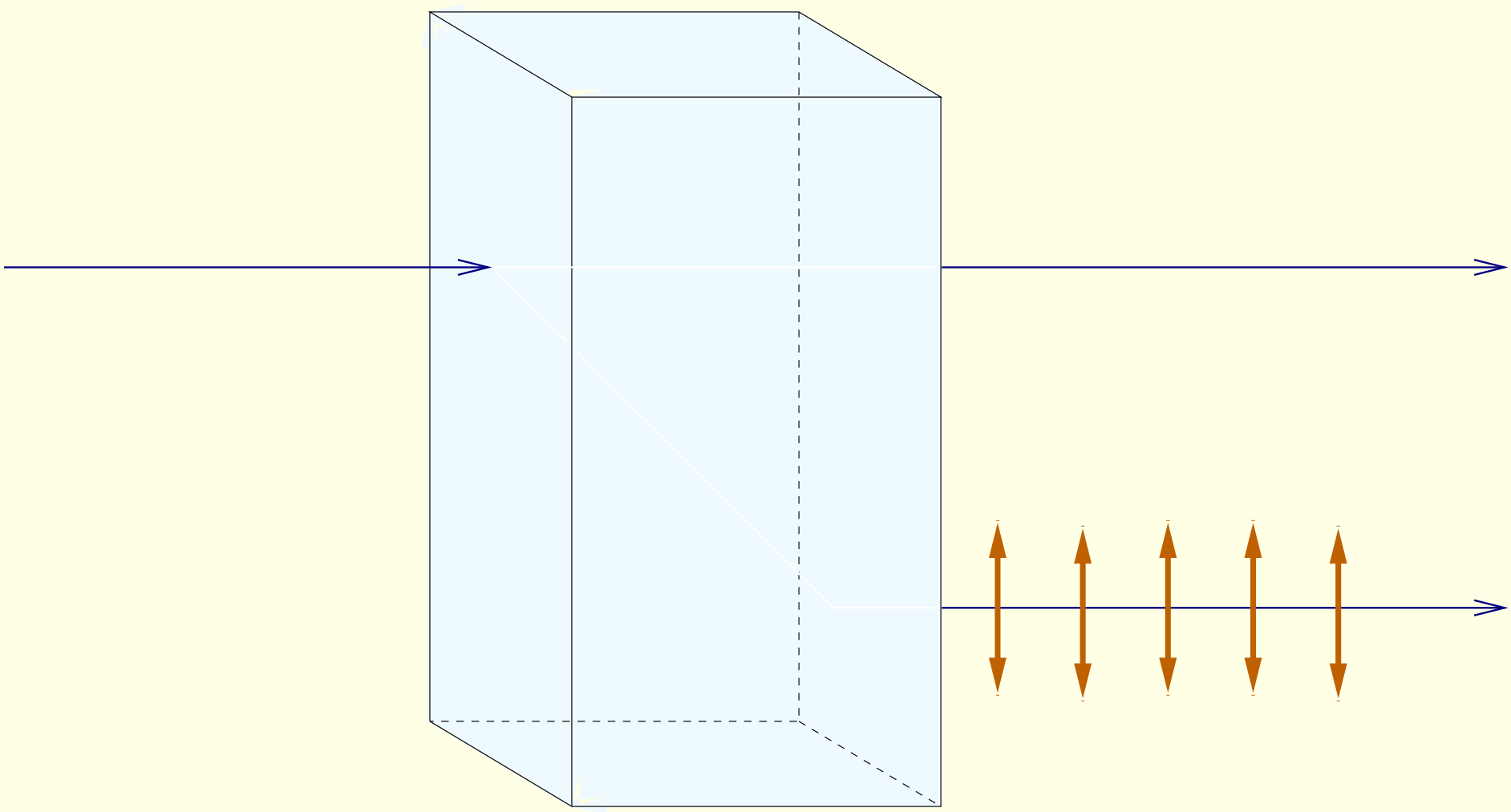
Poziomo spolaryzowane fotony padające na kryształ kalcytu ...



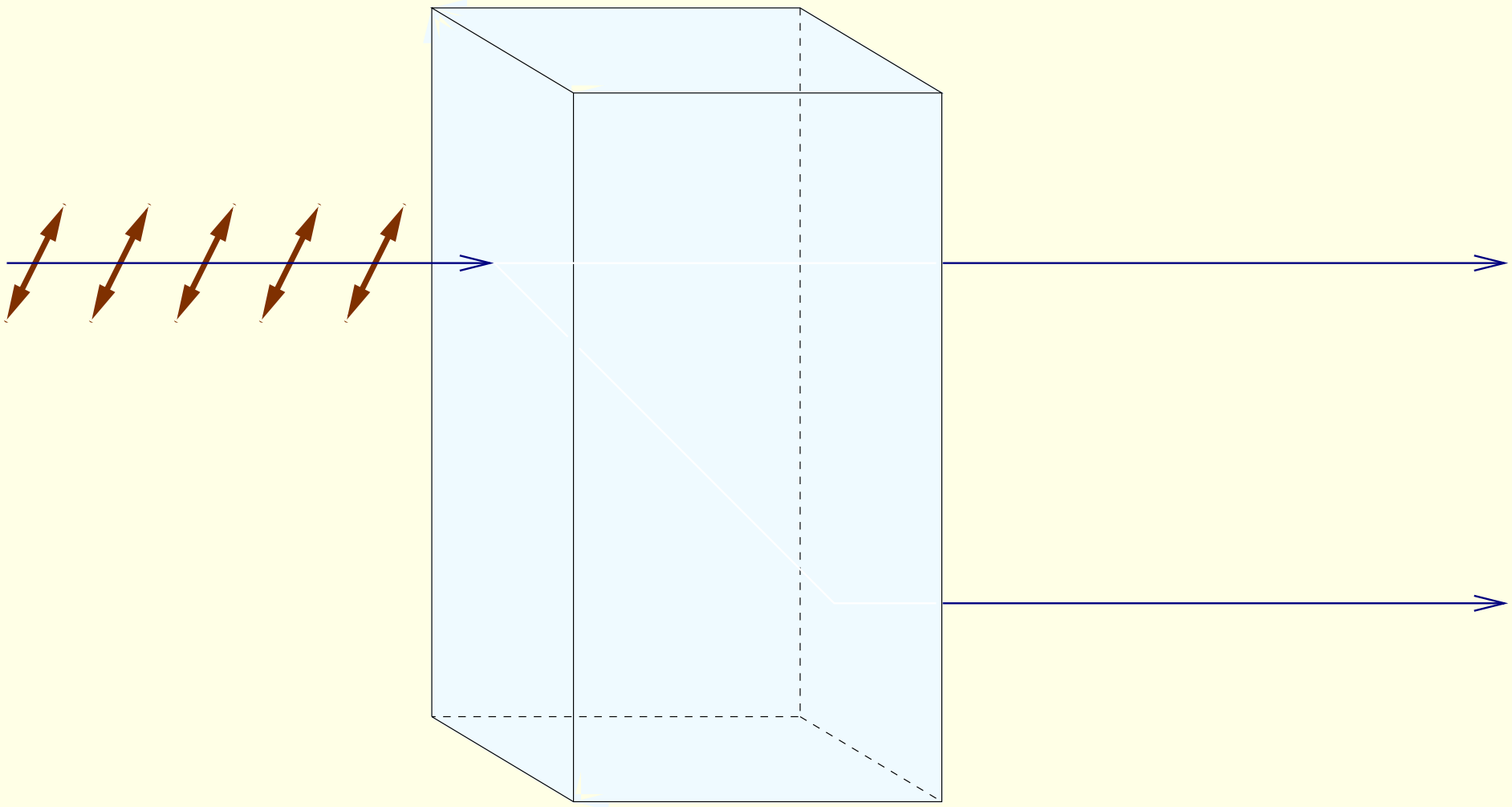
... przechodzą przez kryształ kalcytu bez zmiany kierunku propagacji tworząc promień zwyczajny.



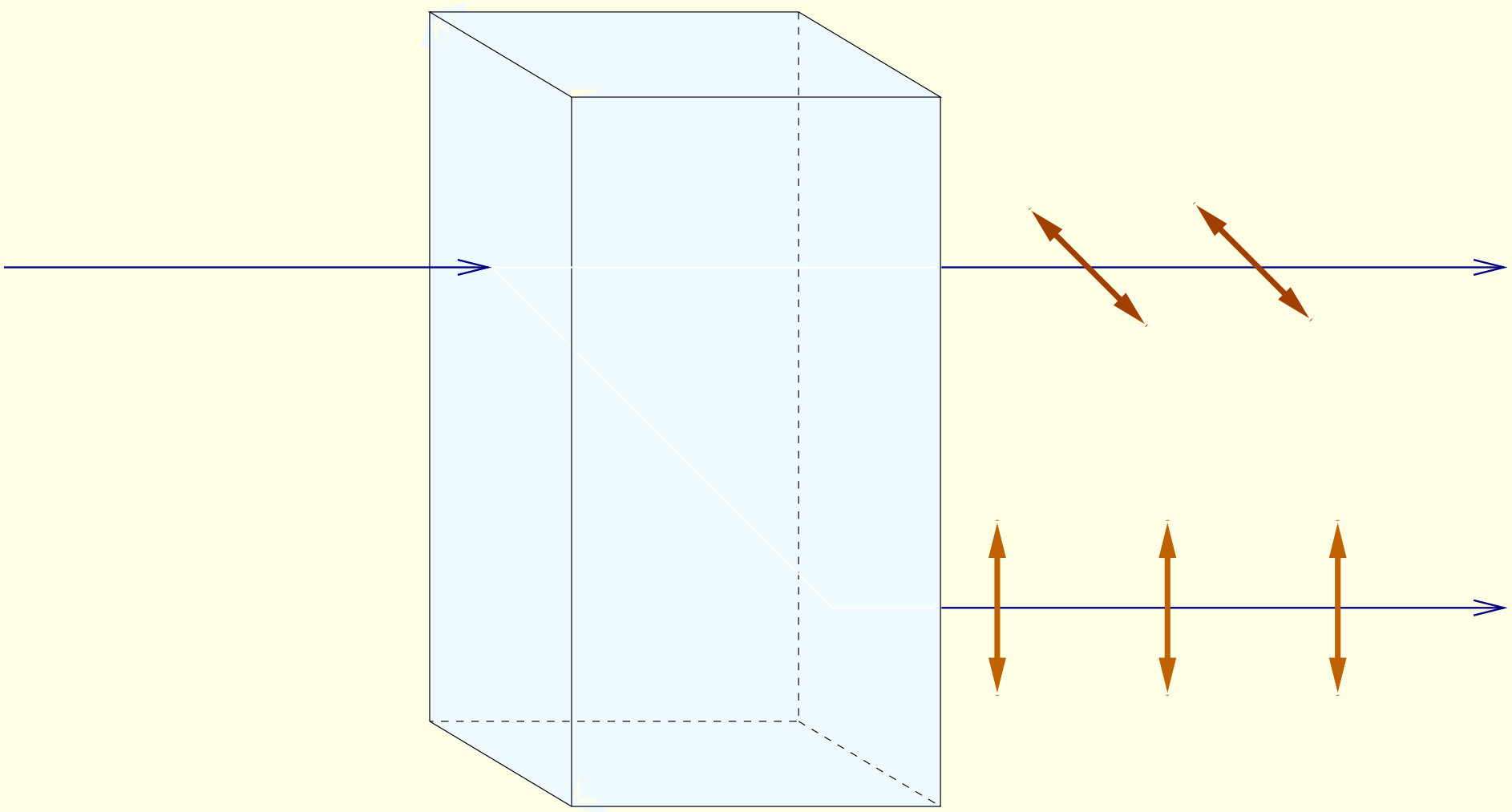
Pionowo spolaryzowane fotony padające na kryształ kalcytu ...



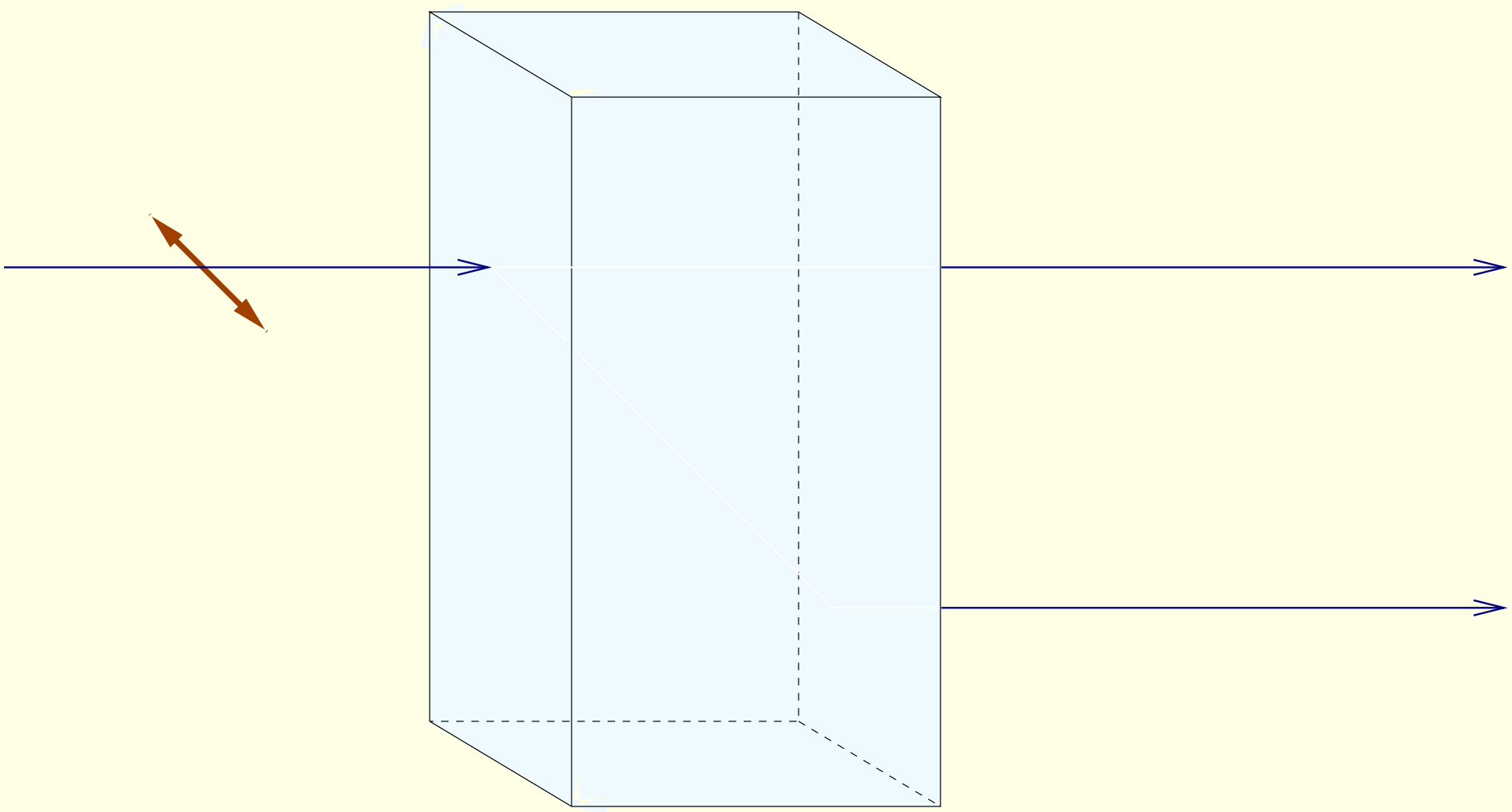
... zostają odchylone tworząc promień nadzwyczajny.



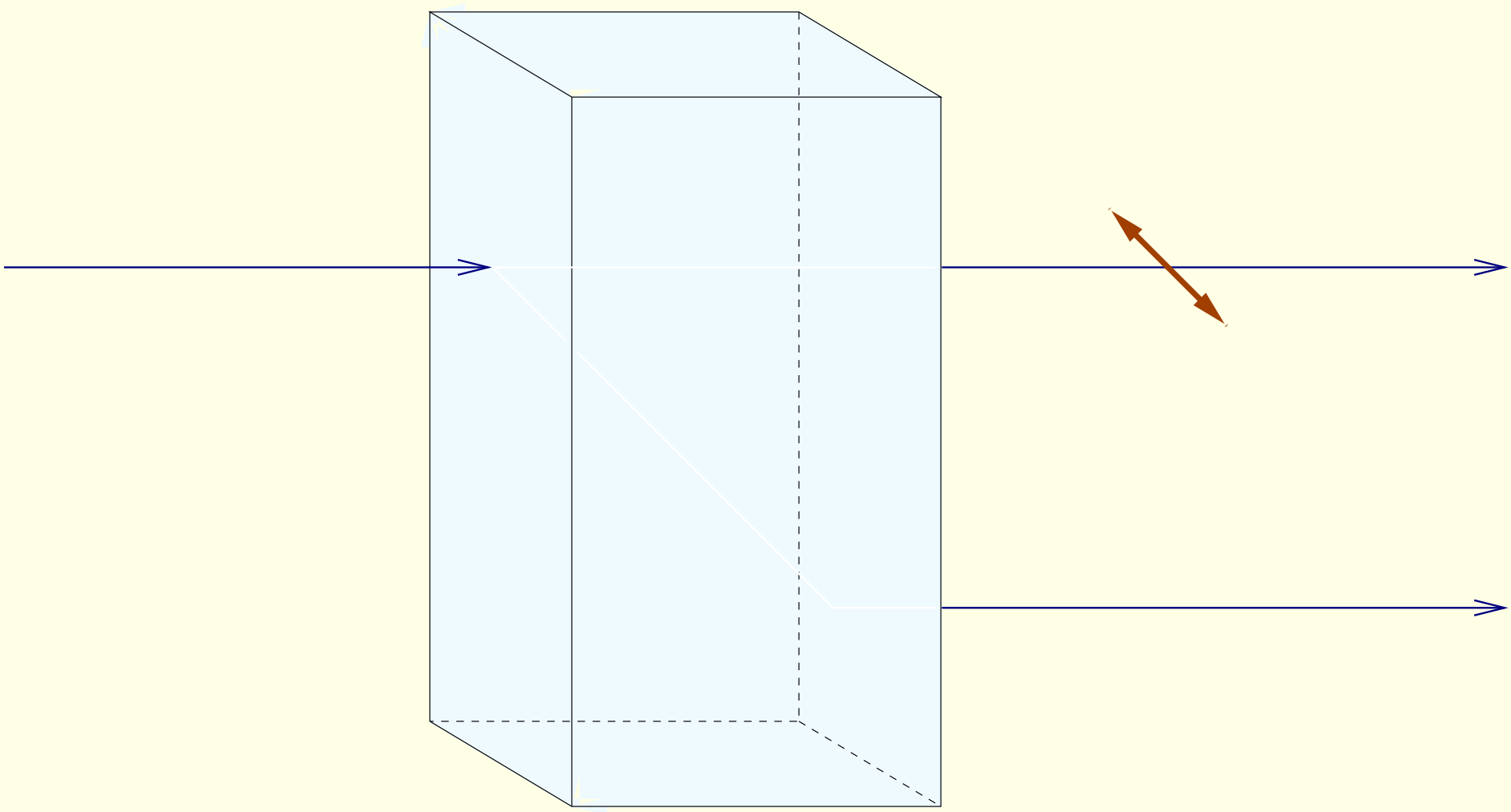
Fotony spolaryzowane ukośnie padające na kryształ kalcytu ...



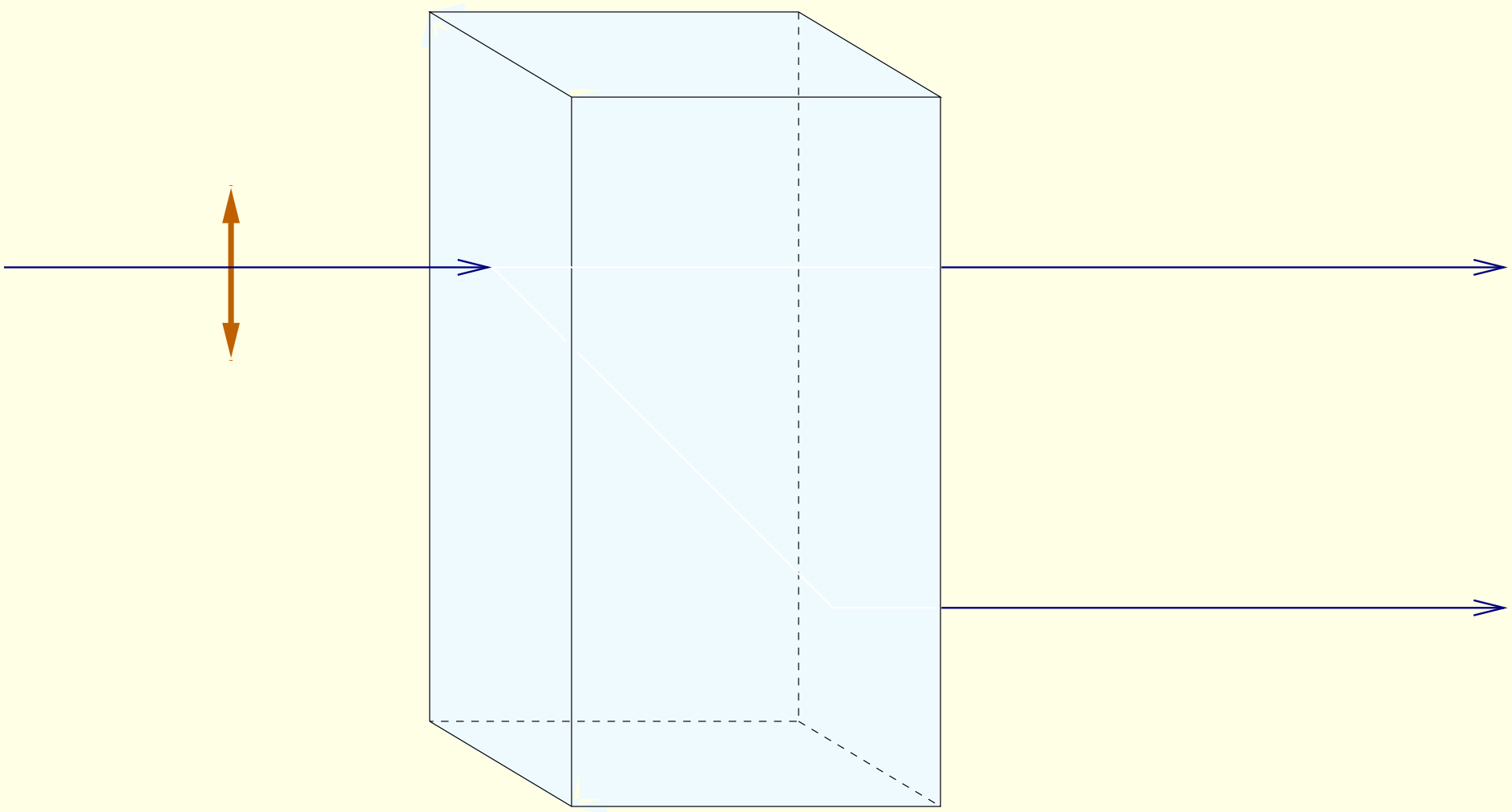
...otrzymują losowo polaryzację poziomą lub pionową i odpowiedni kierunek propagacji.



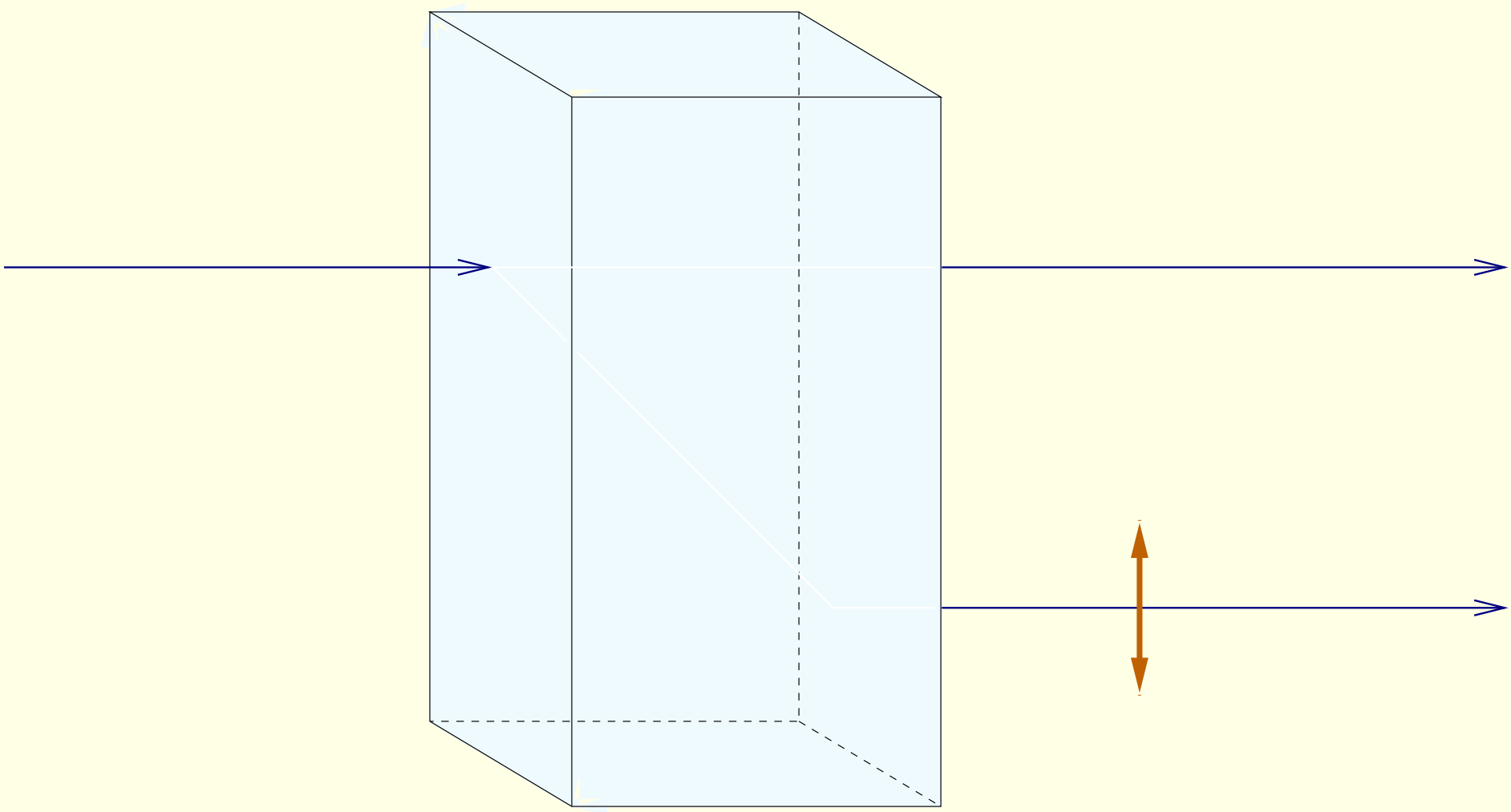
Pojedynczy foton o polaryzacji poziomej ...



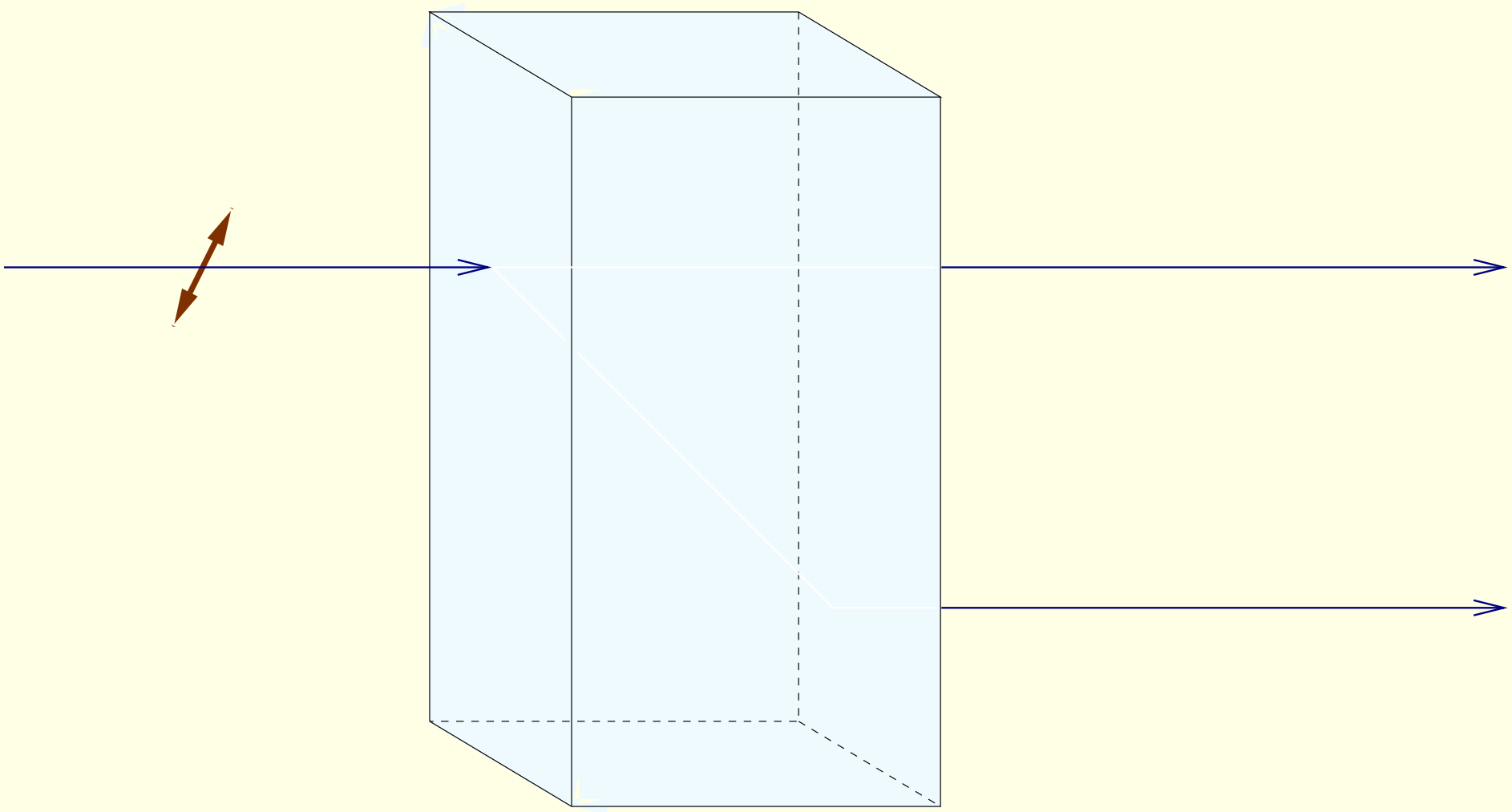
... przechodzi bez zmiany kierunku zachowując polaryzację poziomą.



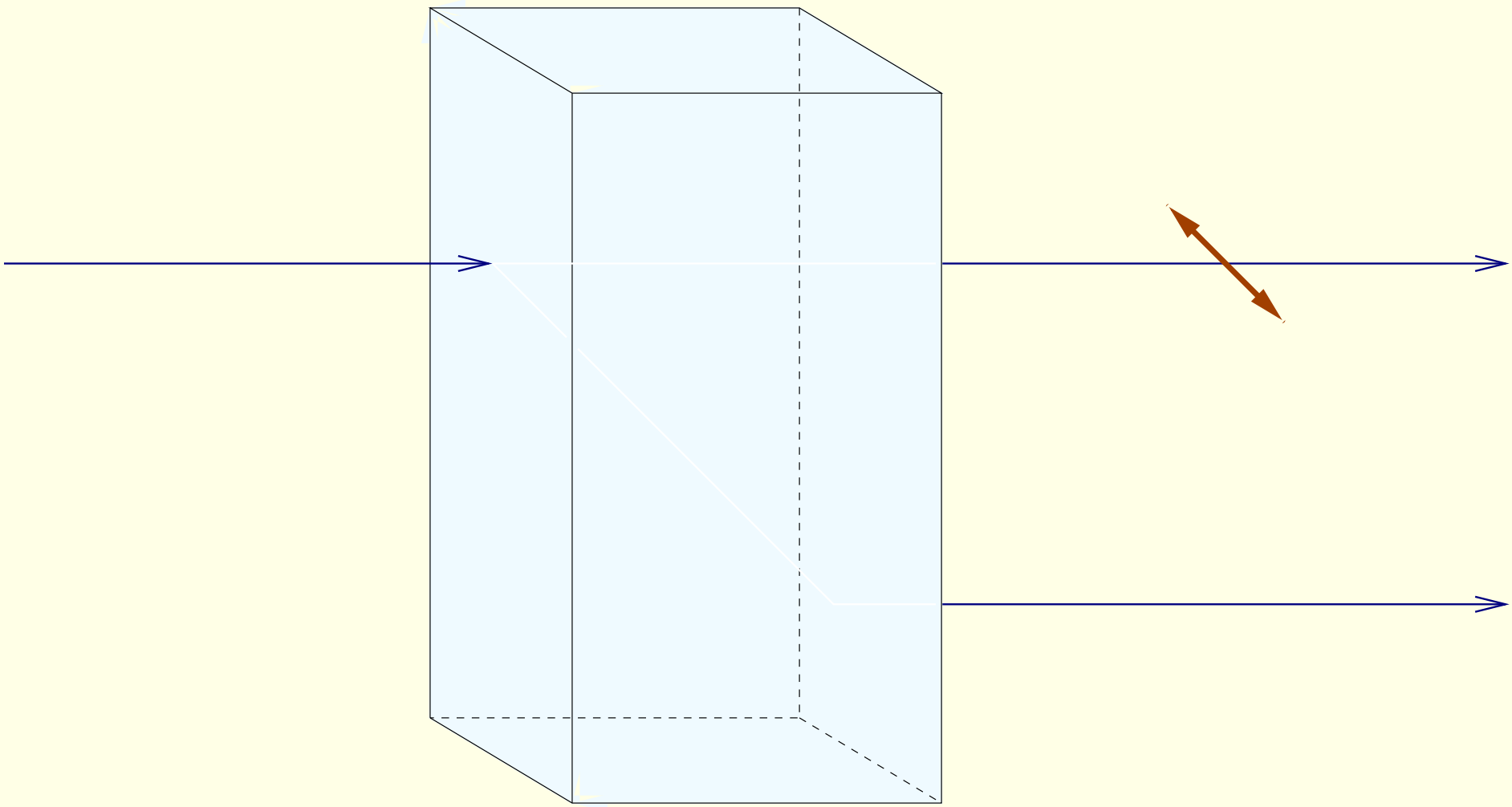
Pojedynczy foton o polaryzacji pionowej ...



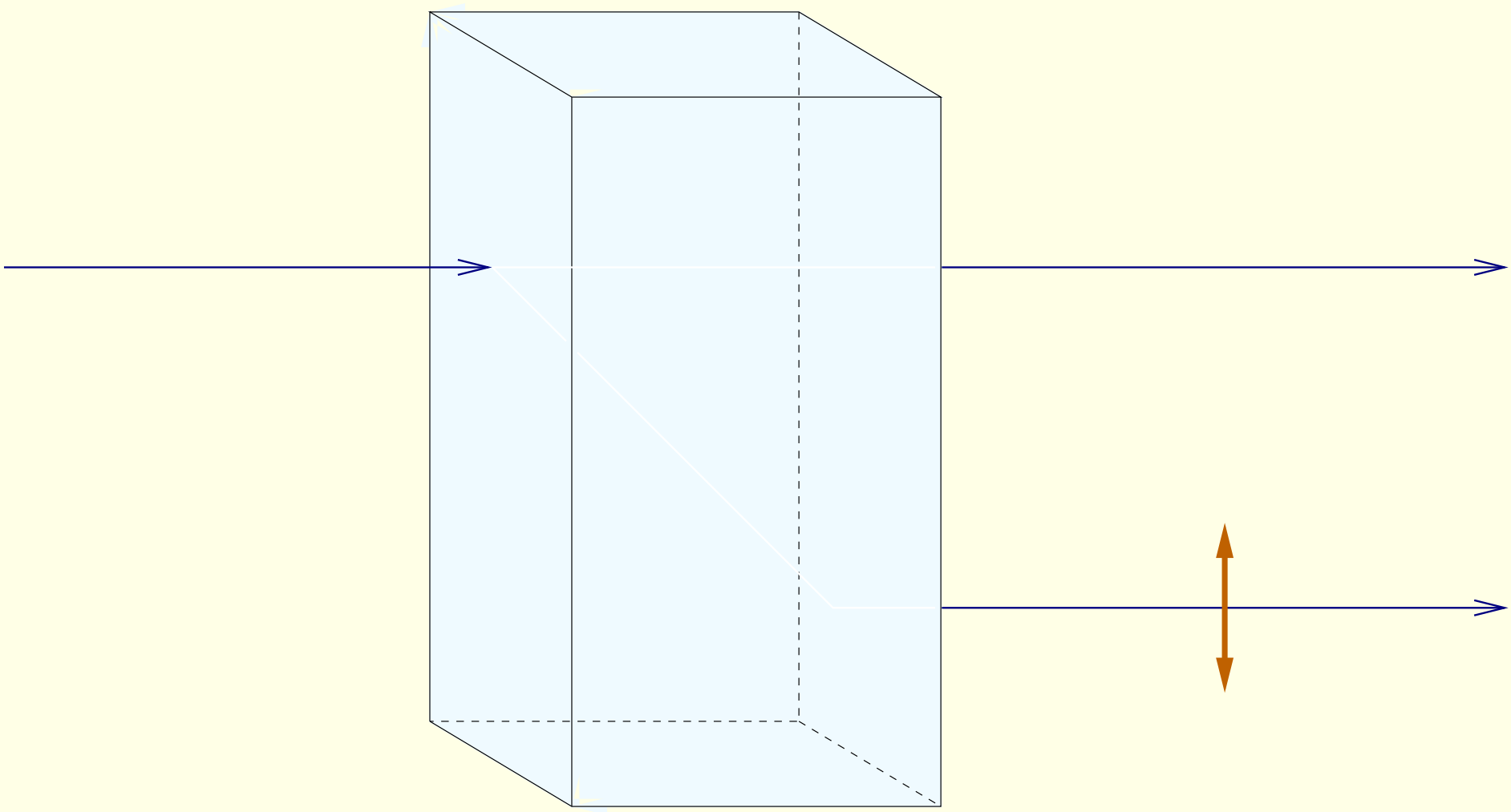
... zmienia kierunek propagacji zachowując polaryzację pionową.



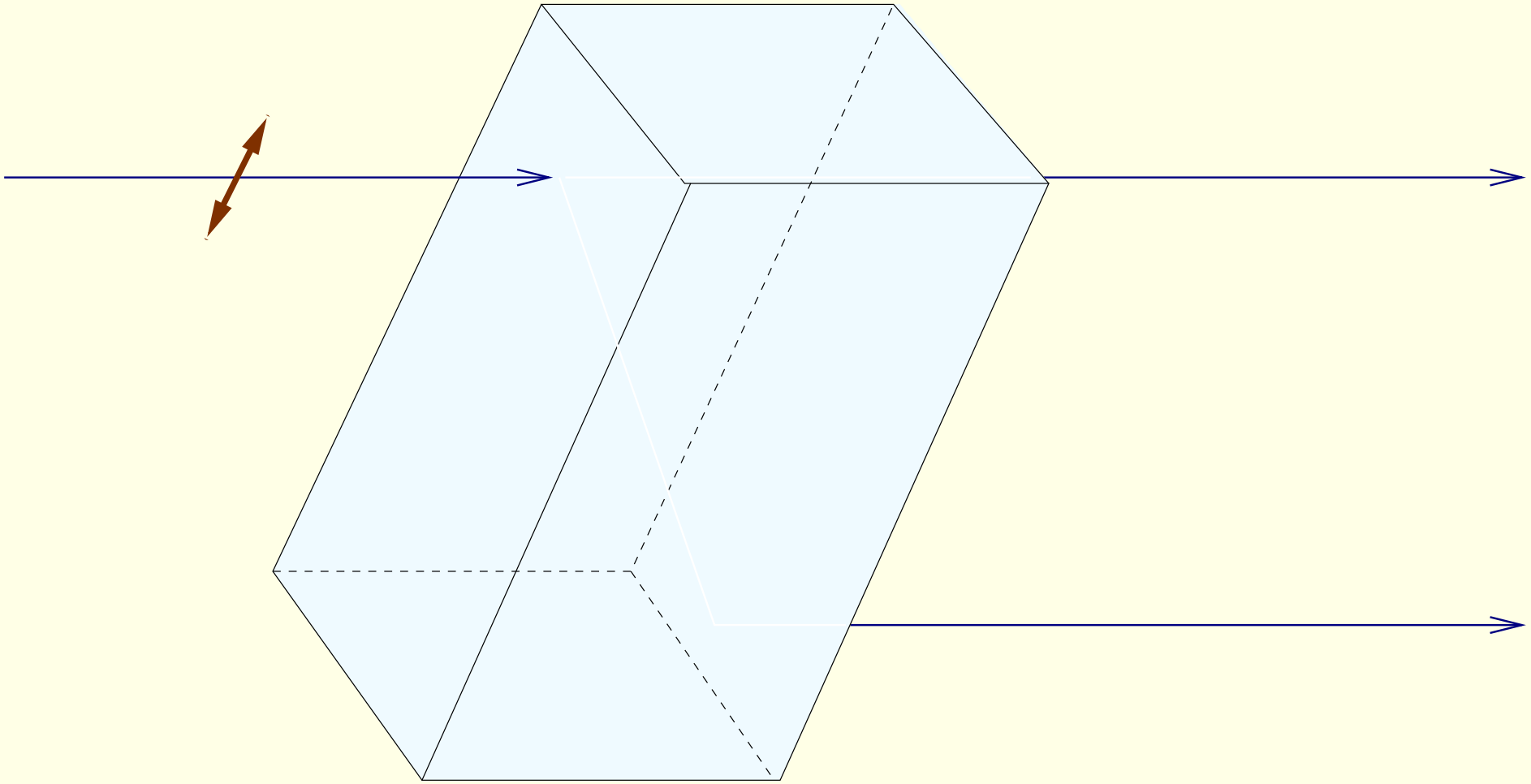
A co z pojedynczym fotonem o polaryzacji ukośnej w stosunku do osi kryształu?



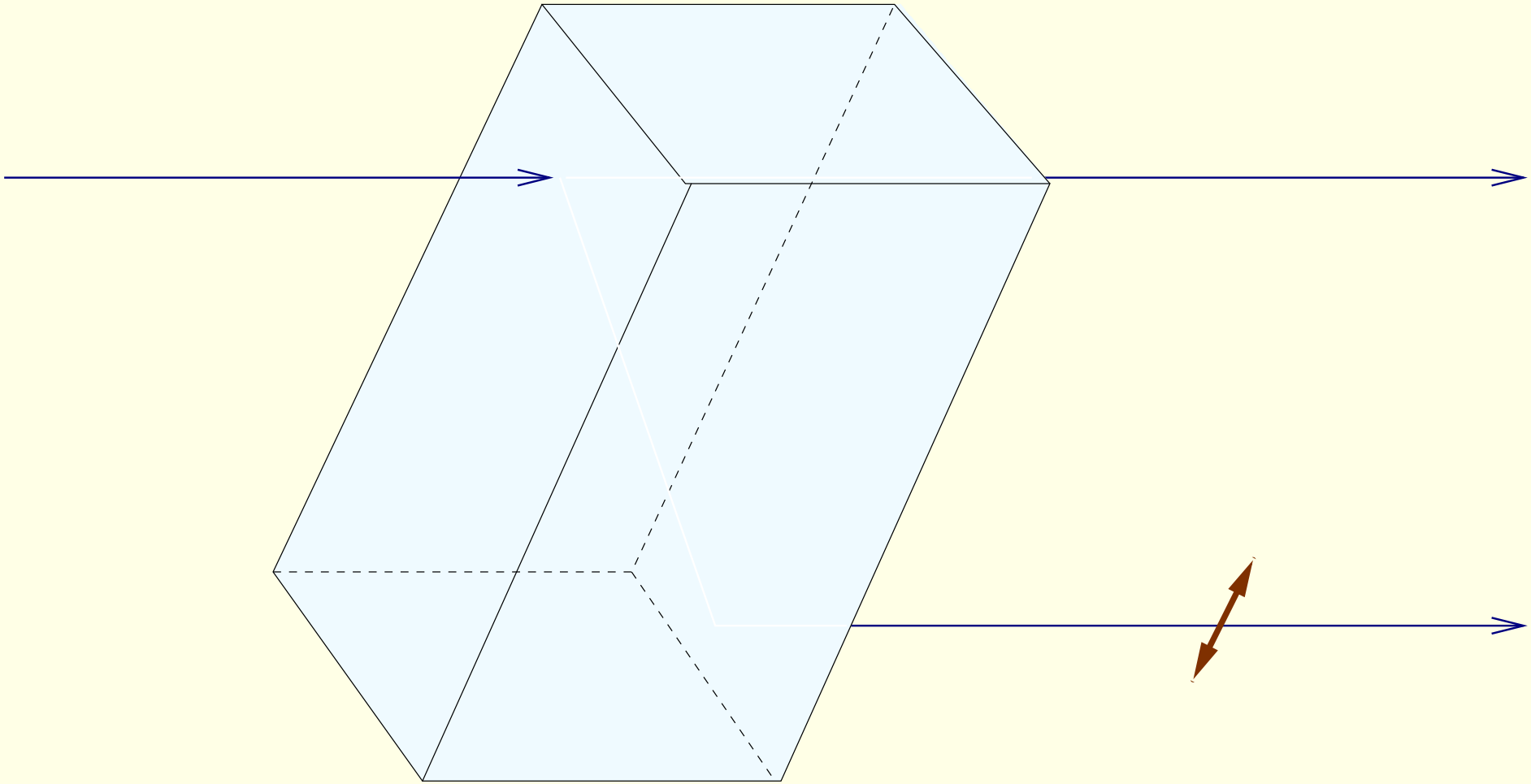
Foton o polaryzacji ukośnej znajdzie się z prawdopodobieństwem 1/2 w wiązce zwyczajnej z polaryzacją poziomą albo ...



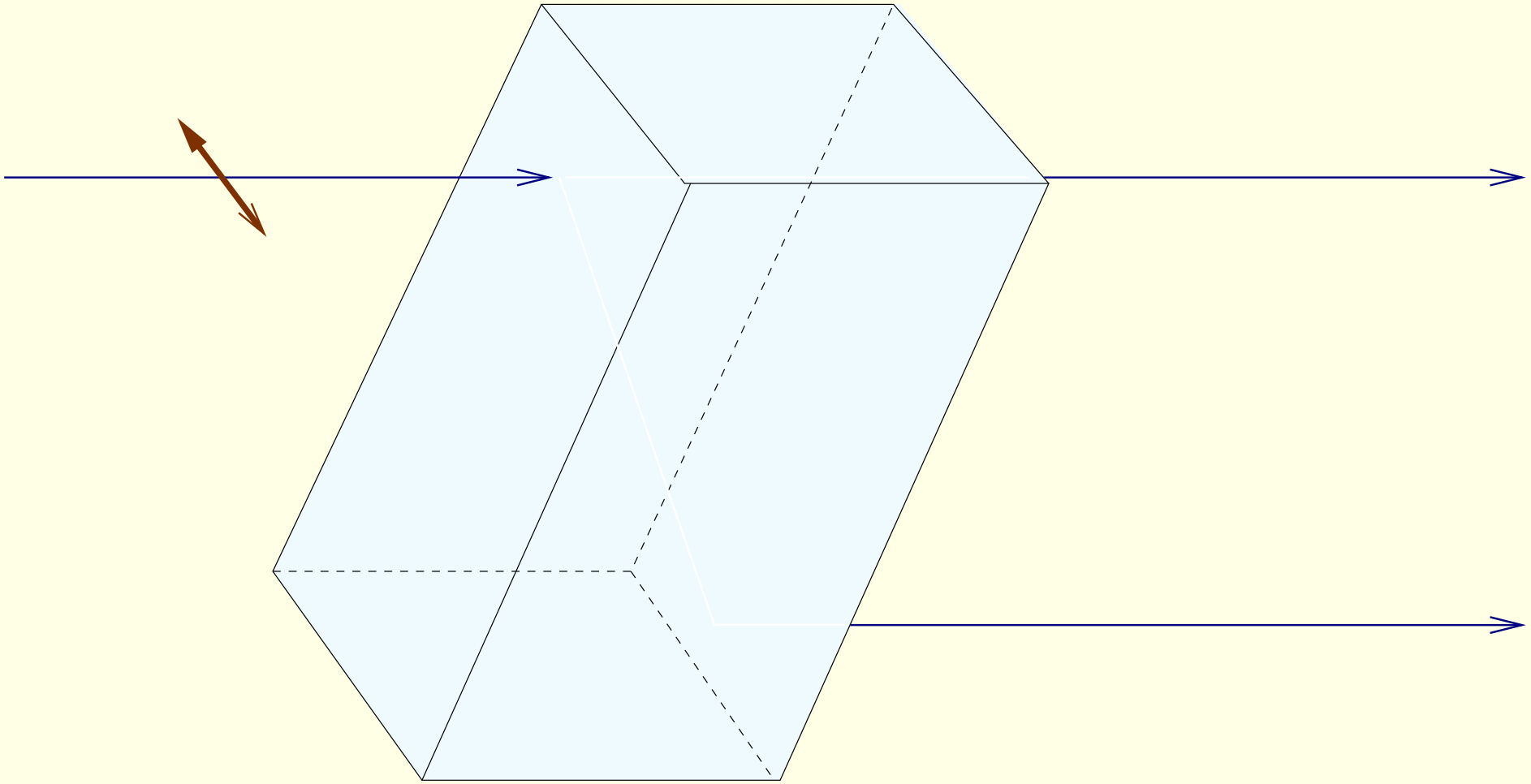
... z prawdopodobieństwem $1/2$ w wiązce nadzwyczajnej z polaryzacją pionową. Obie te możliwości są jednakowo prawdopodobne: foton nie niesie już żadnej informacji o poprzedniej polaryzacji.



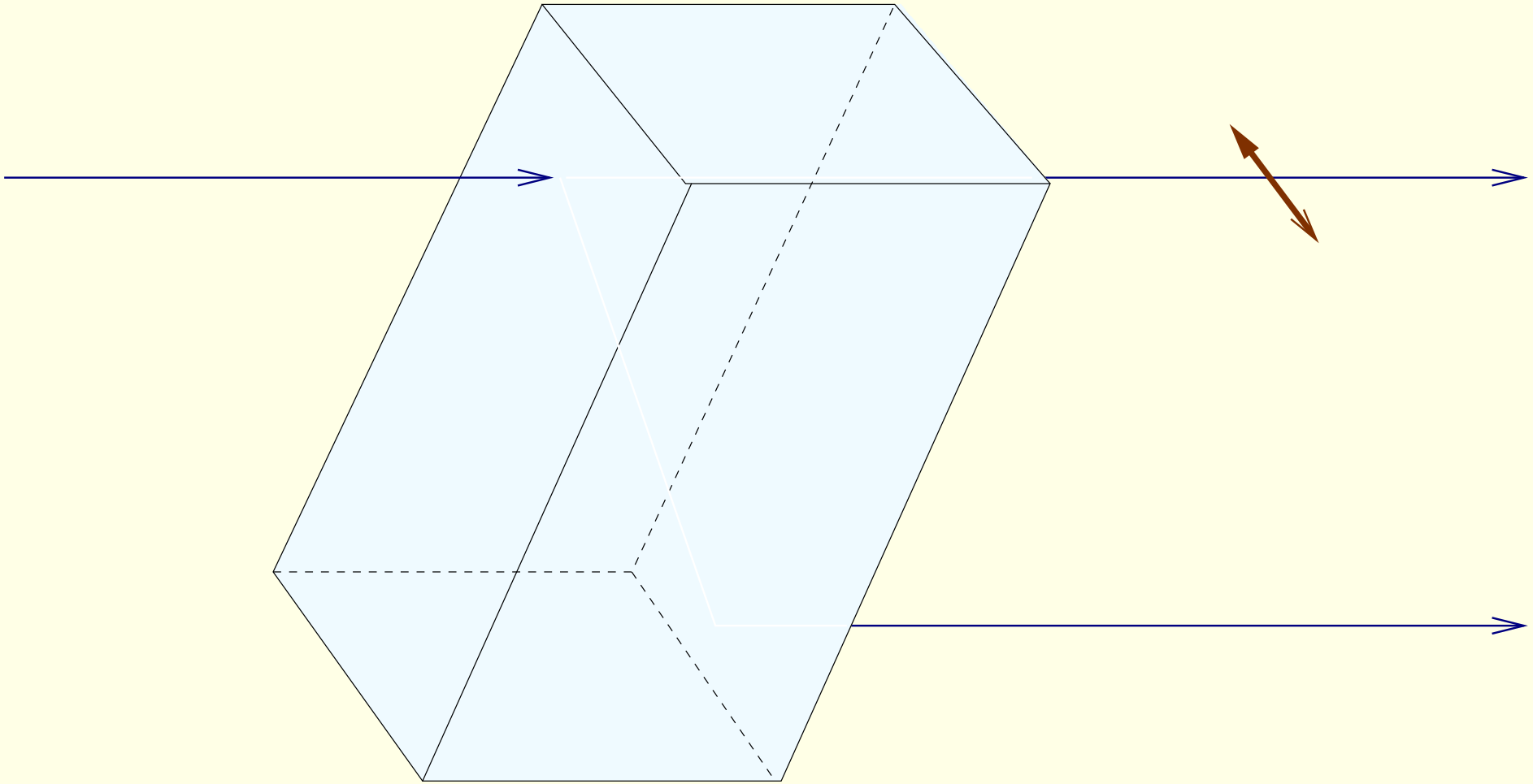
Jeśli obrócimy kryształ o -45° (135°), to foton ukośny -45° staje się fotonem pionowym w nowym układzie i ...



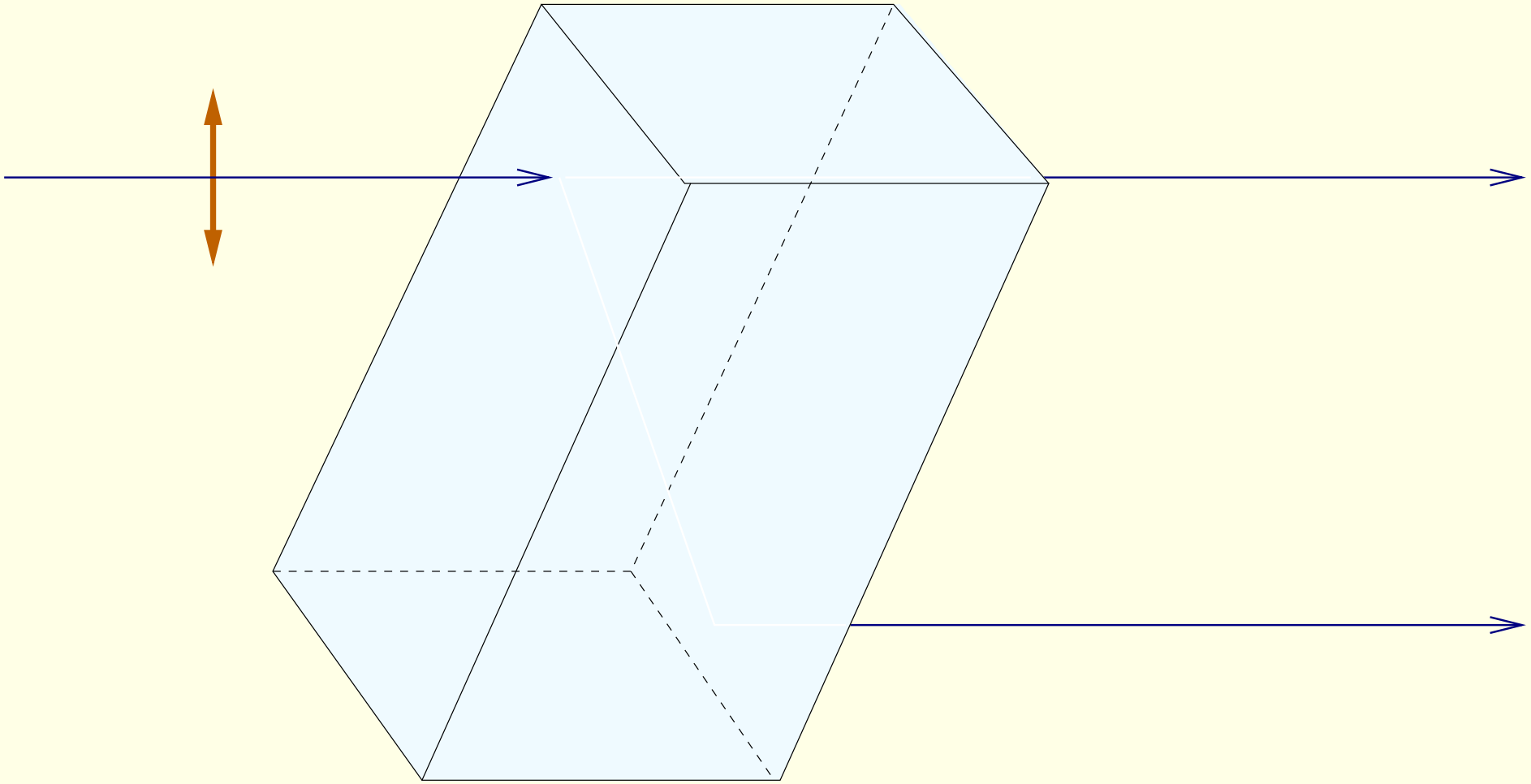
... przechodzi przez kryształ bez zmiany polaryzacji do wiązki nadzwyczajnej.



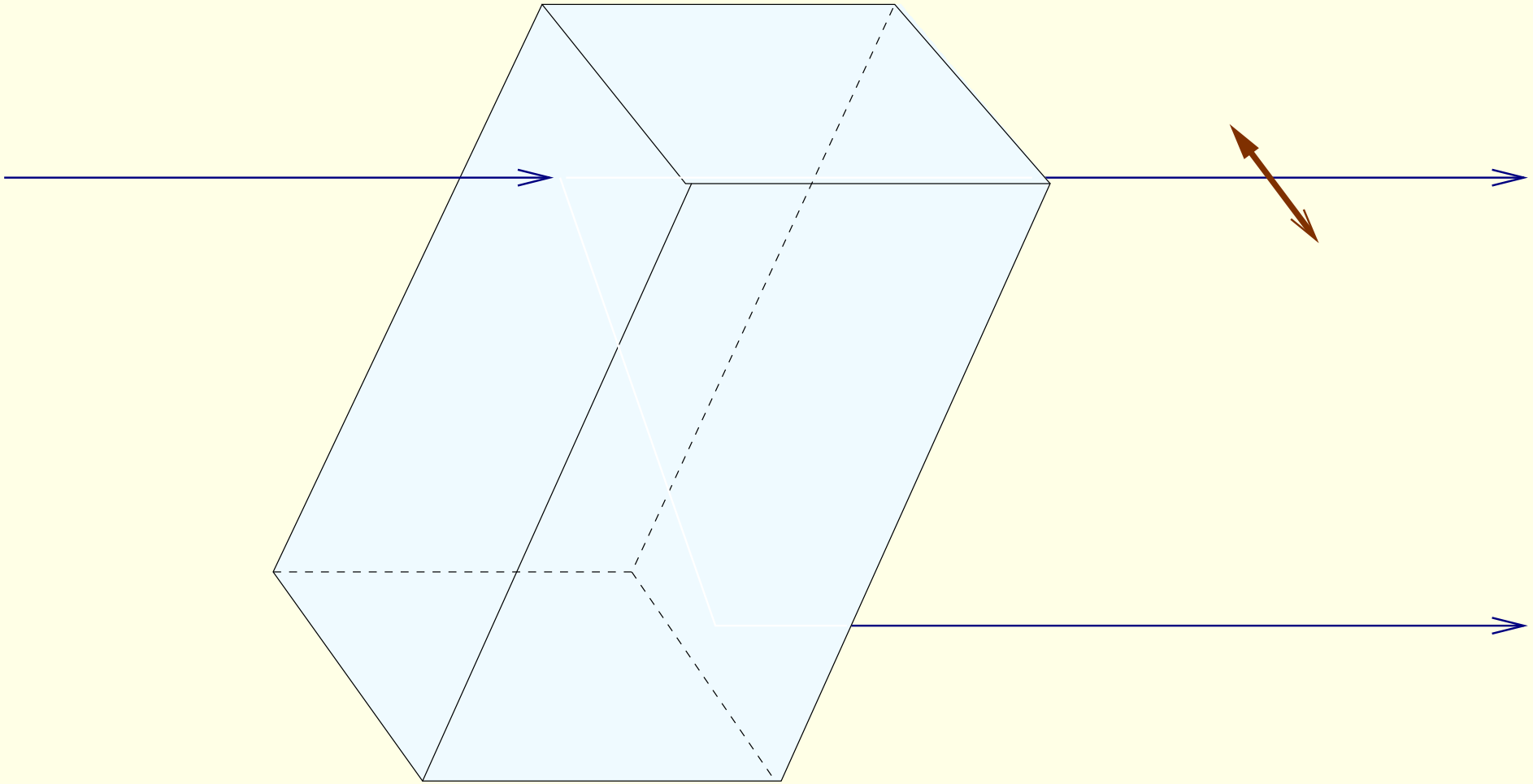
Prostopadły do kierunku -45° foton ukośny 45° staje się dla kryształu fotonem poziomym i ...



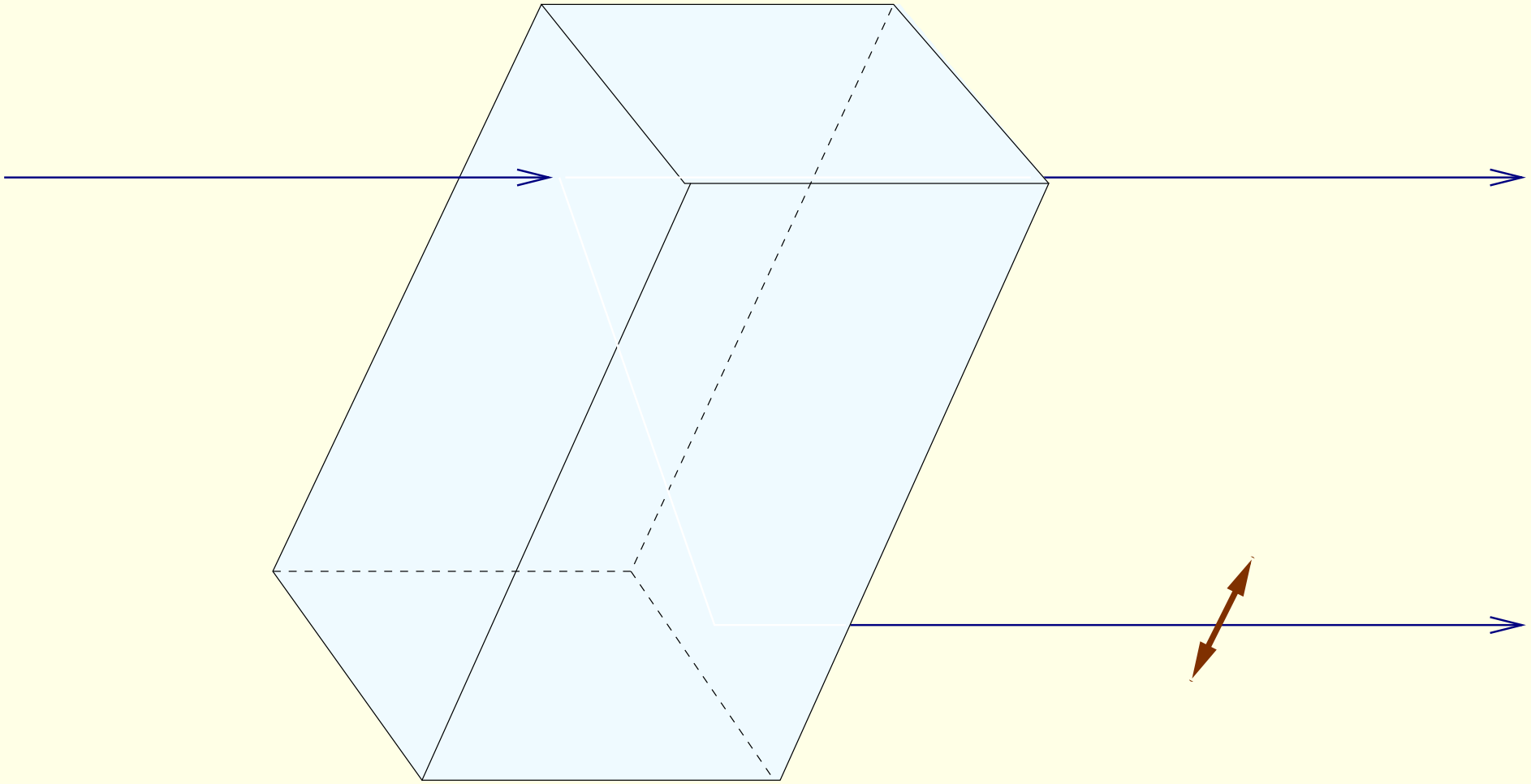
... przechodzi przez kryształ bez zmiany polaryzacji do wiązki zwyczajnej.



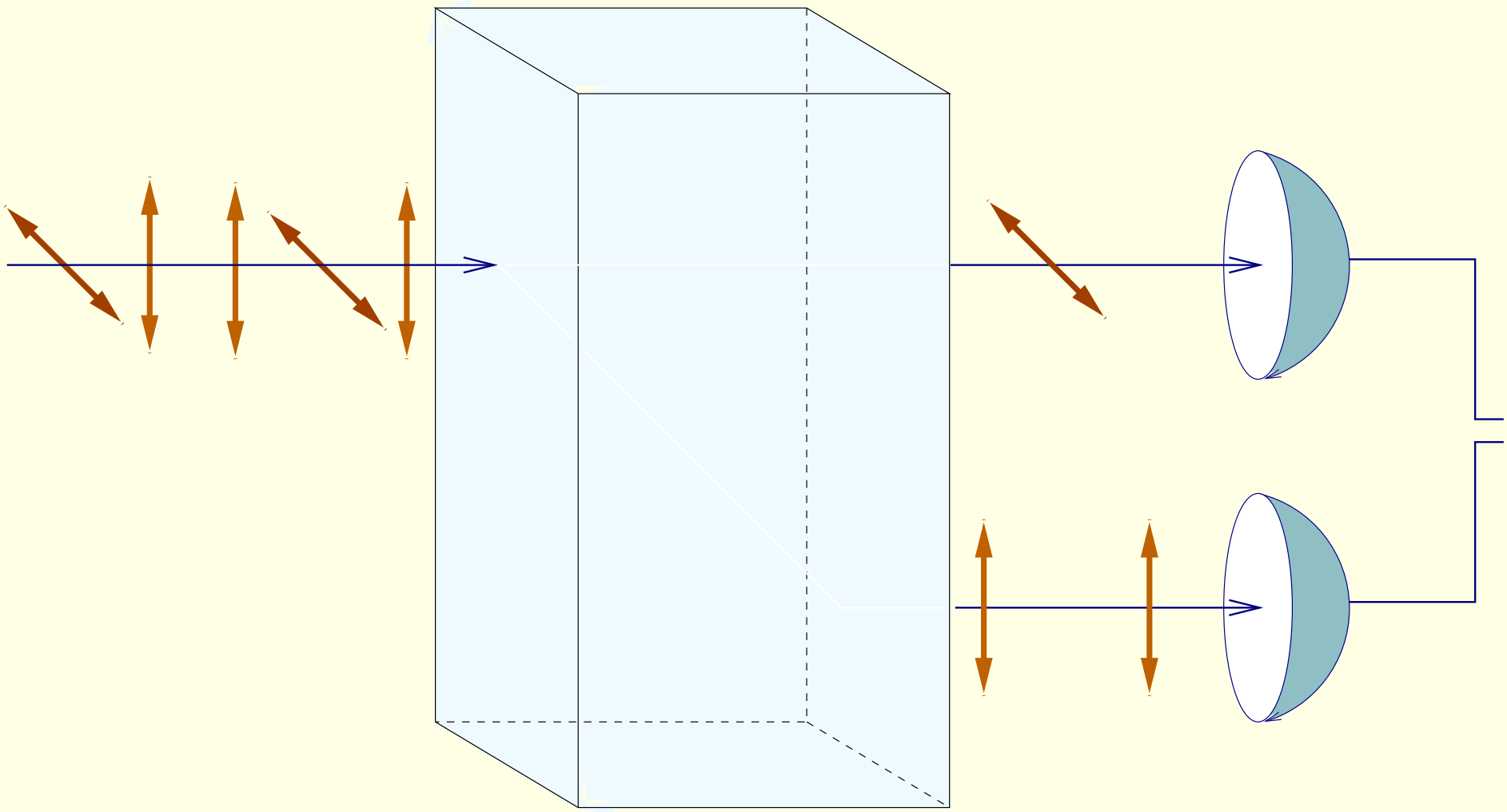
Foton o polaryzacji pionowej (poziomej) staje się ukośnym w stosunku do obróconego kryształu i ...



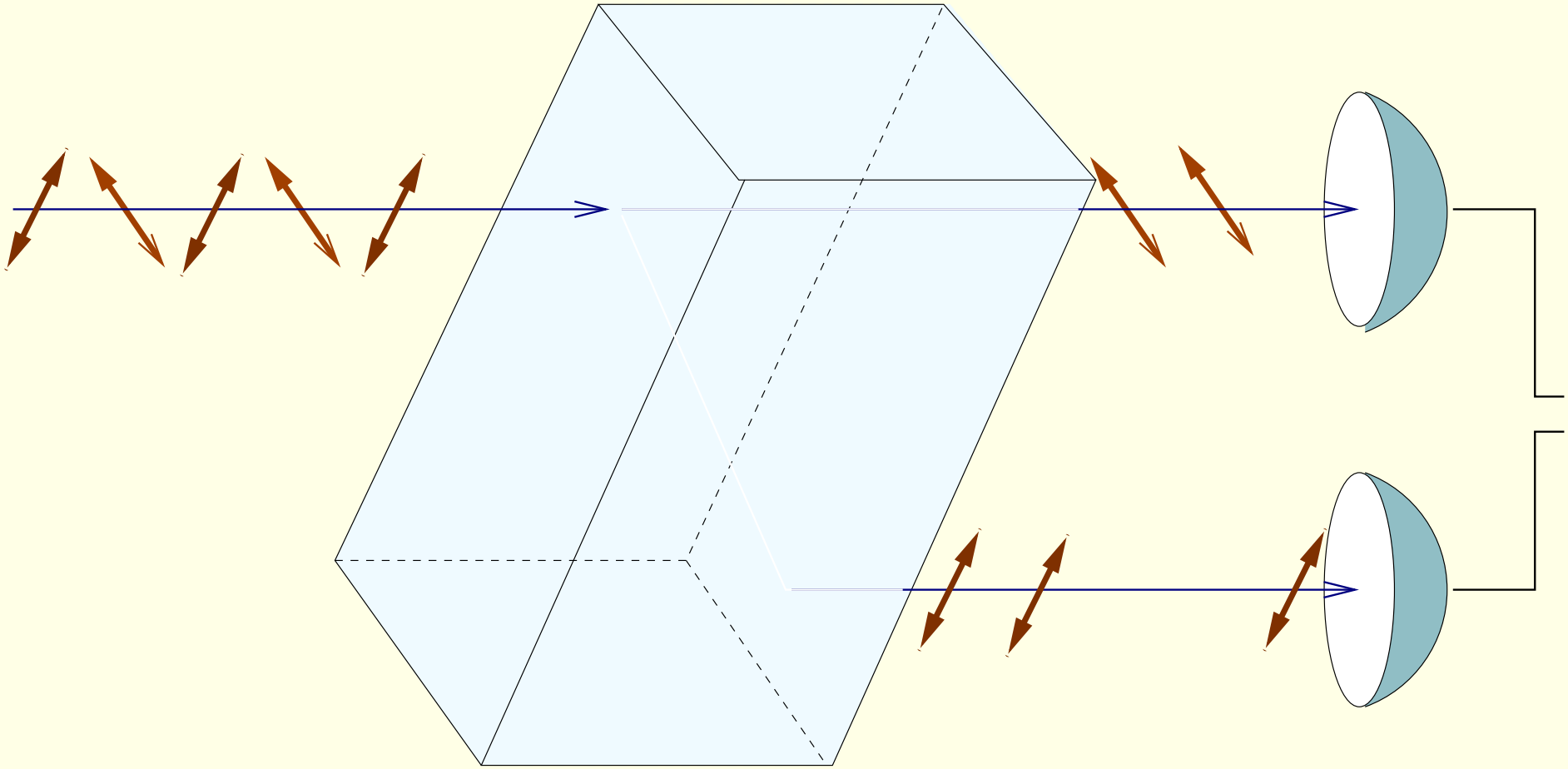
... z prawdopodobieństwem 1/2 przechodzi do wiązki zwyczajnej lub ...



... 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 mechaniki 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 mechaniki kwantowej nie są współmierzalne. Pomiar jednej z nich czyni drugą całkowicie nieokreśloną. Mamy tu do czynienia z zasadą nieoznaczoności Heisenberga.
- Fakt, że wyniki pomiarów w mechanice kwantowej mają charakter losowy umożliwia, jak się okazuje, 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 mechaniki kwantowej nie są współmierzalne. Pomiar jednej z nich czyni drugą całkowicie nieokreśloną. Mamy tu do czynienia z zasadą nieoznaczoności Heisenberga.
- Fakt, że wyniki pomiarów w mechanice kwantowej mają charakter losowy umożliwia, jak się okazuje, bezpieczne przekazywanie klucza kryptograficznego!

Zaraz zobaczymy w jaki sposób!

6 Kryptografia kwantowa

6.1 Alfabety kwantowe

6 Kryptografia kwantowa

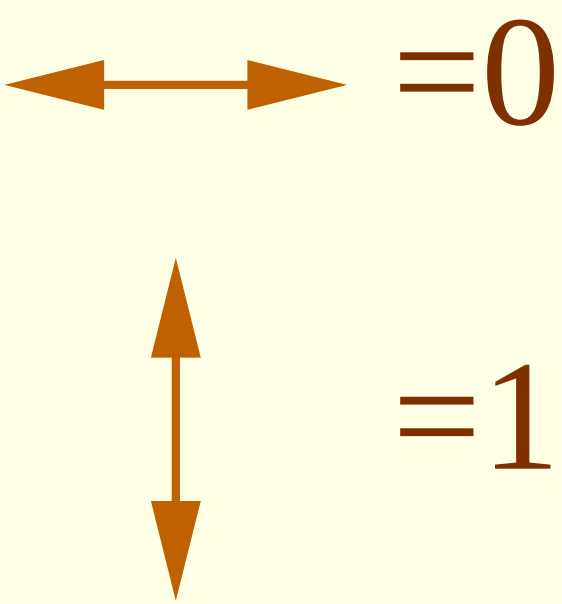
6.1 Alfabety kwantowe

Alfabet prosty

6 Kryptografia kwantowa

6.1 Alfabety kwantowe

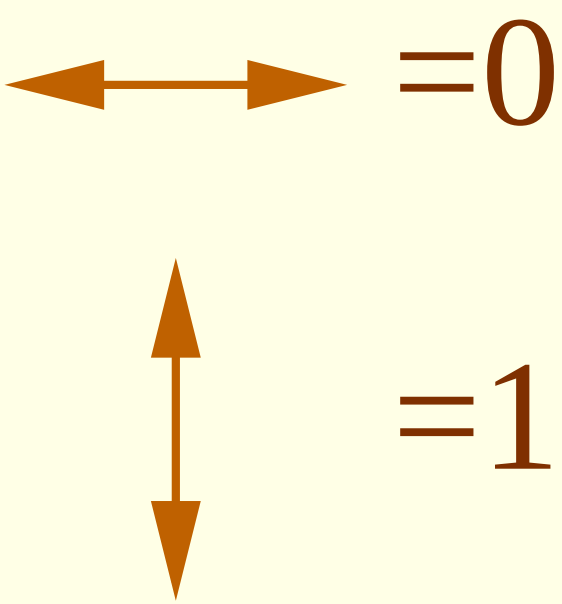
Alfabet prosty



6 Kryptografia kwantowa

6.1 Alfabety kwantowe

Alfabet prosty



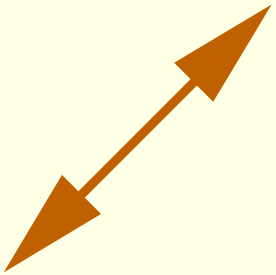
Alfabet ukośny

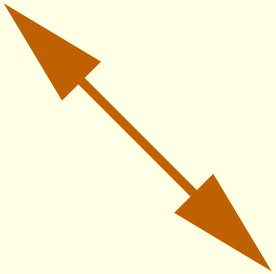
6 Kryptografia kwantowa

6.1 Alfabety kwantowe

Alfabet prosty

Alfabet ukośny

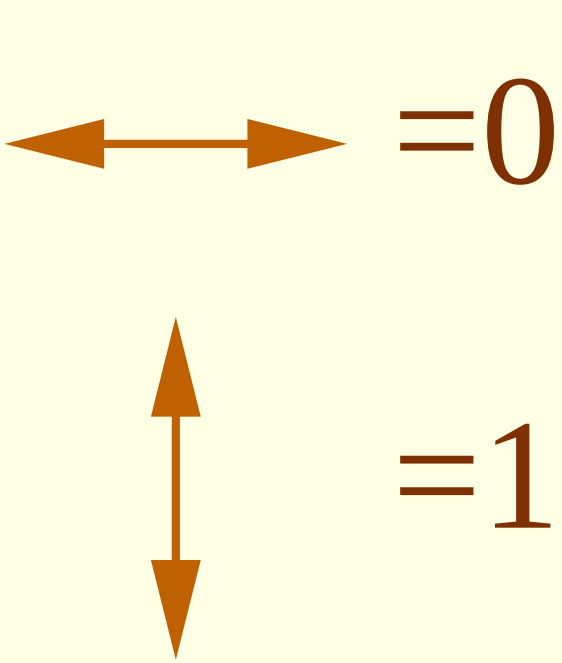




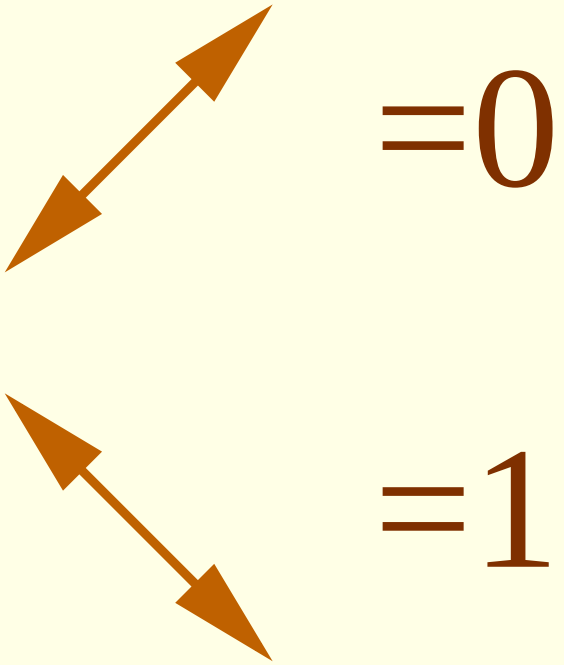
6 Kryptografia kwantowa

6.1 Alfabety kwantowe

Alfabet prosty



Alfabet ukośny



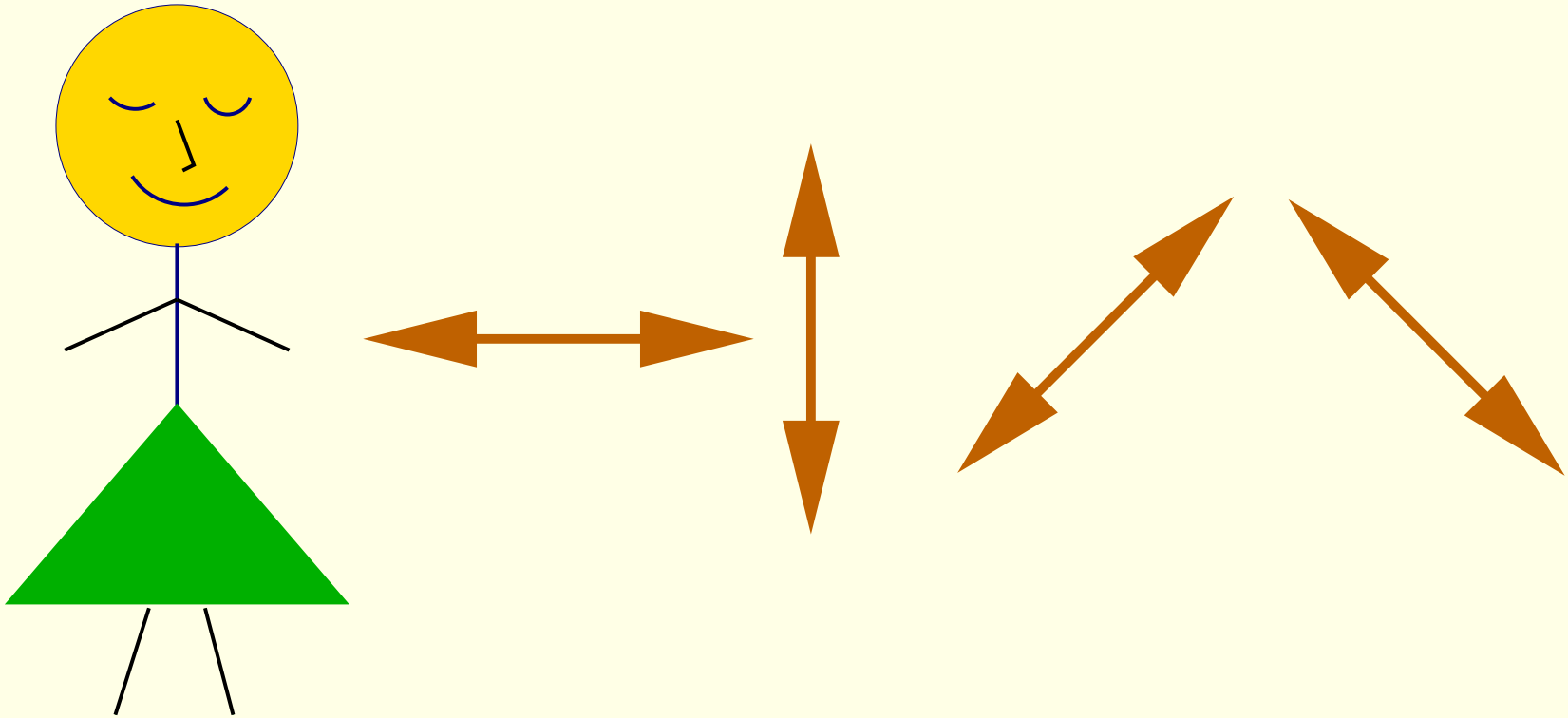
Dysponujemy dwoma różnymi alfabetami kwantowymi. Dwie wzajemnie prostopadłe polaryzacje stanowią znaki alfabetu, którym możemy przypisać wartości binarne 0 lub 1 i w ten sposób kodować informację, którą chcemy przesłać kanałem kwantowym.

6.2 Protokół BB84 (Bennett i Brassard, 1984)

Charles Bennett

Gilles Brassard

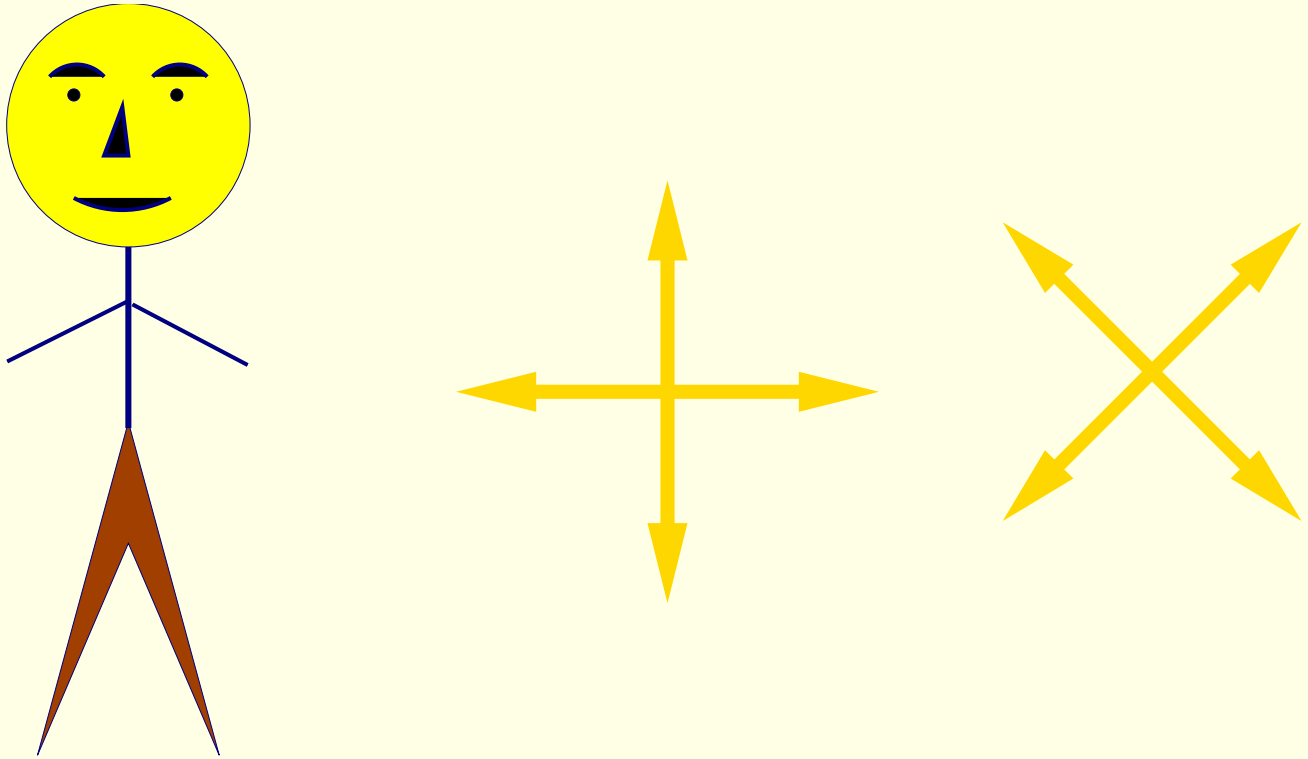
Krok 1



Alicja wybiera losowo jedną z czterech polaryzacji i wysyła do Bolka foton o takiej polaryzacji.

Ciąg fotonów o określonych polaryzacjach 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 publicznie informuje go czy wybrana przez niego baza (prosta lub ukośna) była właściwa czy nie.

Krok 3

Bolek notuje wyniki pomiarów zachowując je w tajemnicy.

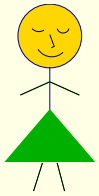
Krok 4

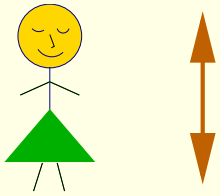
Bolek publicznie informuje Alicję jakiej bazy używał do pomiaru, zaś Alicja publicznie informuje go czy wybrana przez niego baza (prosta lub ukośna) była właściwa czy nie.

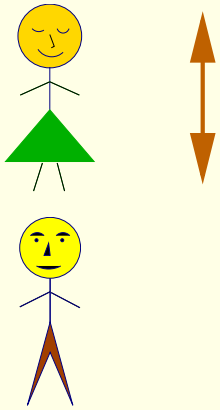
Krok 5

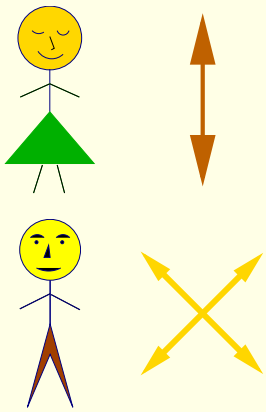
Alicja i Bolek przechowują wyniki pomiarów, dla których Bolek użył właściwej bazy. Wyniki tych pomiarów można zapisać w postaci binarnej przypisując zera polaryzacji 0° i 45° zaś jedynki polaryzacji 90° i 135°. Uzyskany w ten sposób losowy ciąg zer i jedynek może stanowić klucz kryptograficzny.

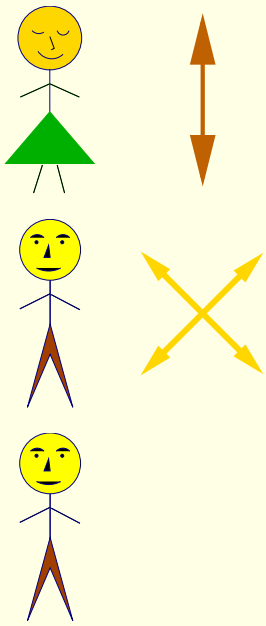
Jak to działa?

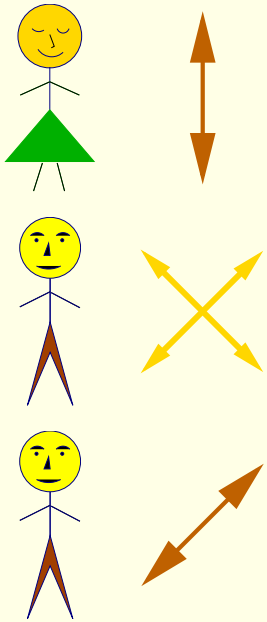


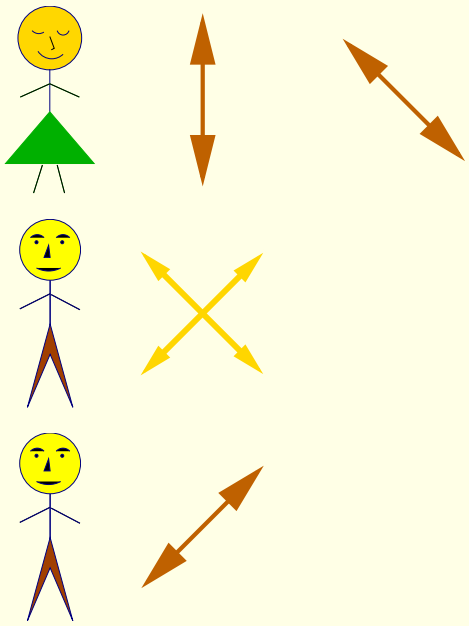


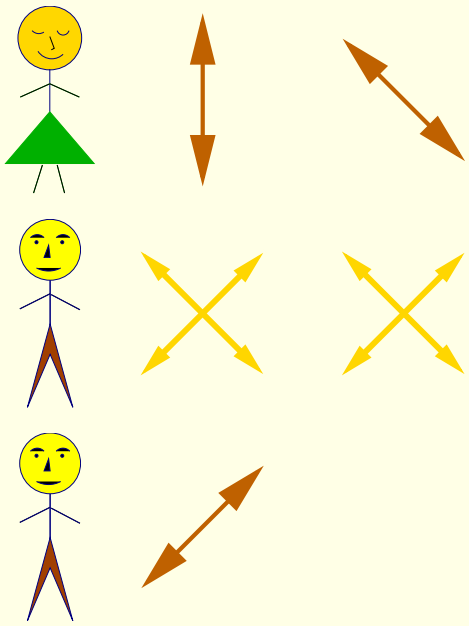


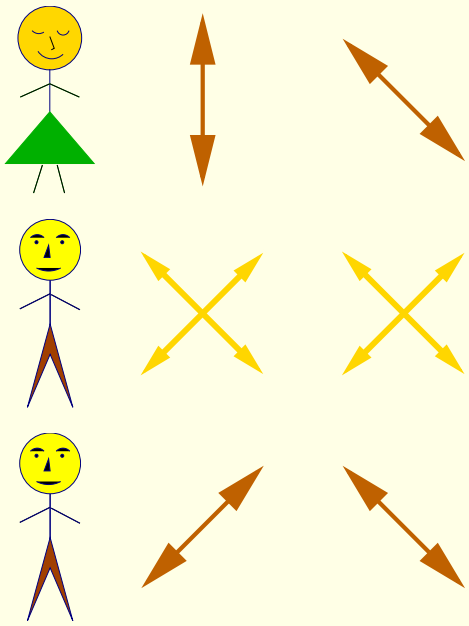


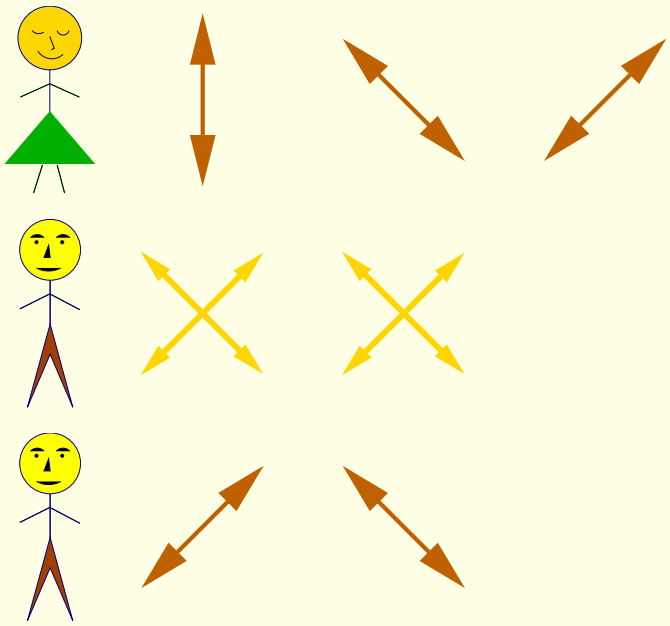


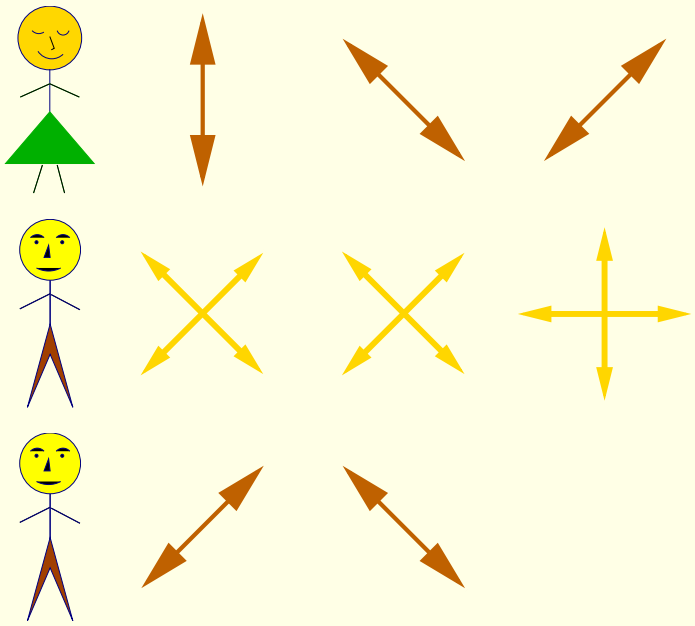


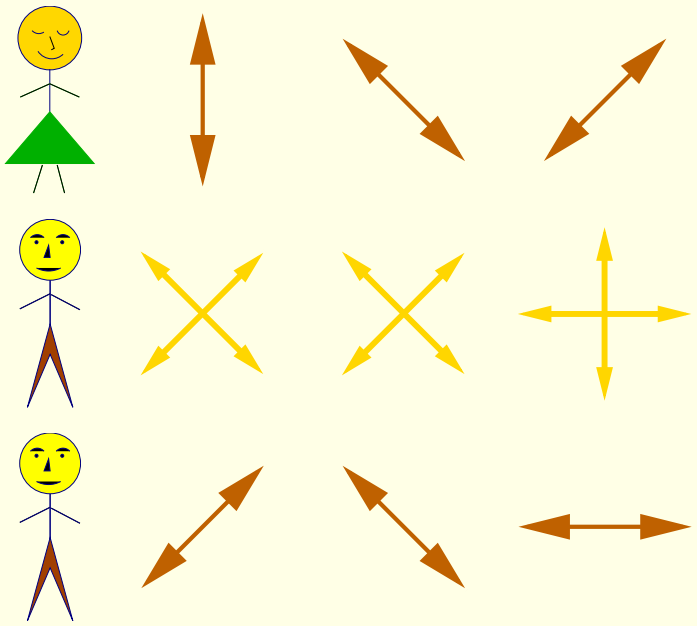


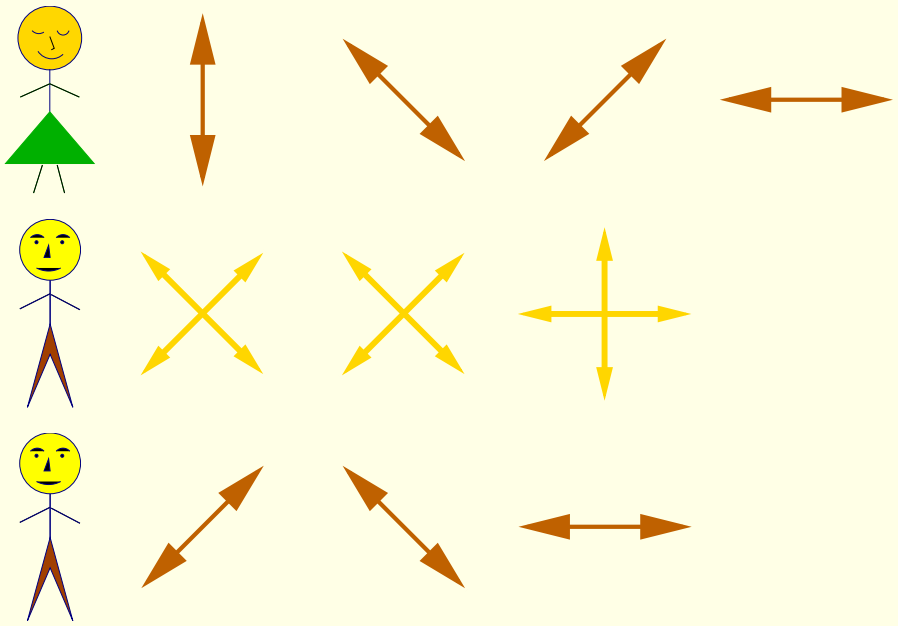


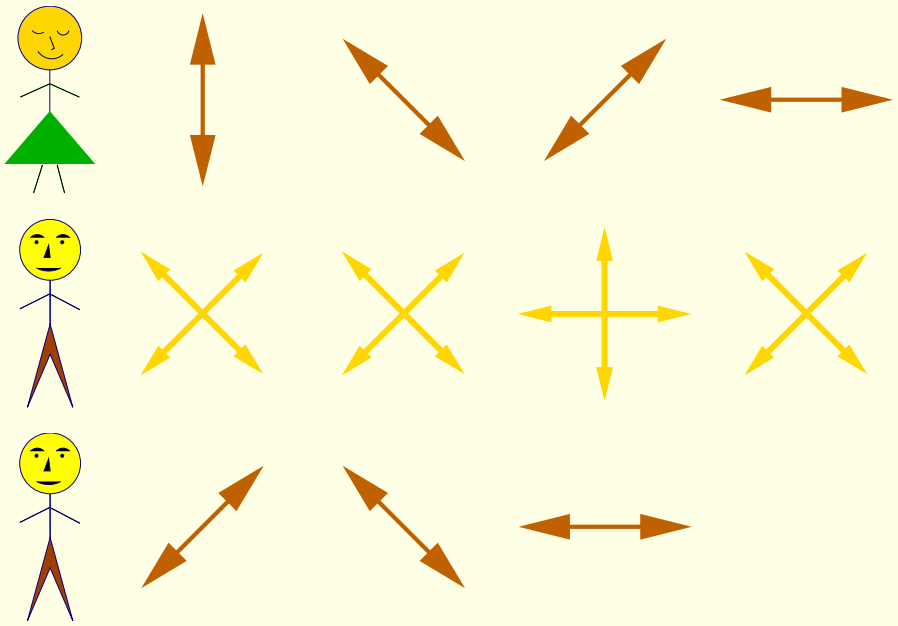


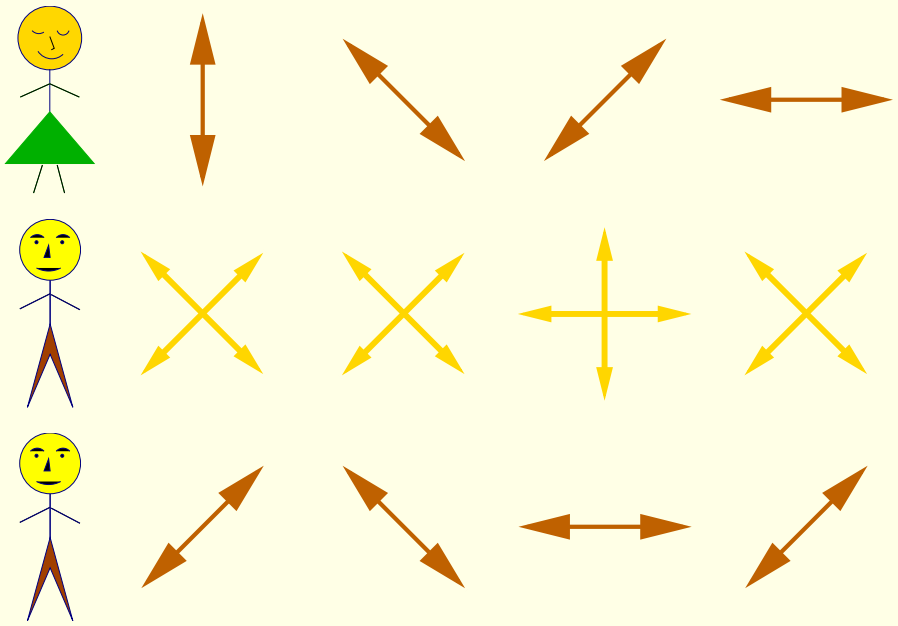


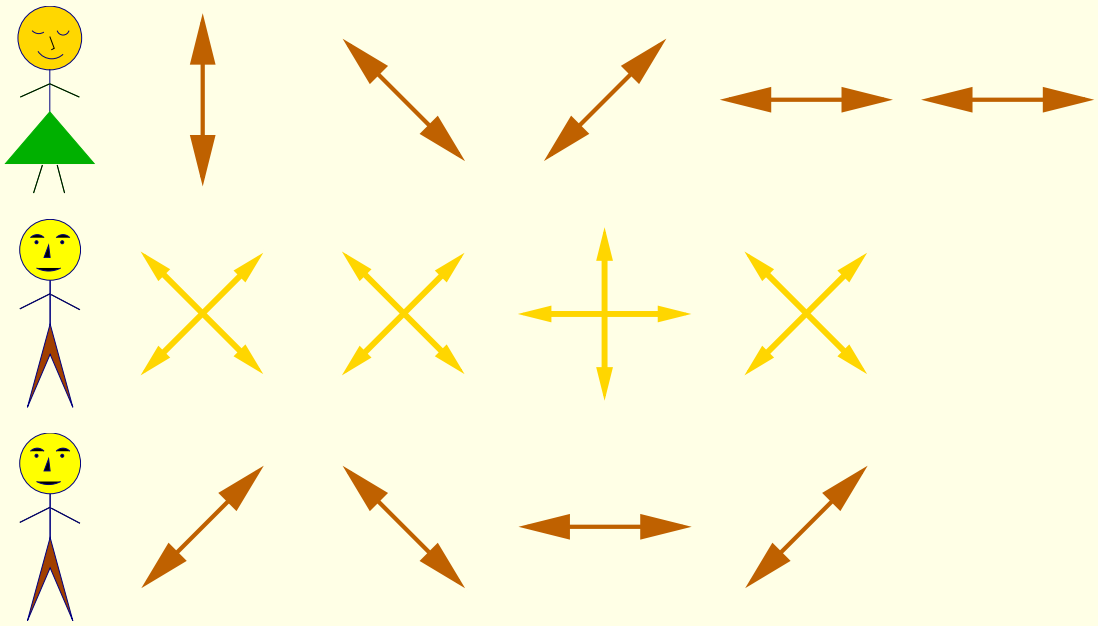


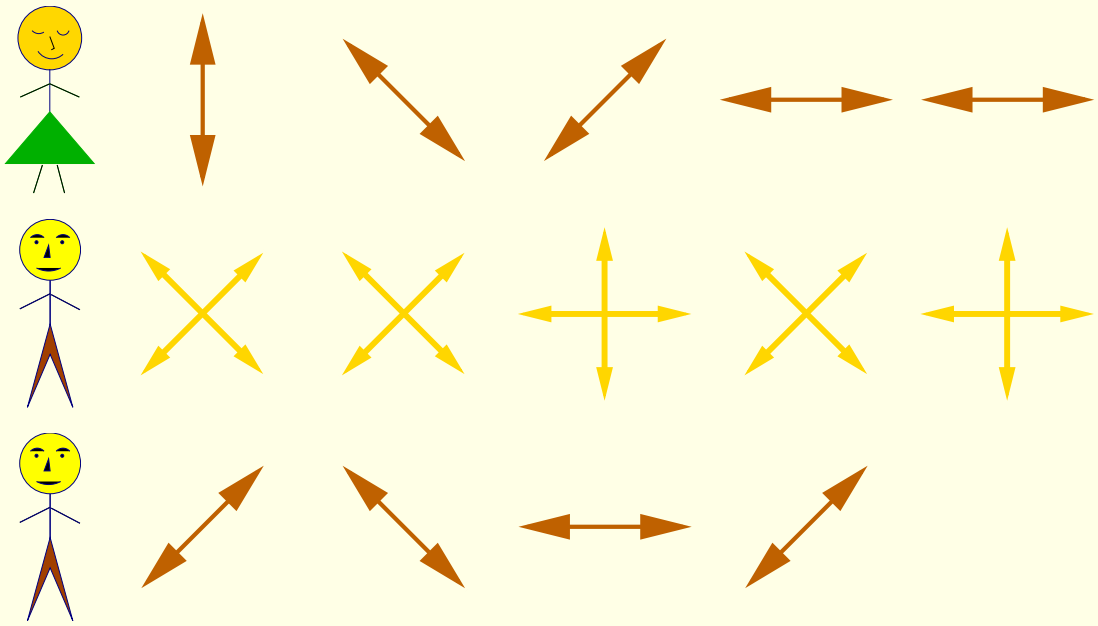


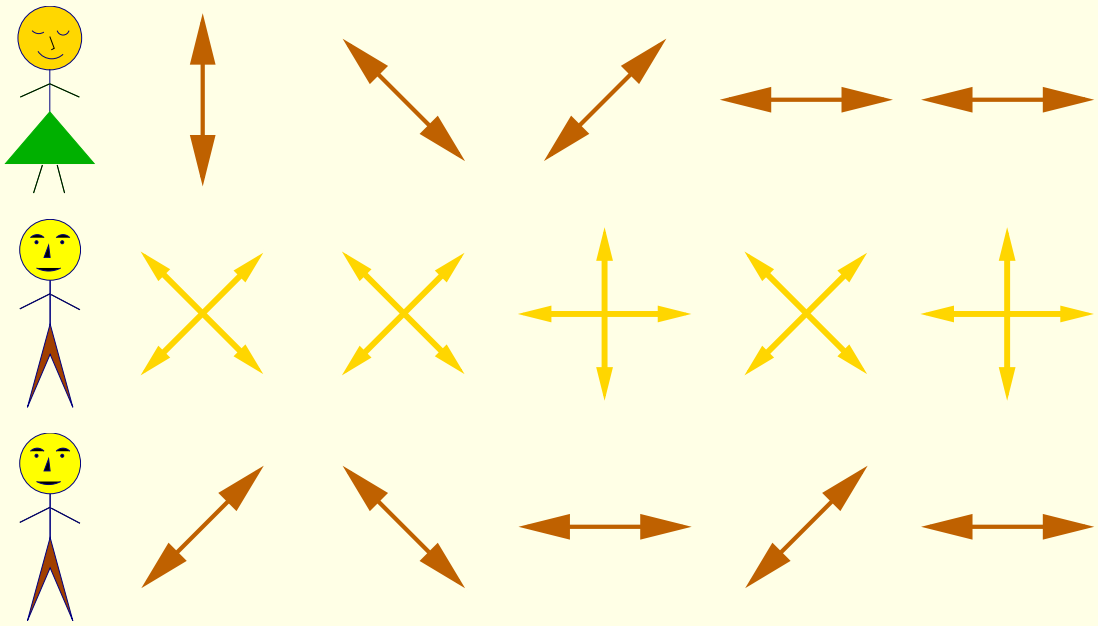


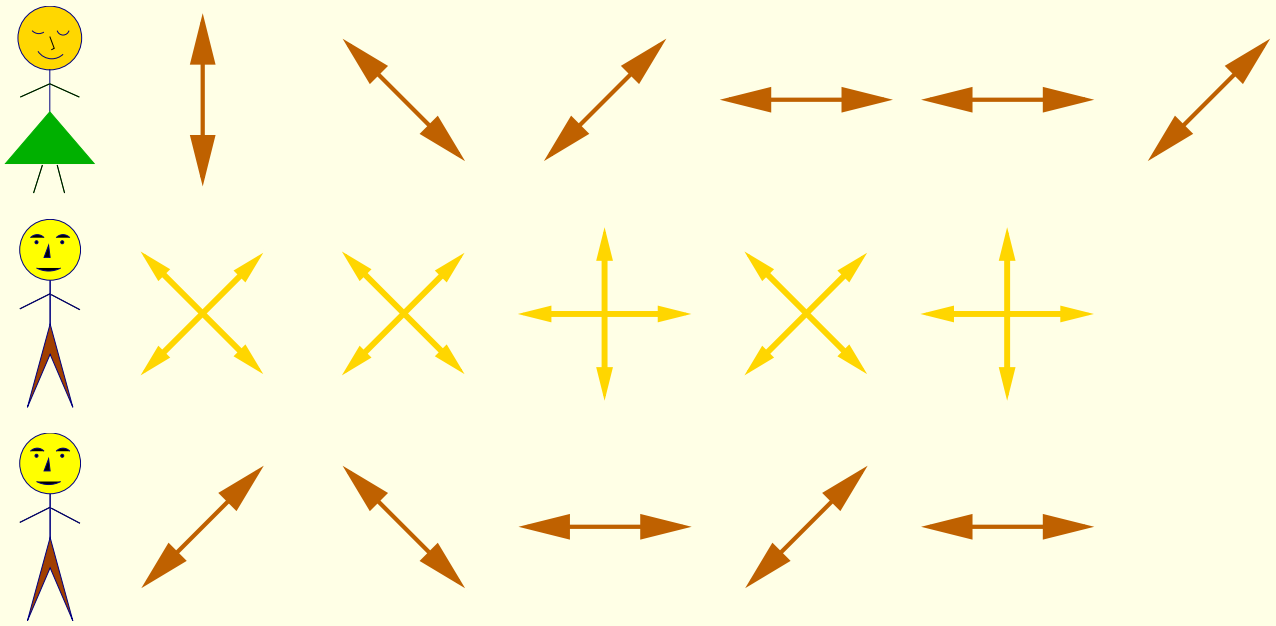


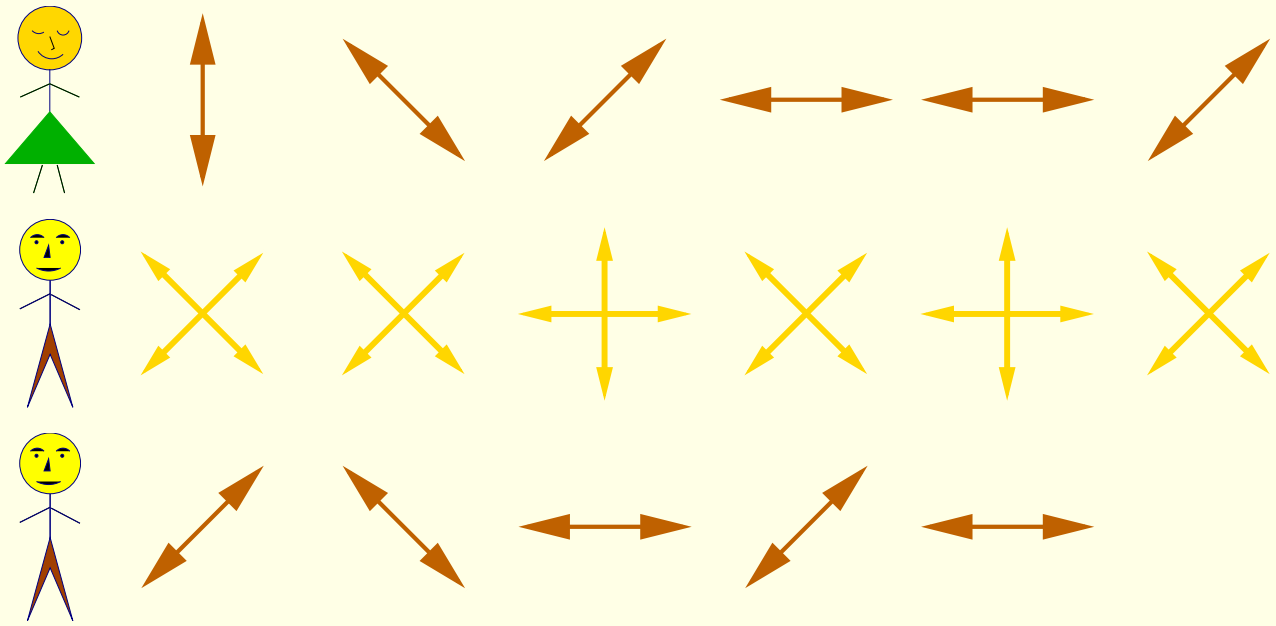


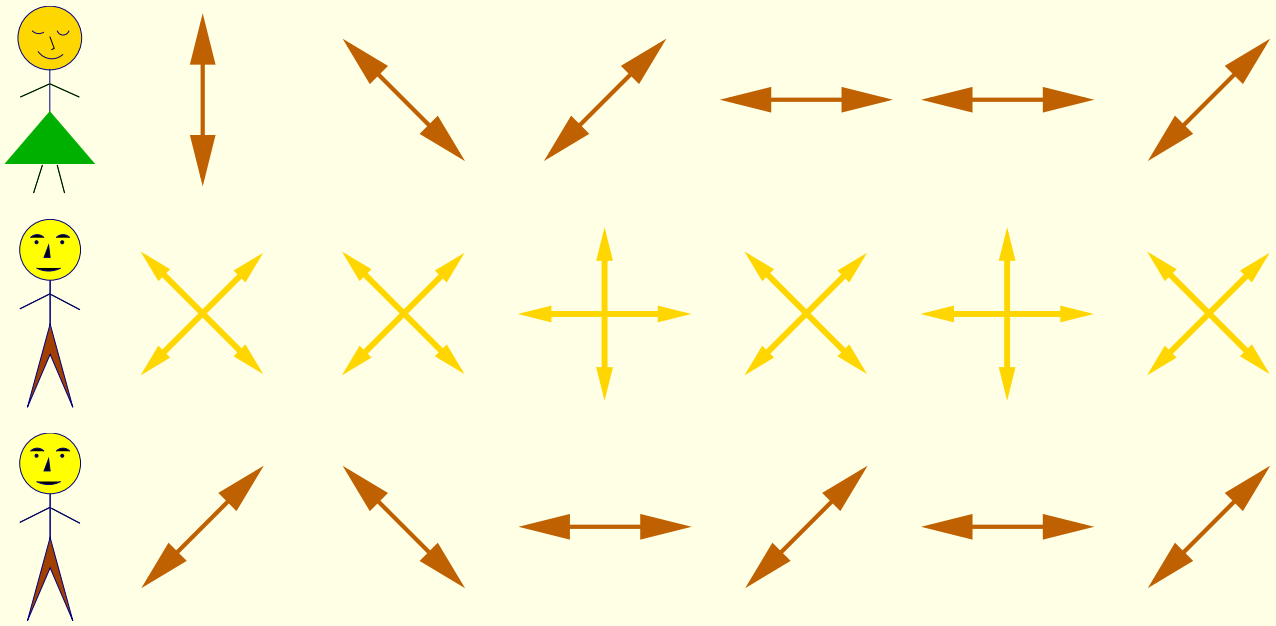


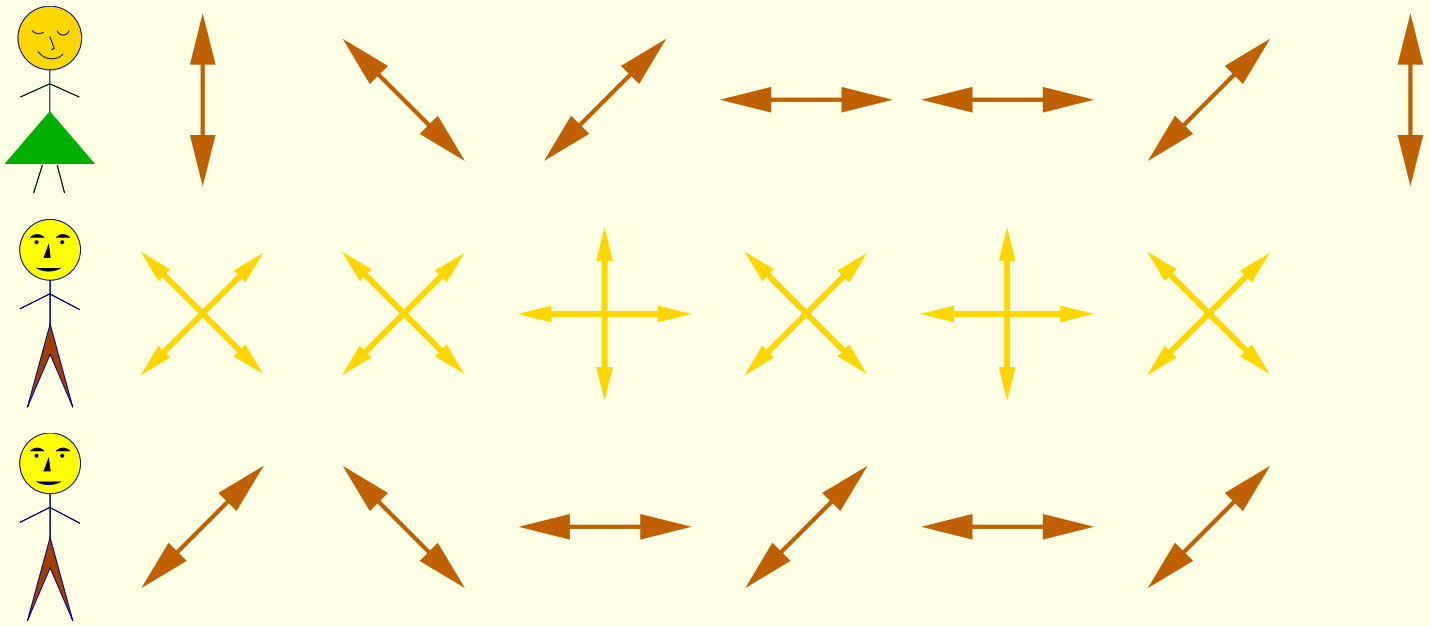


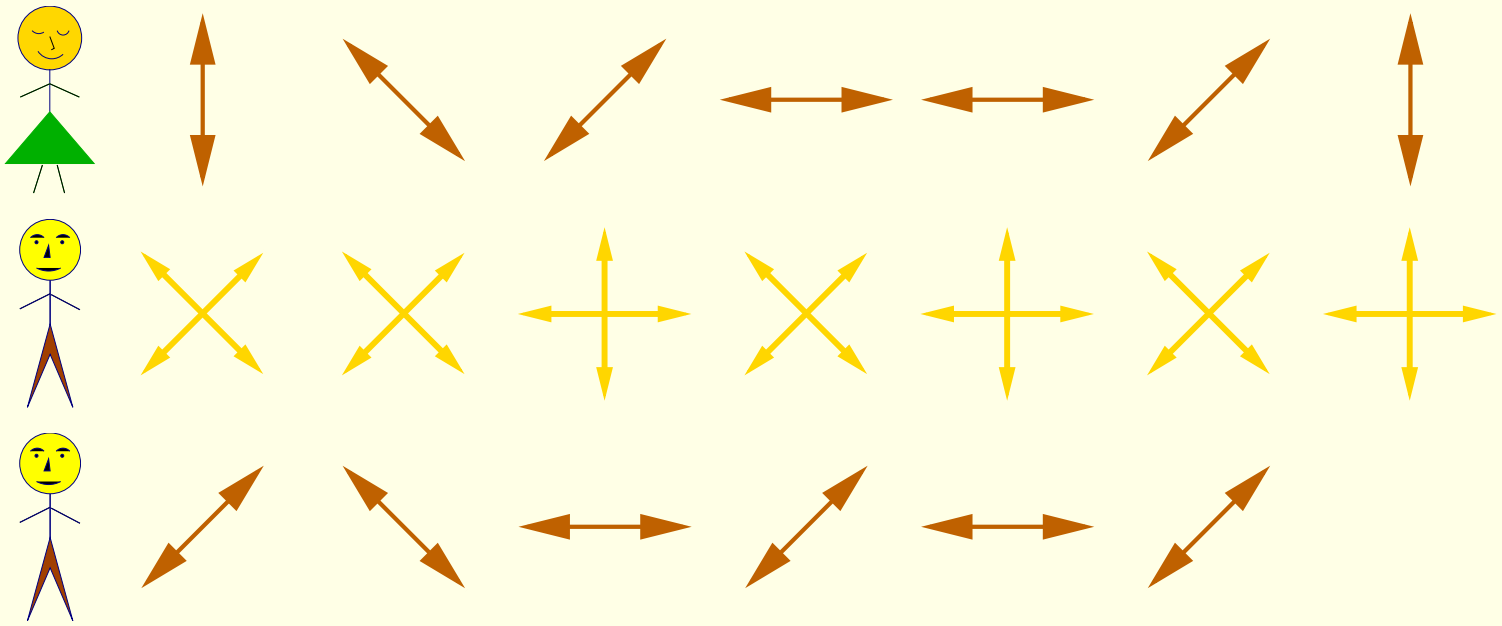


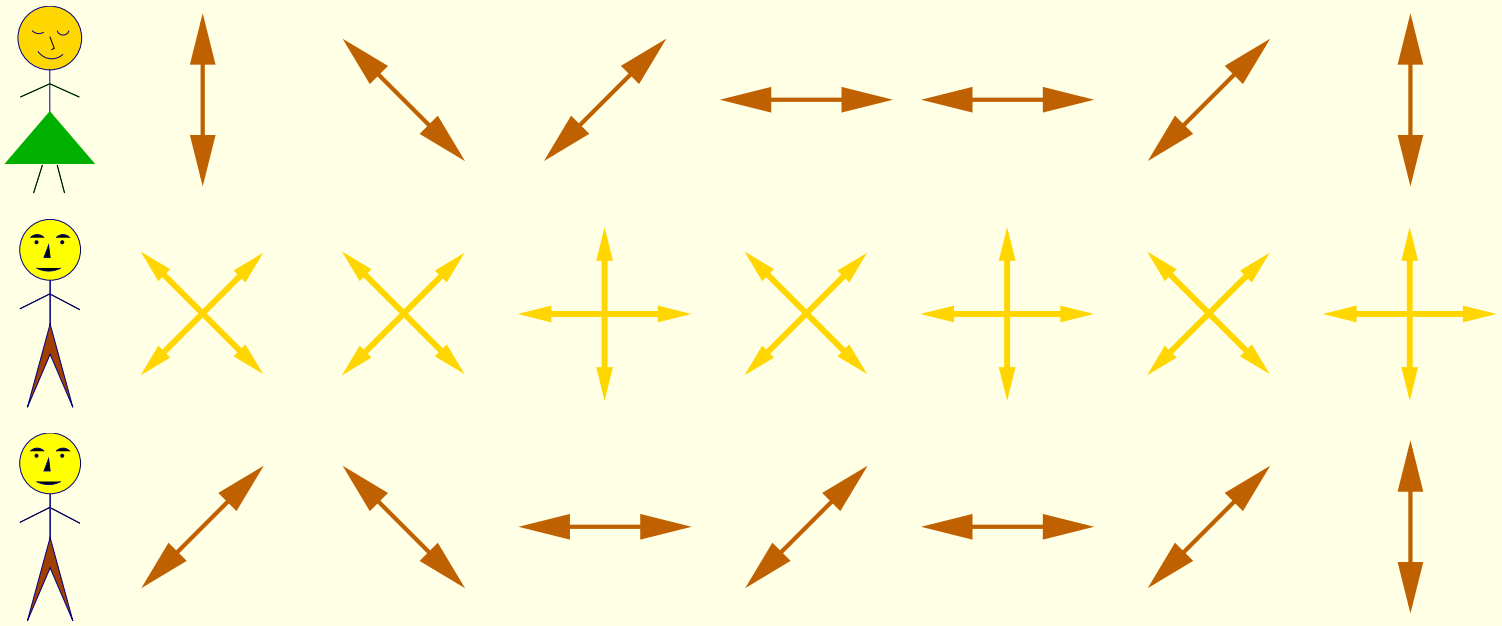


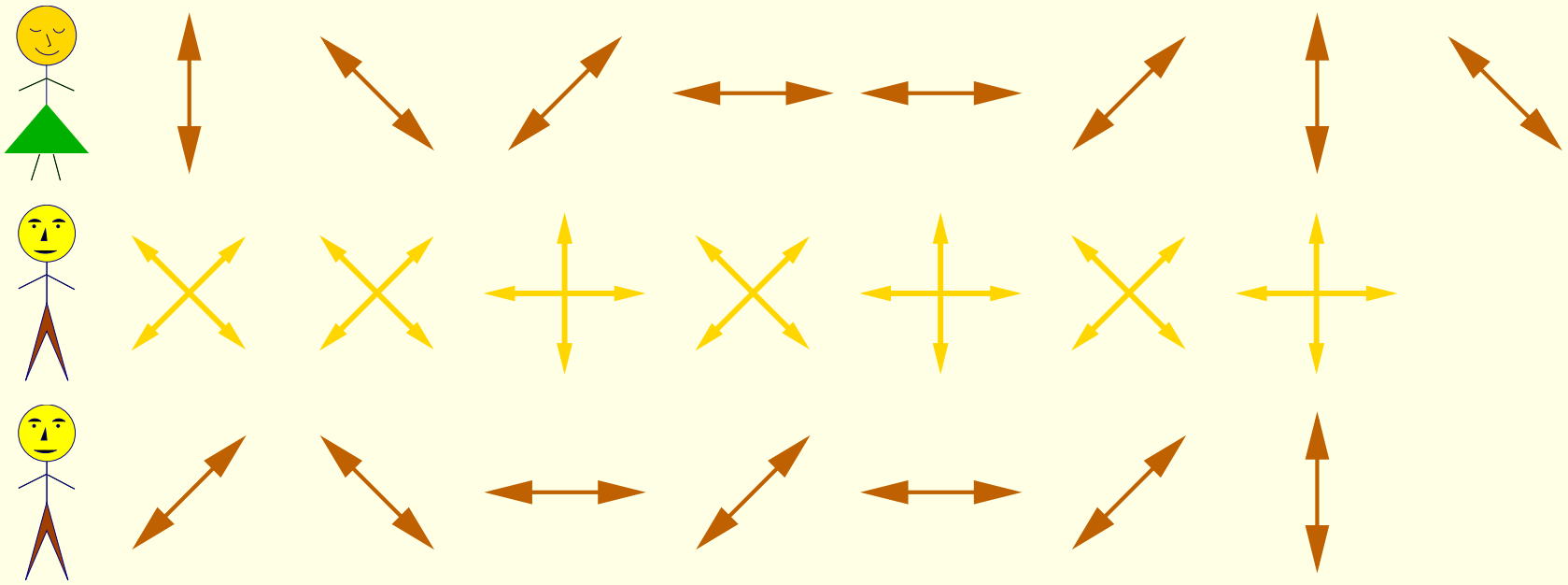


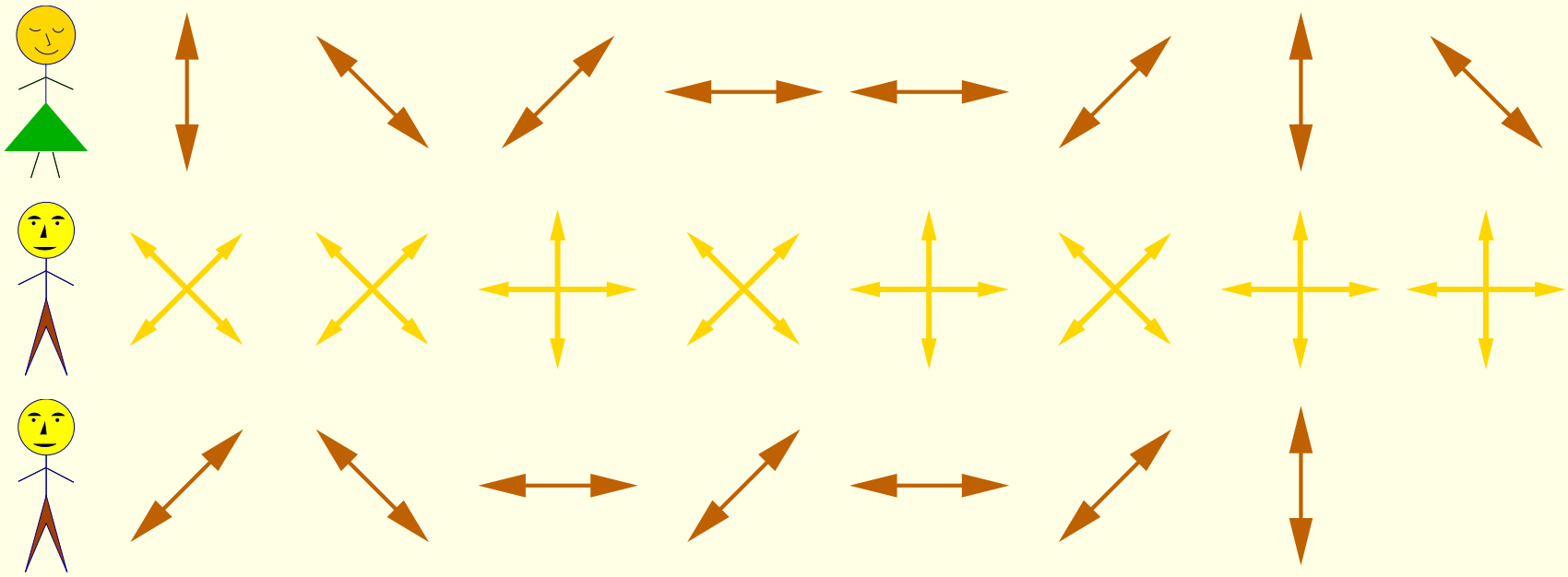


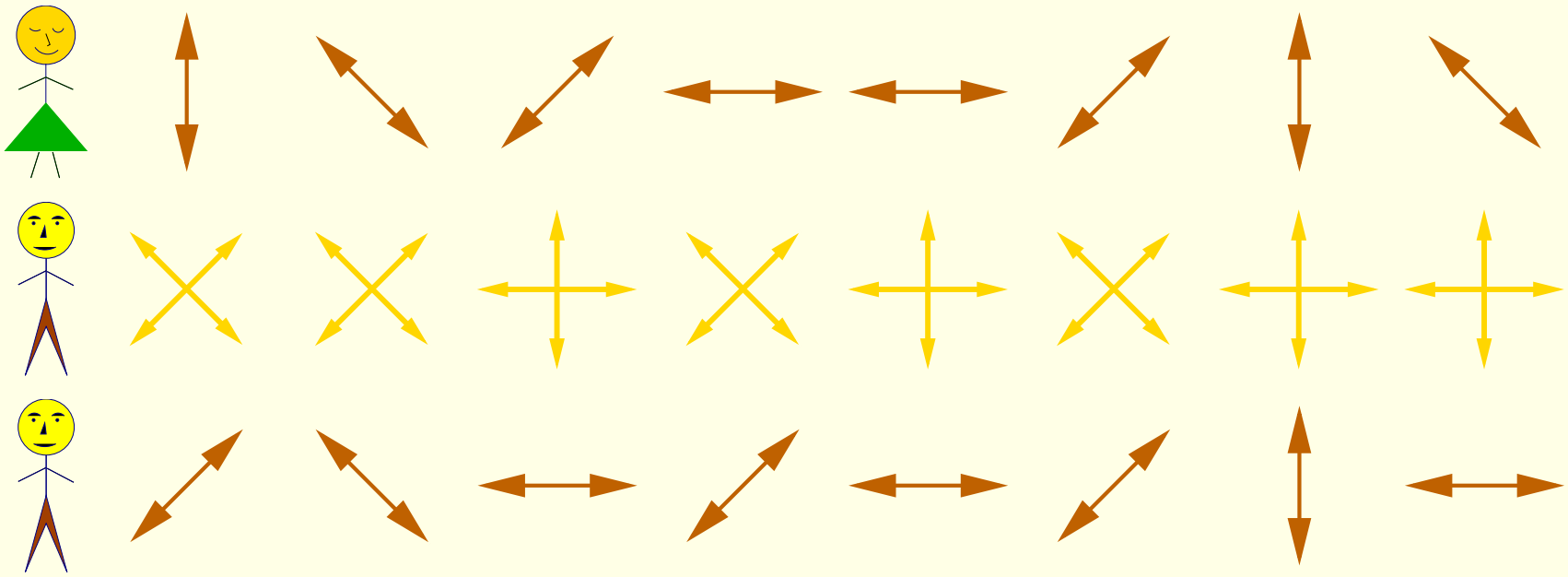


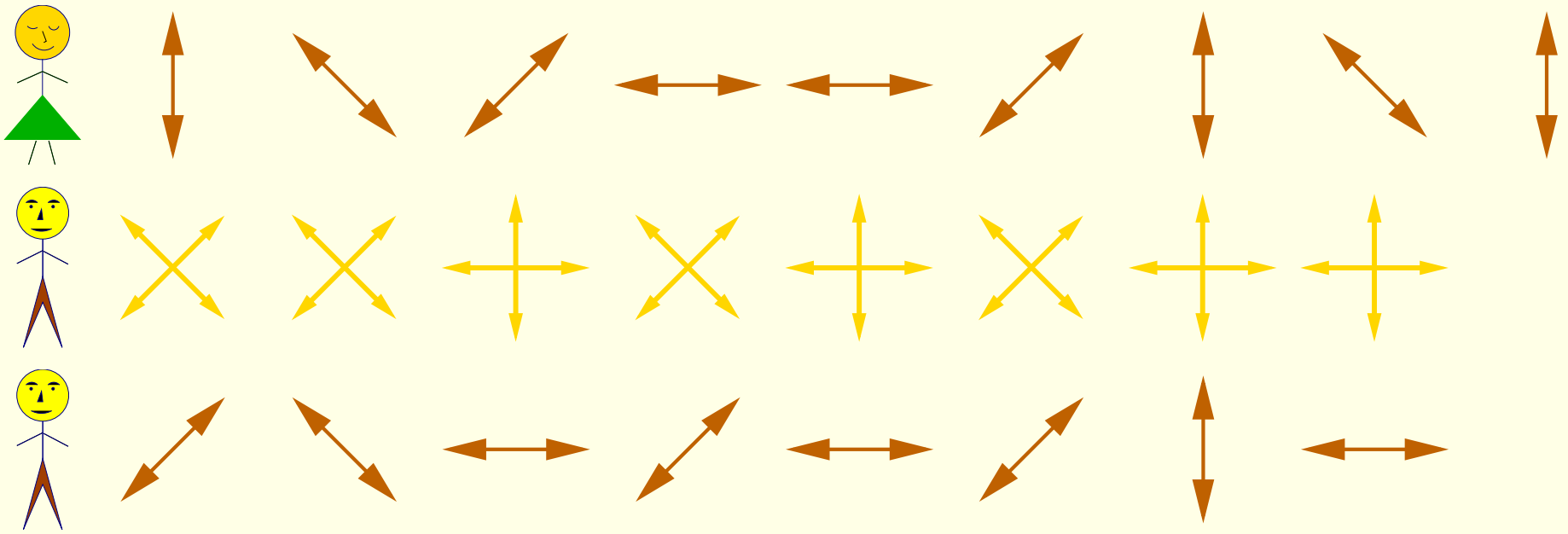


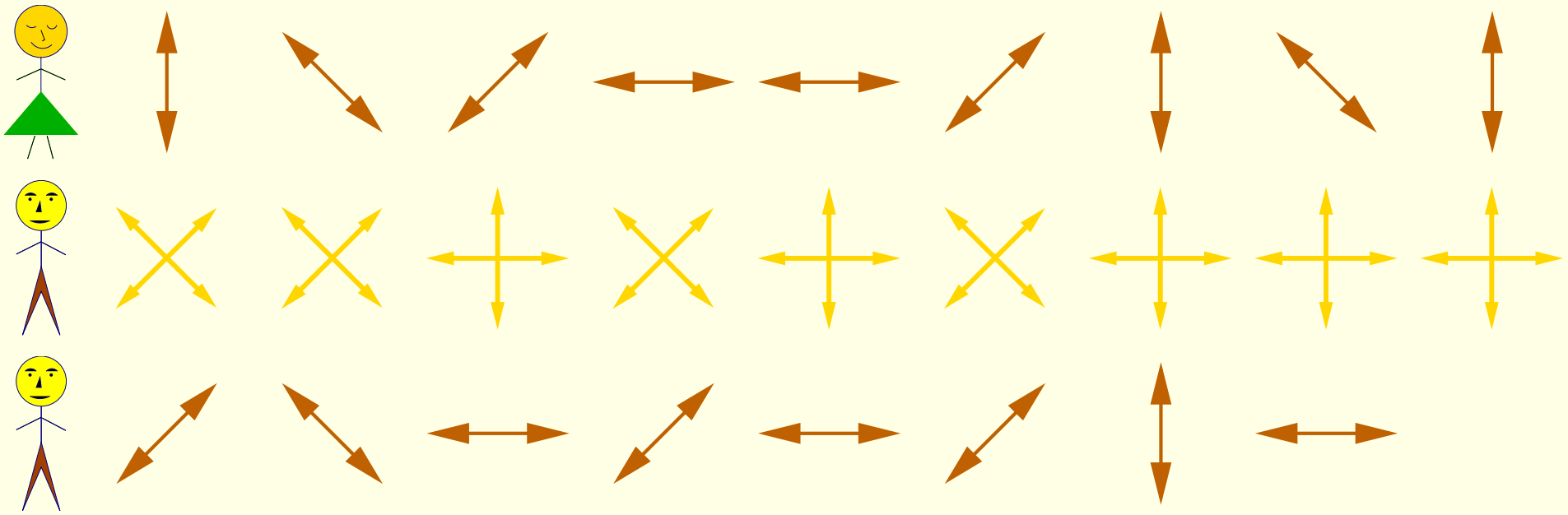


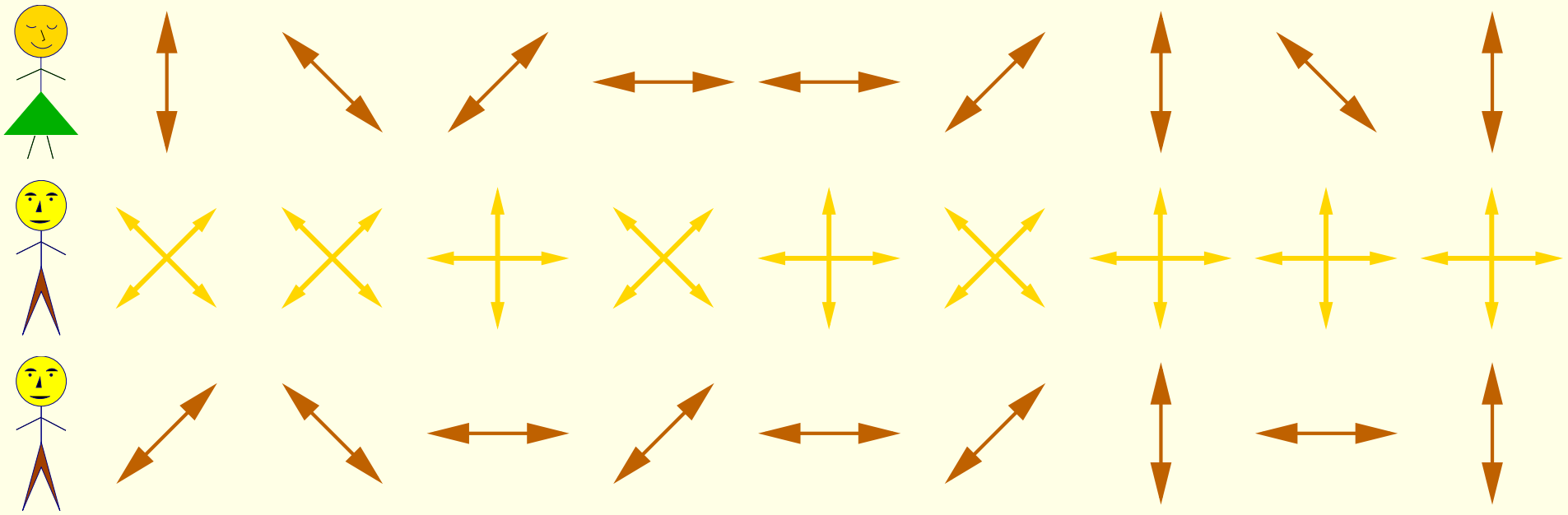


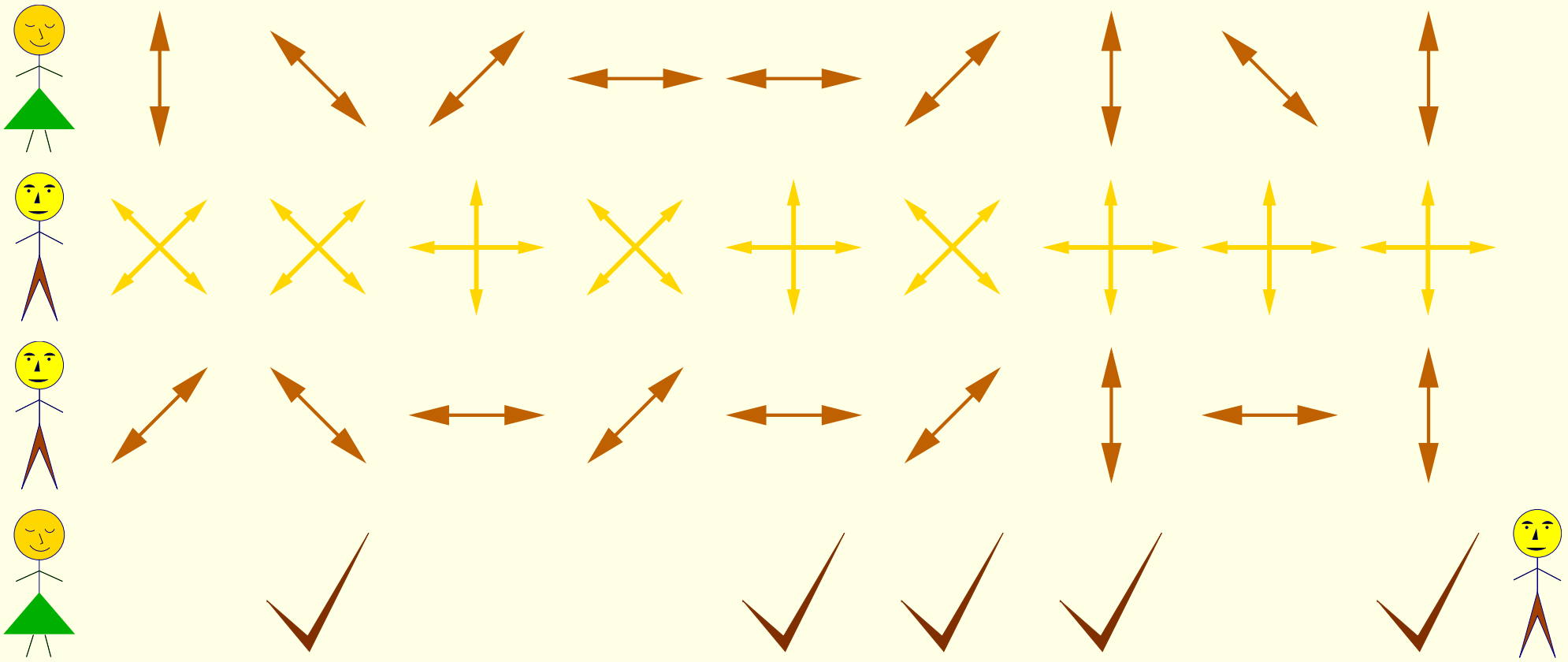


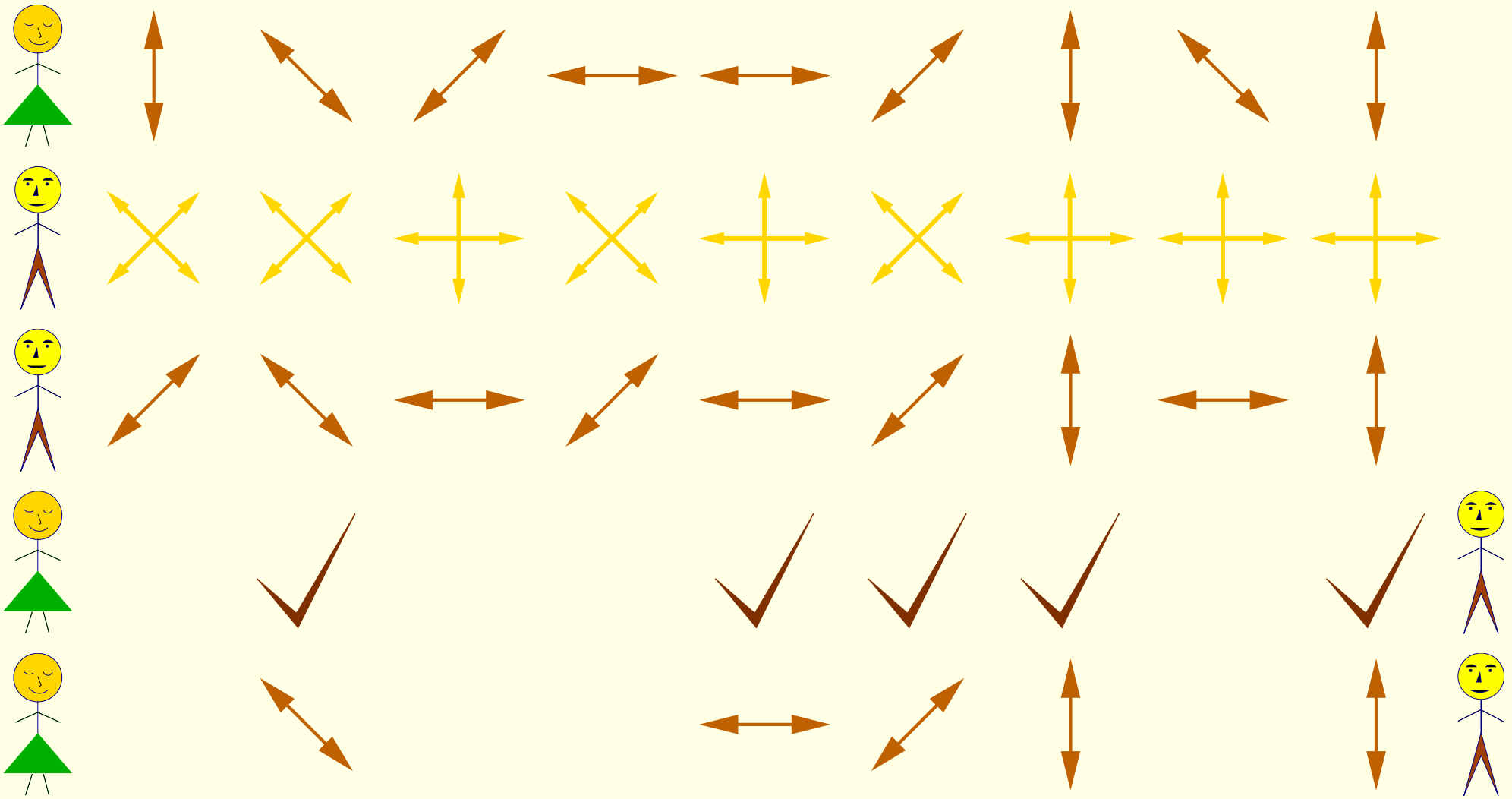


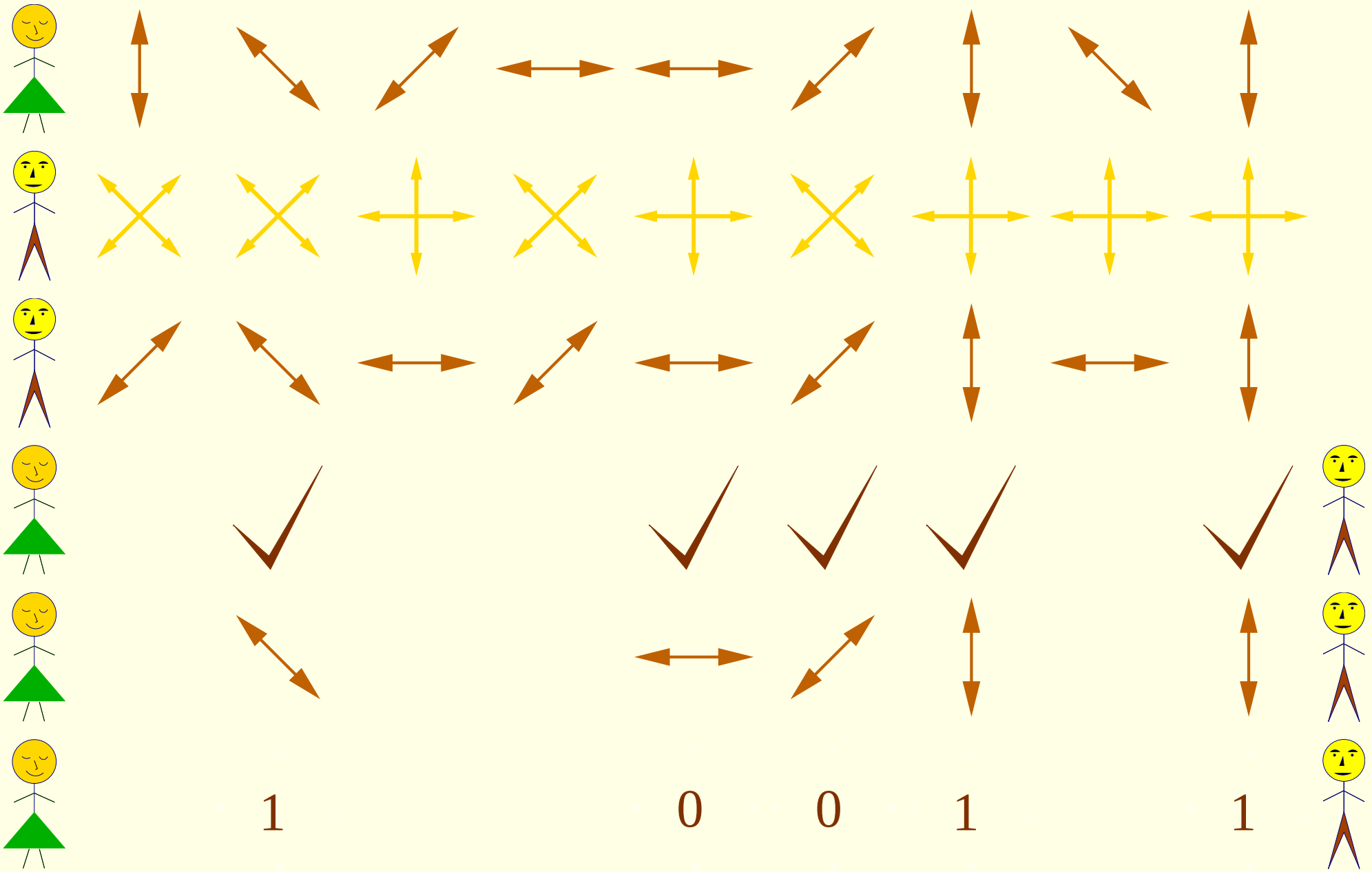




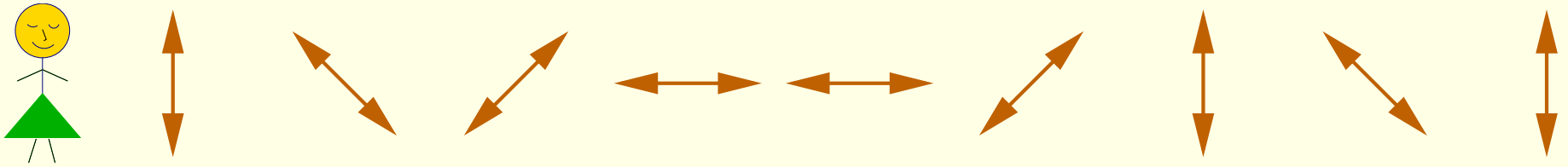


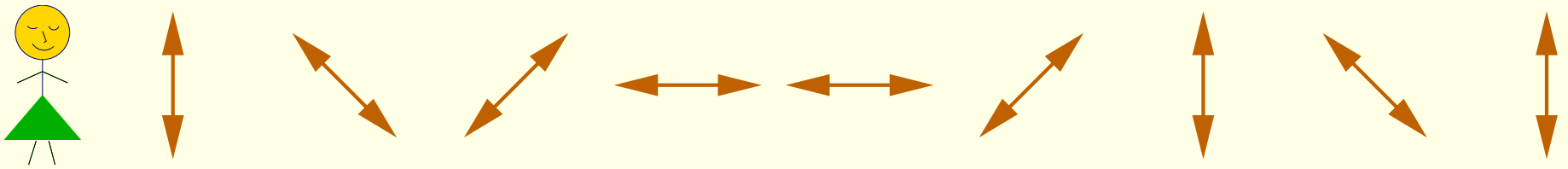




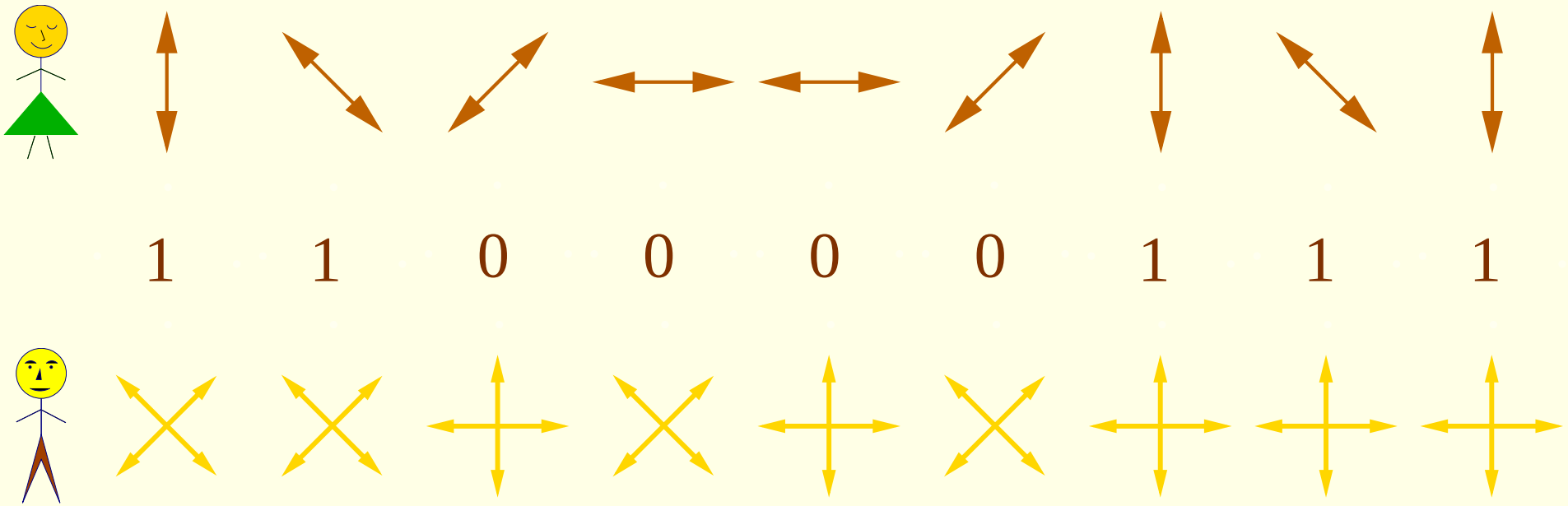

1
0
0
1
1

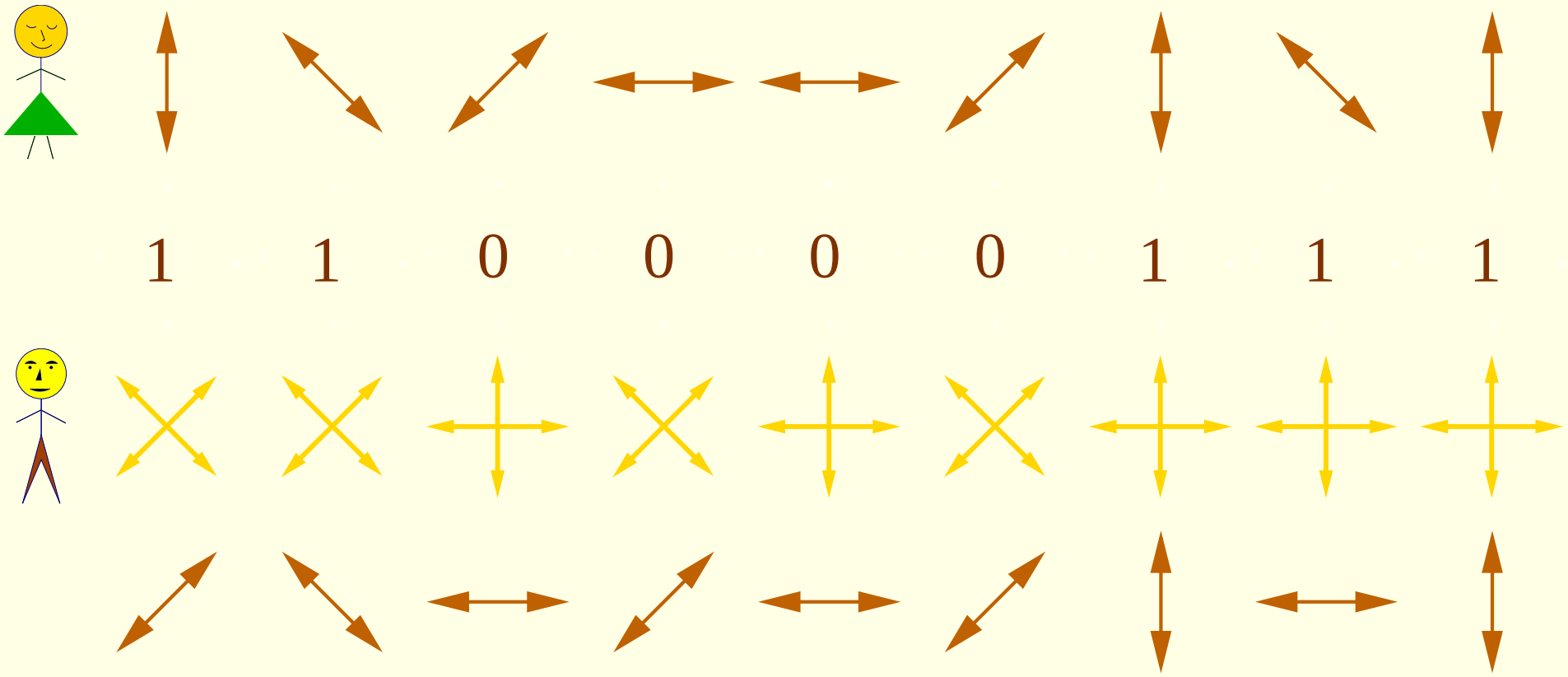
Błędne bity

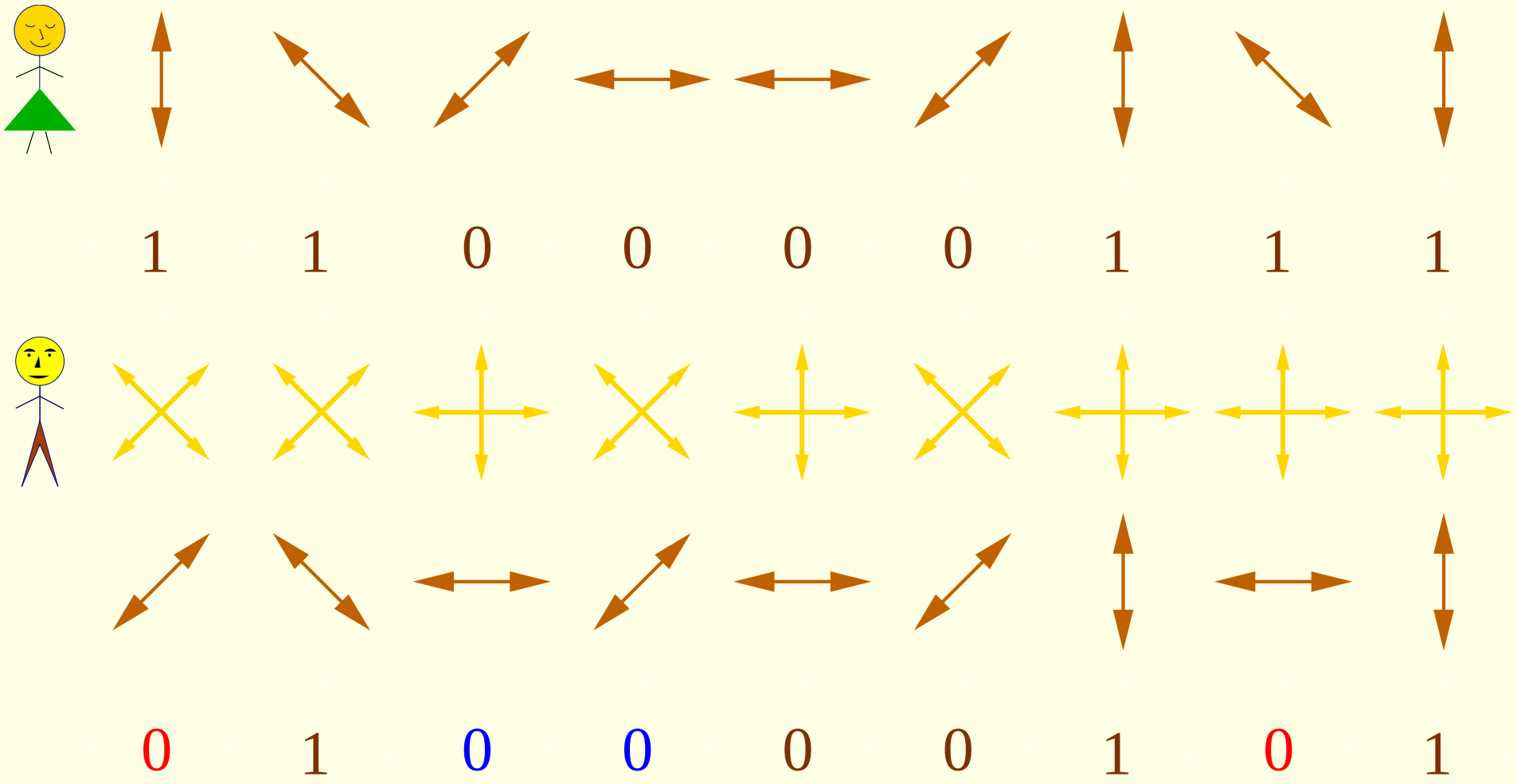


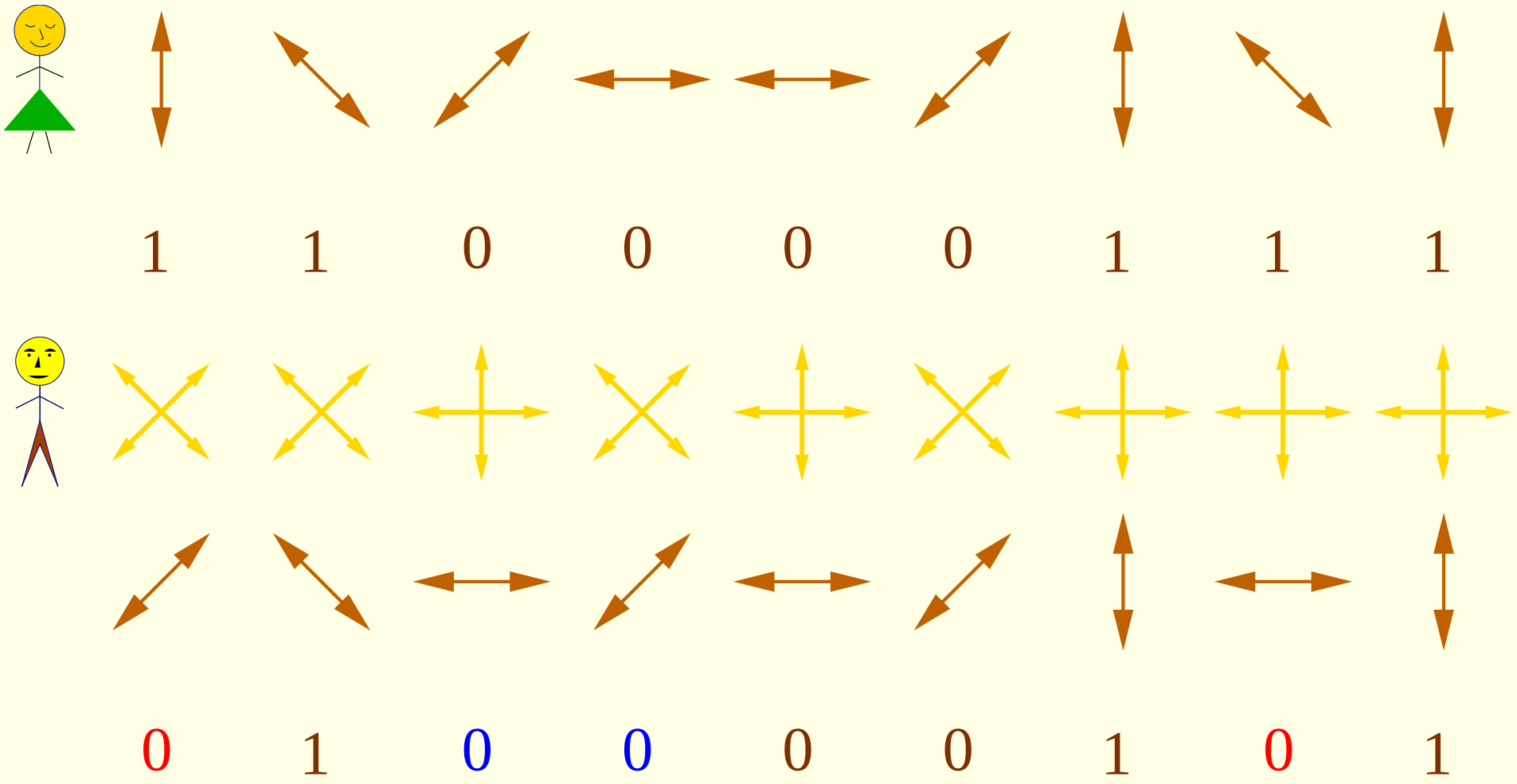


1 1 0 0 0 0 1 1 1


1 1 0 0 0 0 1 1 1

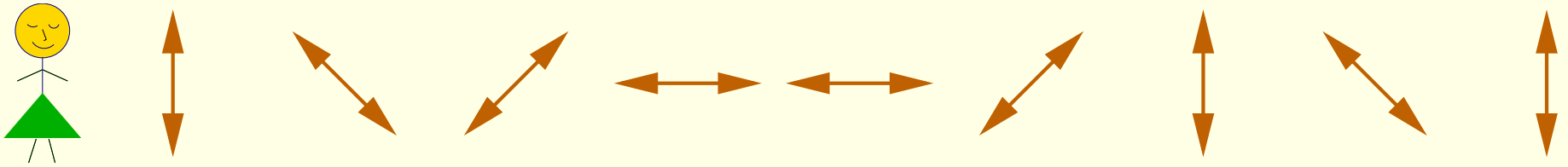

1 1 0 0 0 0 1 1 1

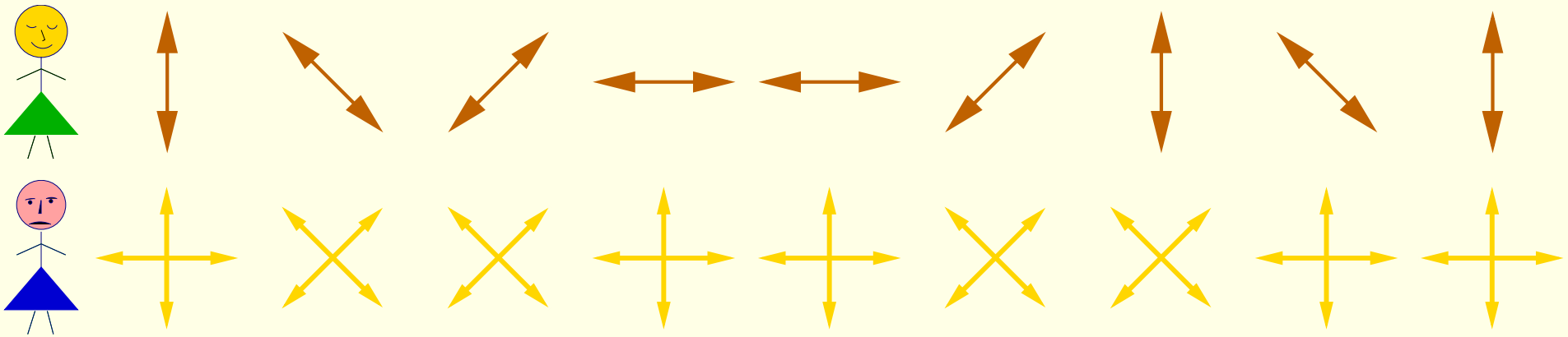

1 1 0 0 0 0 1 1 1
0 1 0 0 0 0 1 0 1

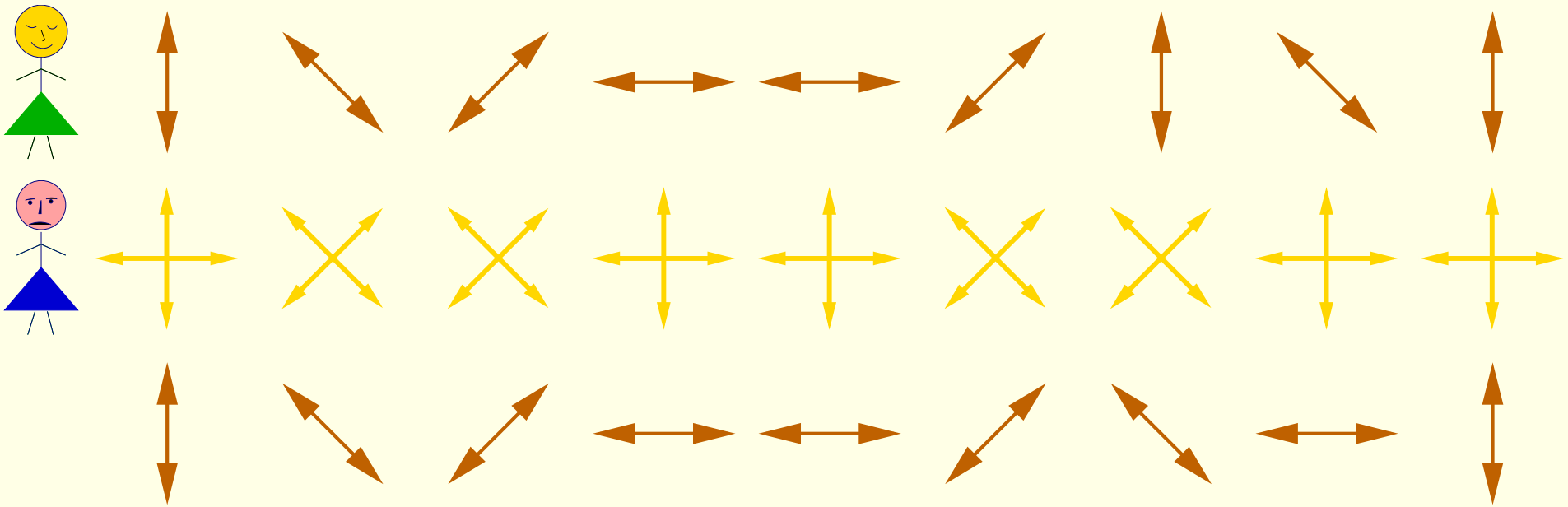


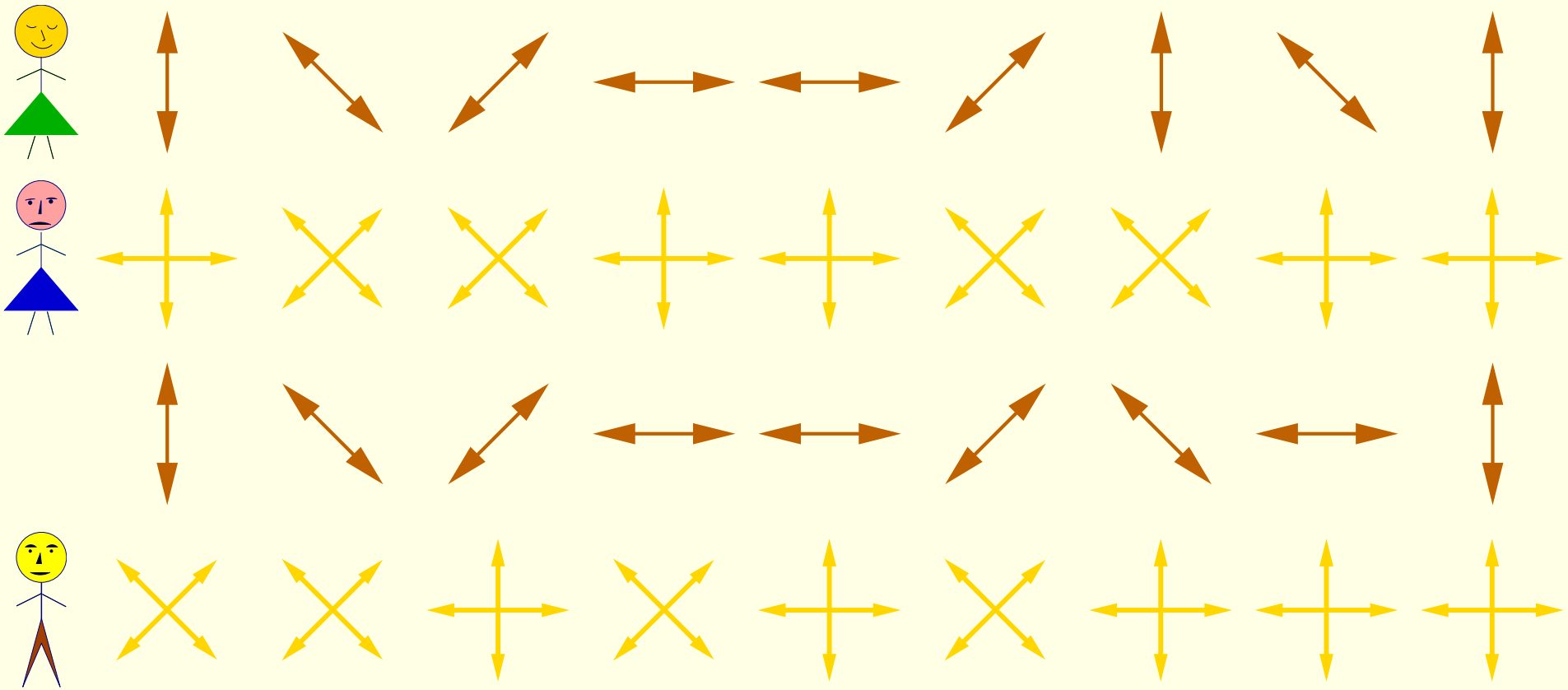
Średnio 50% bitów zarejestrowanych przez Bolka to bity pewne (brązowe), 25% bitów to bity prawidłowe mimo złego wyboru bazy (niebieskie) i 25% to bity nieprawidłowe (czerwone).

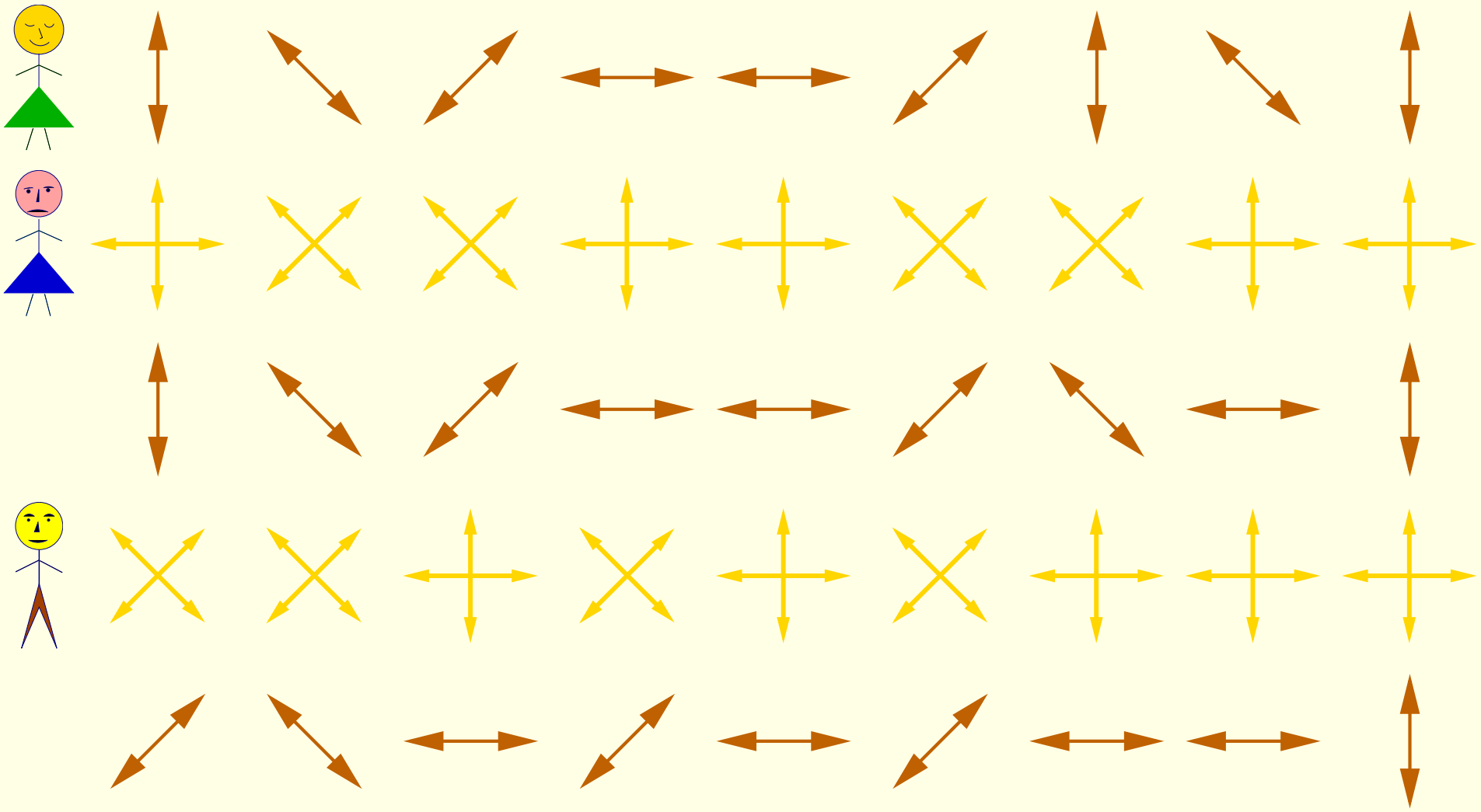
Ewa podsłuchuje

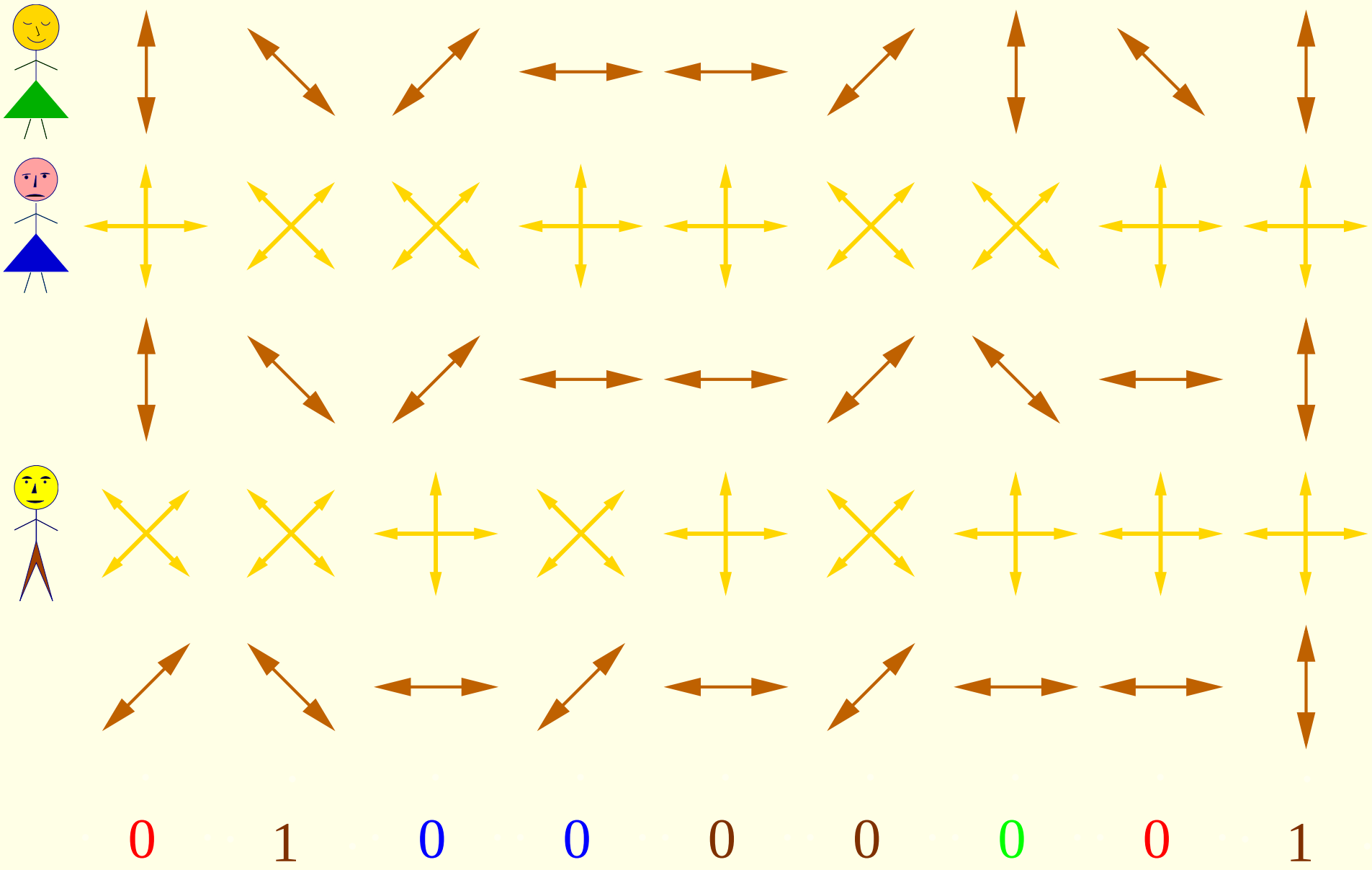


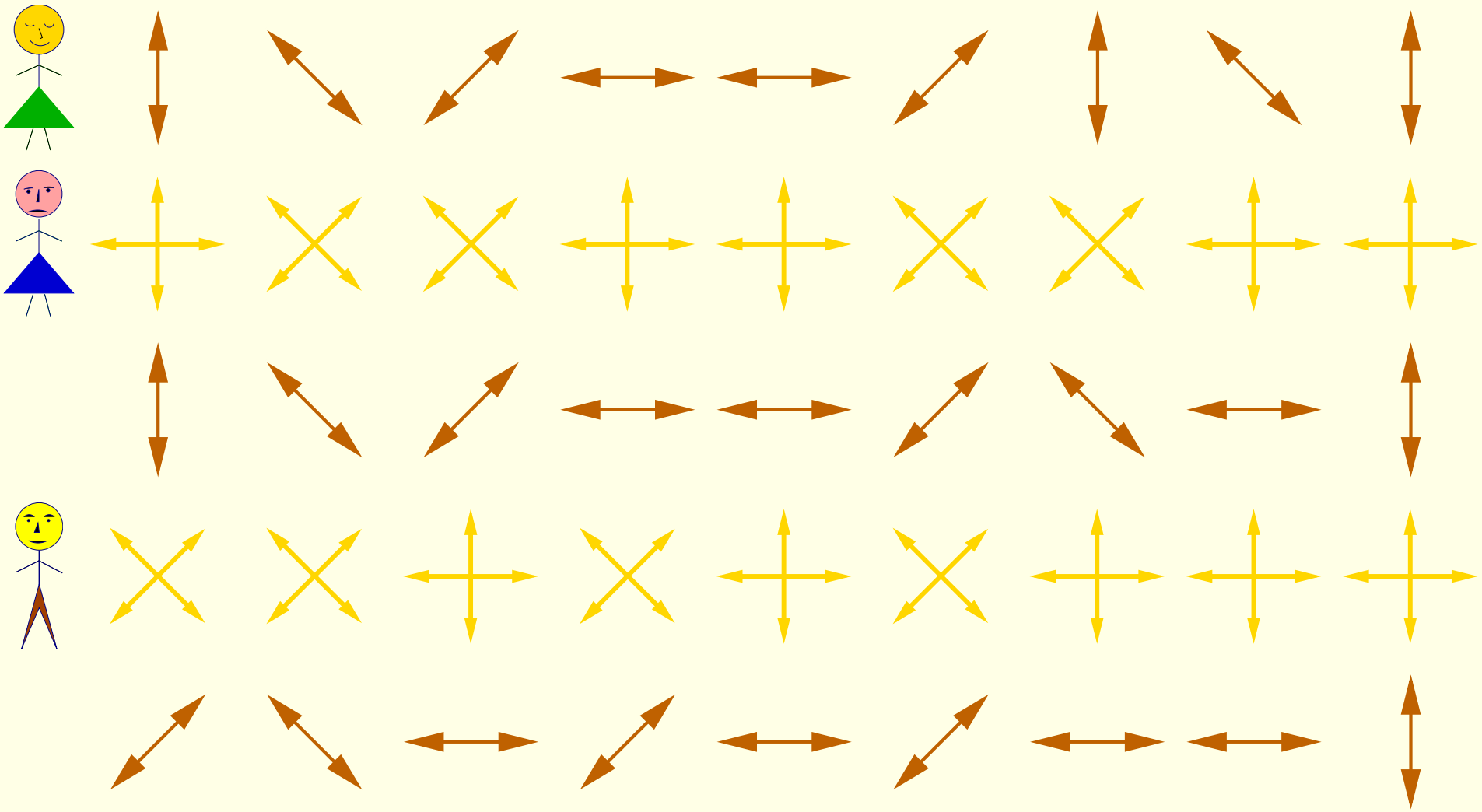









0 1 0 0 0 0 0 0 1



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

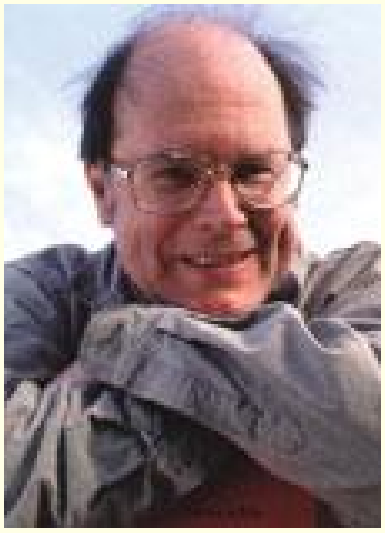
protokół oparty na EPR

- Istnieją inne protokoły kwantowe, np.

Artur Ekert

1991

protokół oparty na EPR



Charles Bennett

1992

protokół B92

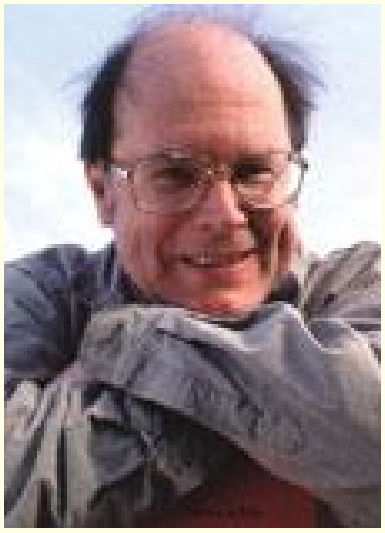
baza nieortogonalna

- Istnieją inne protokoły kwantowe, np.

Artur Ekert

1991

protokół oparty na EPR



Charles Bennett

1992

protokół B92

baza nieortogonalna

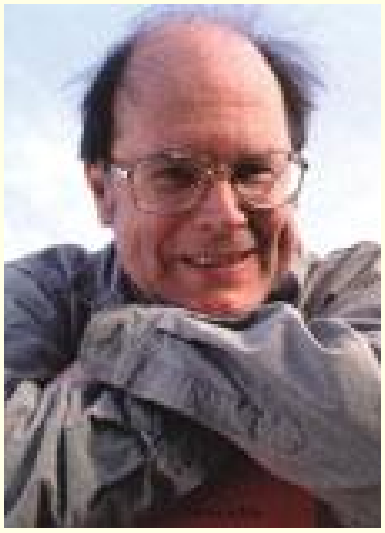
- Zamiast polaryzacji można używać fazy fotonów jako kubitów

- Istnieją inne protokoły kwantowe, np.

Artur Ekert

1991

protokół oparty na EPR



Charles Bennett

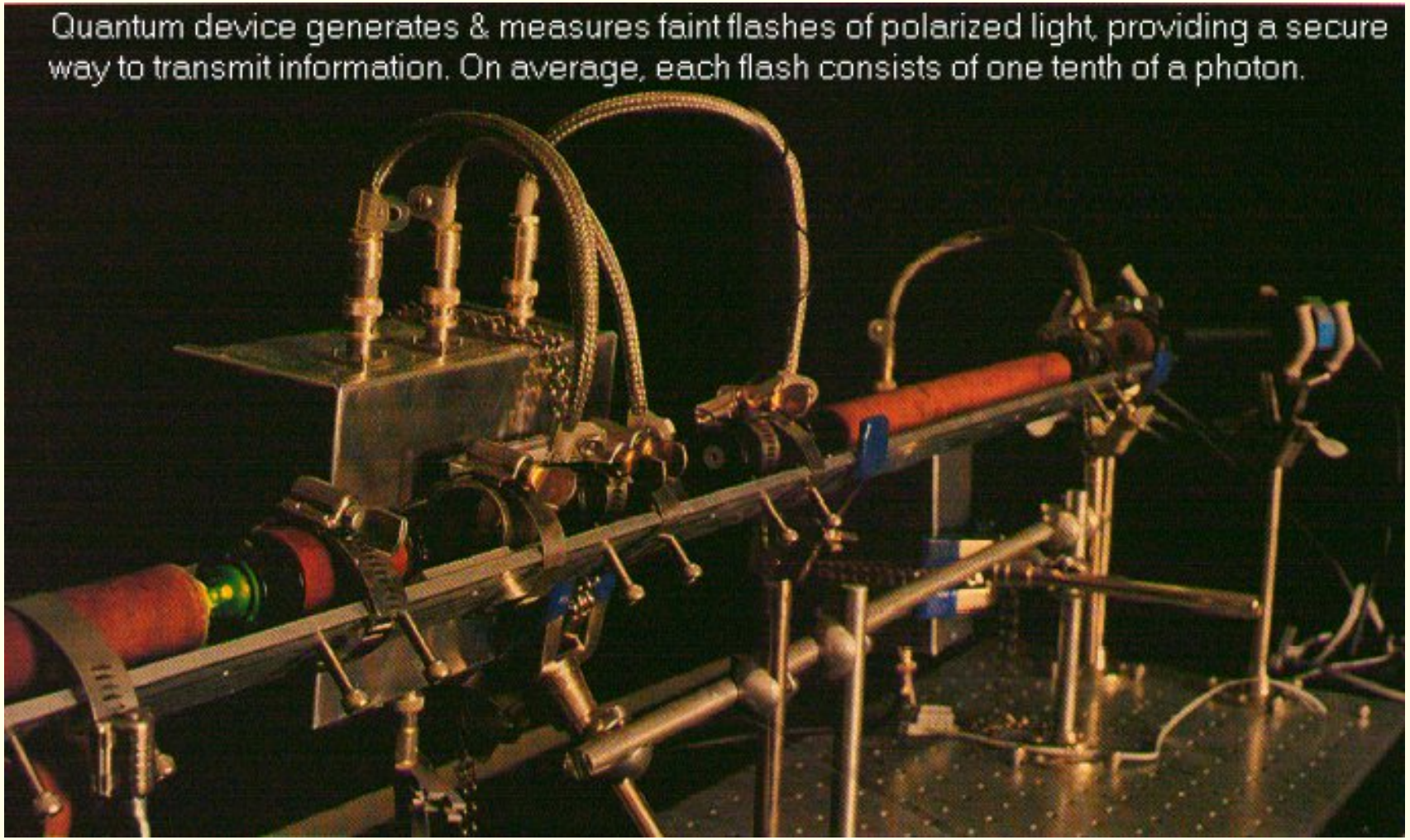
1992

protokół B92

baza nieortogonalna

- Zamiast polaryzacji można używać fazy fotonów jako kubitów
- Ciągle pojawiają się nowe propozycje!

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

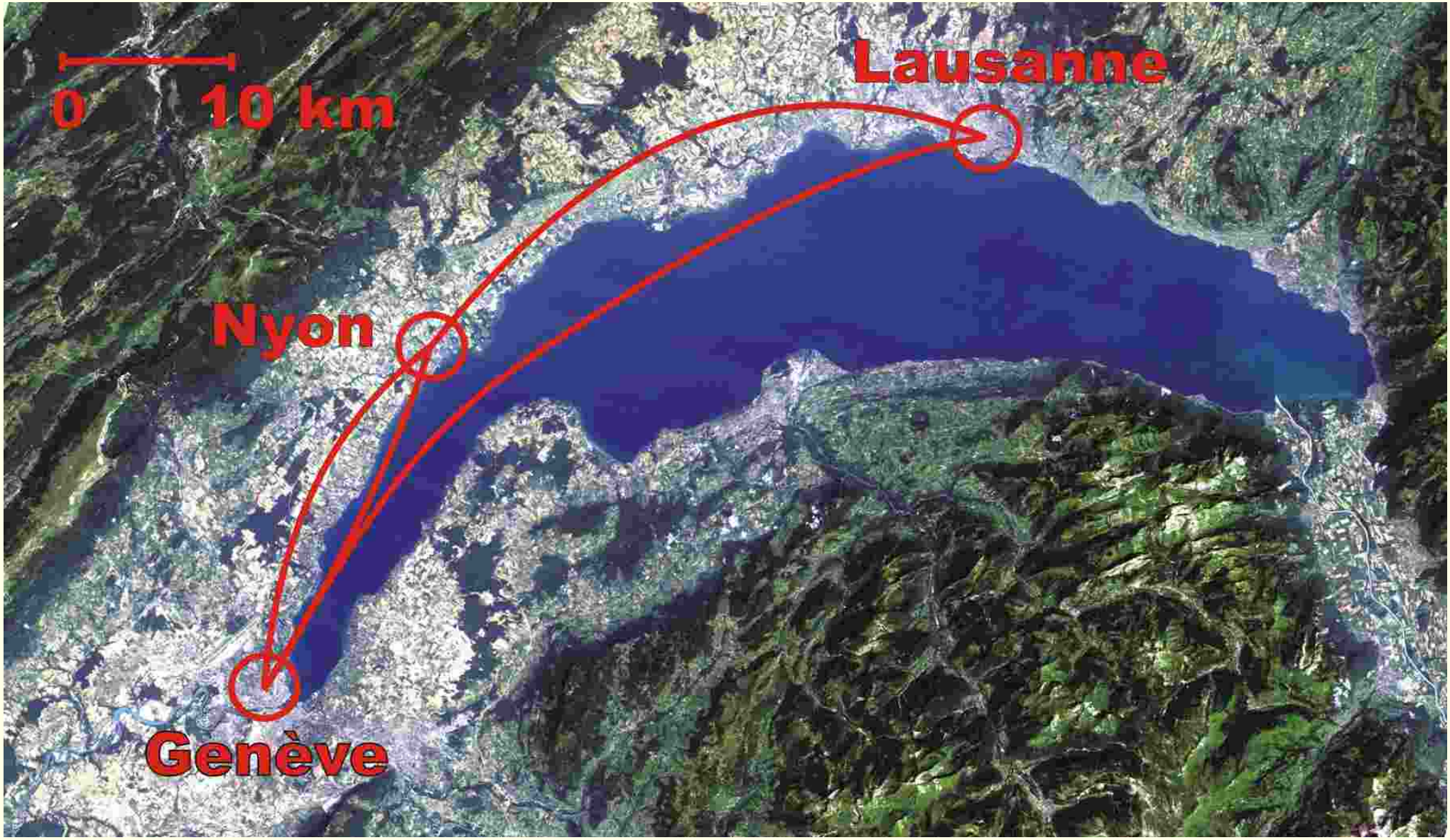
Nicolas Gisin

Group of Applied Physics

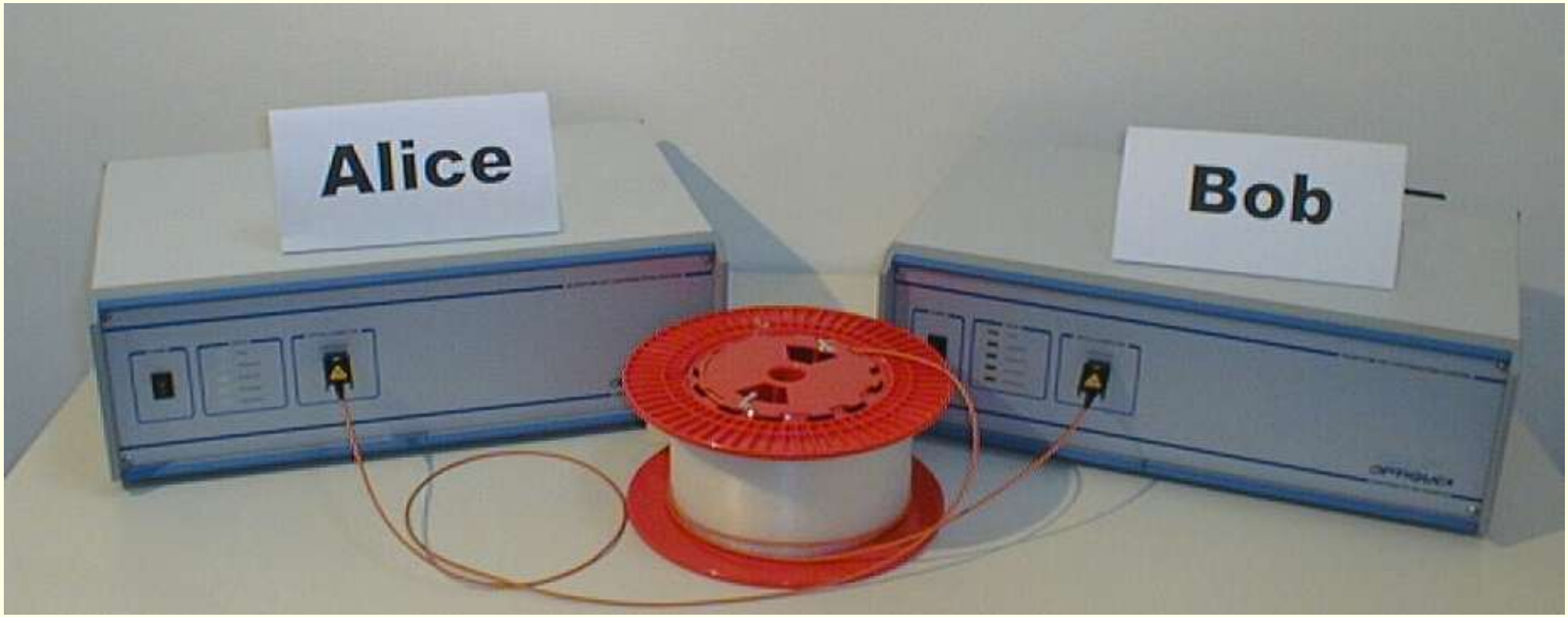
sekcja optyczna

Uniwersytet w Genewie

Eksperymenty kwantowe z wykorzystaniem komercyjnych światłowodów

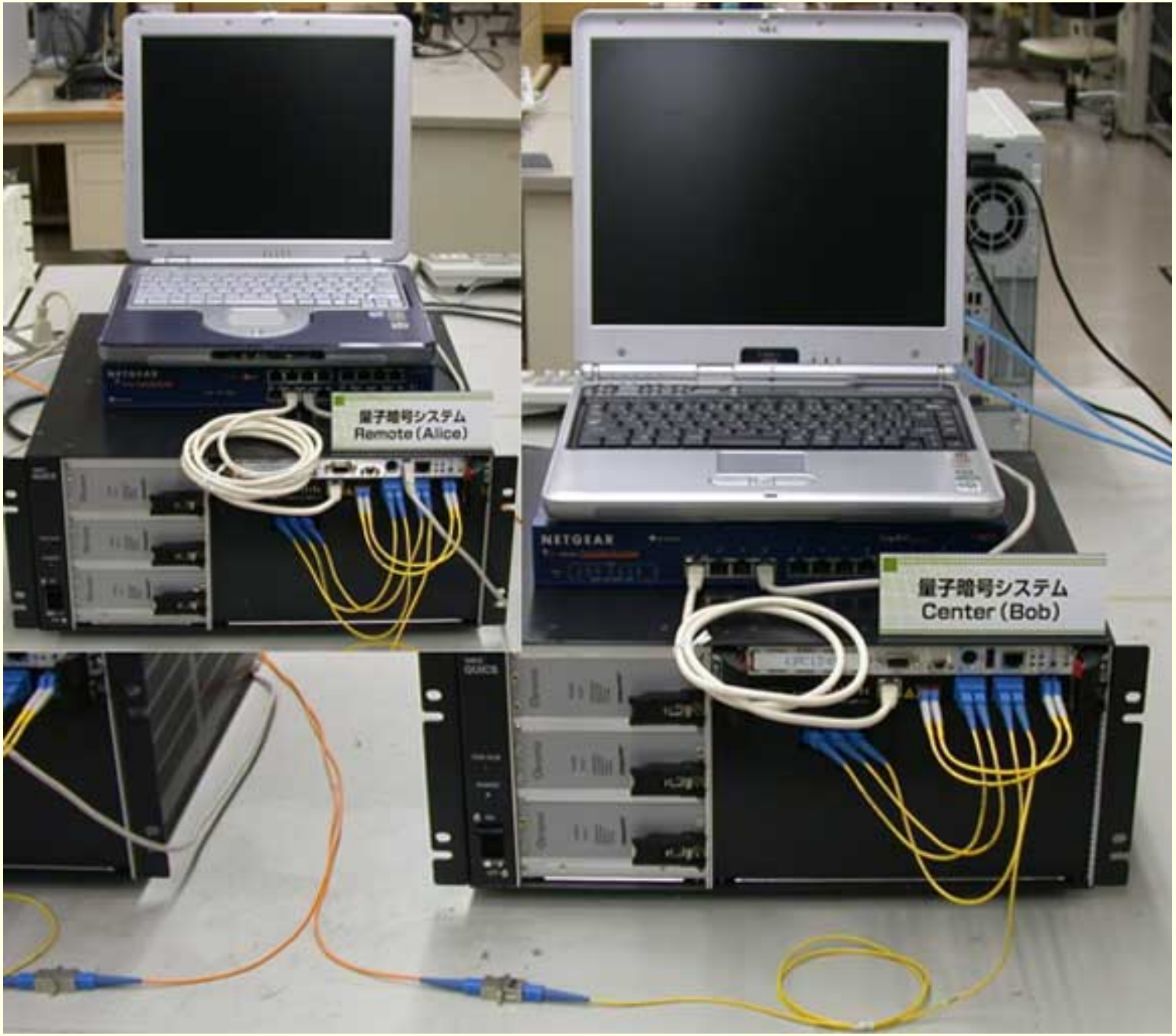


Genewa i okolice — miejsce eksperymentów kwantowych na odległościach kilkudziesięciu kilometrów w komercyjnych światłowodach, N. Gisin, W. Tittel i inni, 2000 ...



Komercyjny zestaw do kryptografii kwantowej produkowany przez firmę id Quantique w Szwajcarii

Anton Zeilinger demonstruje pierwszy czek przesłany z wykorzystaniem kryptografii kwantowej (21 kwietnia 2004)



Zestaw do kryptografii kwantowej firmy NEC

Zestaw do kryptografii kwantowej firmy Toshiba

Kryptografia kwantowa jest już produktem rynkowym!

- Przy połączeniach światłowodowych uzyskuje się odległości ponad 100 kilometrów
- W otwartej przestrzeni uzyskuje się odległości ponad 20 km.
- Istnieje kilka firm, które produkują urządzenia do kryptografii kwantowej.
- Uruchomiono pierwsze sieci z kwantową dystrybucją klucza.
- Wykonano pierwsze przekazy wideo szyfrowane kluczem kwantowym.
- Unia Europejska zainwestuje 11 mln € w ciągu 4 lat w system SECOQC (Secure Communication based on Quantum Cryptography)

Kryptografia kwantowa jest już produktem rynkowym!

- Przy połączeniach światłowodowych uzyskuje się odległości ponad 100 kilometrów
- W otwartej przestrzeni uzyskuje się odległości ponad 20 km.
- Istnieje kilka firm, które produkują urządzenia do kryptografii kwantowej.
- Uruchomiono pierwsze sieci z kwantową dystrybucją klucza.
- Wykonano pierwsze przekazy wideo szyfrowane kluczem kwantowym.
- Unia Europejska zainwestuje 11 mln € w ciągu 4 lat w system SECOQC (Secure Communication based on Quantum Cryptography)

Kryptografia kwantowa jest już produktem rynkowym!

- Przy połączeniach światłowodowych uzyskuje się odległości ponad 100 kilometrów
- W otwartej przestrzeni uzyskuje się odległości ponad 20 km.
- Istnieje kilka firm, które produkują urządzenia do kryptografii kwantowej.
- Uruchomiono pierwsze sieci z kwantową dystrybucją klucza.
- Wykonano pierwsze przekazy wideo szyfrowane kluczem kwantowym.
- Unia Europejska zainwestuje 11 mln € w ciągu 4 lat w system SECOQC (Secure Communication based on Quantum Cryptography)

Kryptografia kwantowa jest już produktem rynkowym!

- Przy połączeniach światłowodowych uzyskuje się odległości ponad 100 kilometrów
- W otwartej przestrzeni uzyskuje się odległości ponad 20 km.
- Istnieje kilka firm, które produkują urządzenia do kryptografii kwantowej.
- Uruchomiono pierwsze sieci z kwantową dystrybucją klucza.
- Wykonano pierwsze przekazy wideo szyfrowane kluczem kwantowym.
- Unia Europejska zainwestuje 11 mln € w ciągu 4 lat w system SECOQC (Secure Communication based on Quantum Cryptography)

Kryptografia kwantowa jest już produktem rynkowym!

- Przy połączeniach światłowodowych uzyskuje się odległości ponad 100 kilometrów
- W otwartej przestrzeni uzyskuje się odległości ponad 20 km.
- Istnieje kilka firm, które produkują urządzenia do kryptografii kwantowej.
- Uruchomiono pierwsze sieci z kwantową dystrybucją klucza.
- Wykonano pierwsze przekazy wideo szyfrowane kluczem kwantowym.
- Unia Europejska zainwestuje 11 mln € w ciągu 4 lat w system SECOQC (Secure Communication based on Quantum Cryptography)

Kryptografia kwantowa jest już produktem rynkowym!

- Przy połączeniach światłowodowych uzyskuje się odległości ponad 100 kilometrów
- W otwartej przestrzeni uzyskuje się odległości ponad 20 km.
- Istnieje kilka firm, które produkują urządzenia do kryptografii kwantowej.
- Uruchomiono pierwsze sieci z kwantową dystrybucją klucza.
- Wykonano pierwsze przekazy wideo szyfrowane kluczem kwantowym.
- Unia Europejska zainwestuje 11 mln € w ciągu 4 lat w system SECOQC (Secure Communication based on Quantum Cryptography)

Kryptografia kwantowa jest już produktem rynkowym!

- Przy połączeniach światłowodowych uzyskuje się odległości ponad 100 kilometrów
- W otwartej przestrzeni uzyskuje się odległości ponad 20 km.
- Istnieje kilka firm, które produkują urządzenia do kryptografii kwantowej.
- Uruchomiono pierwsze sieci z kwantową dystrybucją klucza.
- Wykonano pierwsze przekazy wideo szyfrowane kluczem kwantowym.
- Unia Europejska zainwestuje 11 mln € w ciągu 4 lat w system SECOQC (Secure Communication based on Quantum Cryptography)

Wiek XXI to wiek technologii kwantowej!

Wiek XXI to wiek technologii kwantowej!

Uczcie się optyki kwantowej!

Wiek XXI to wiek technologii kwantowej!

Uczcie się optyki kwantowej!

Będziecie potrzebni!