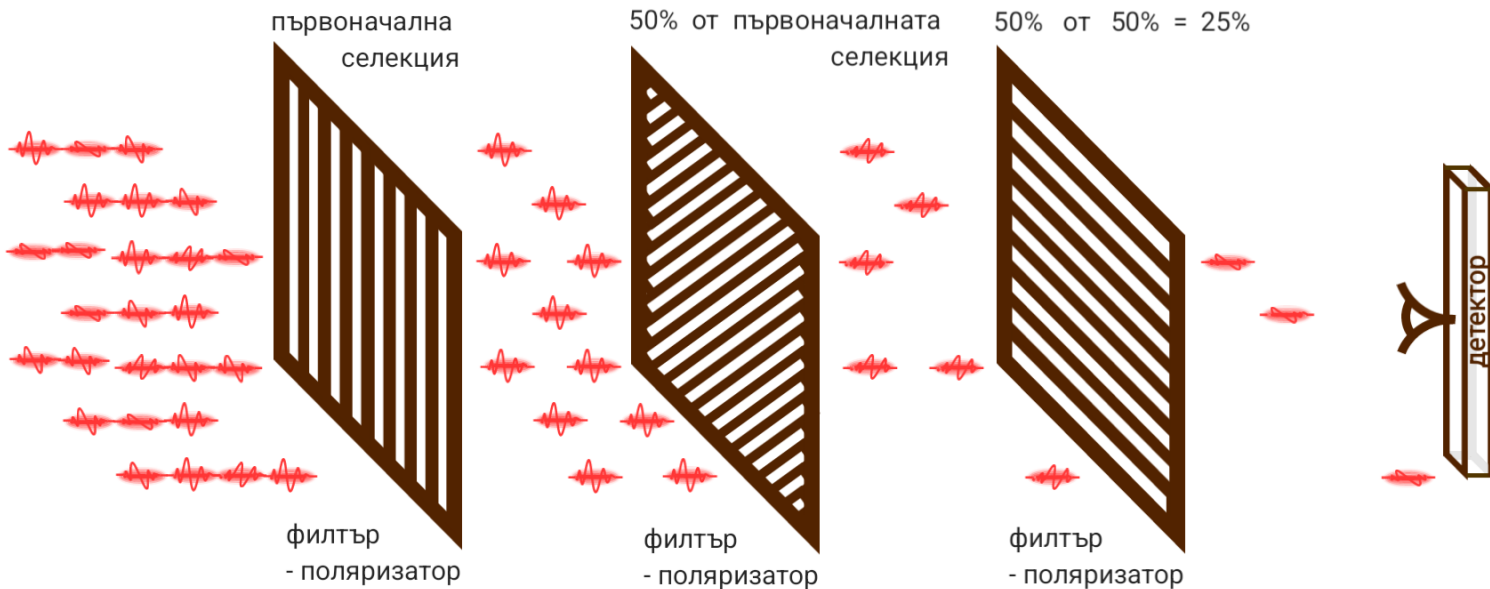
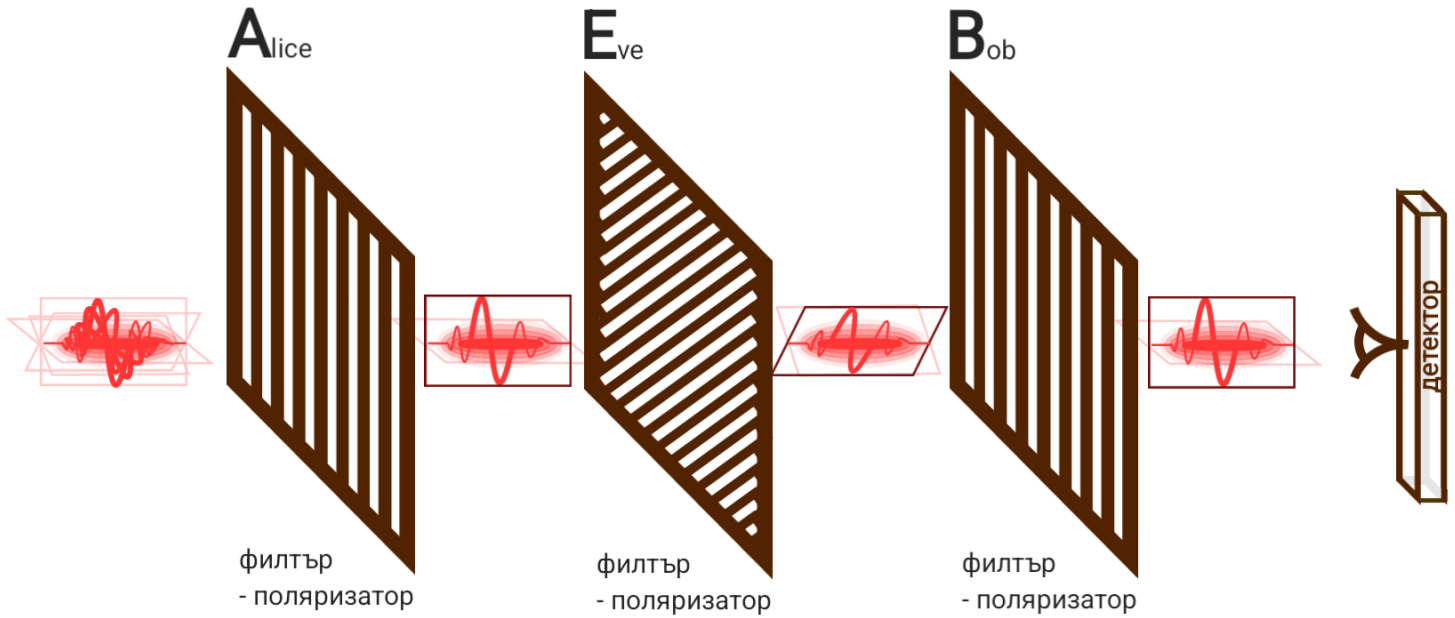


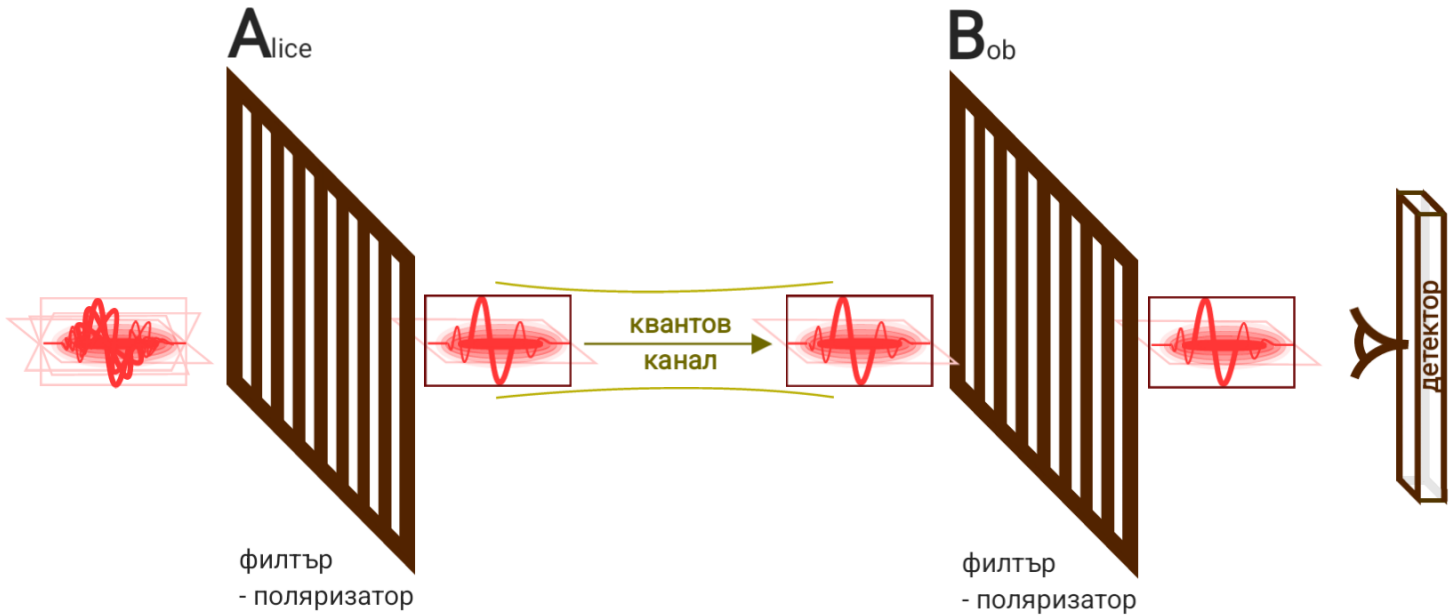
ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"



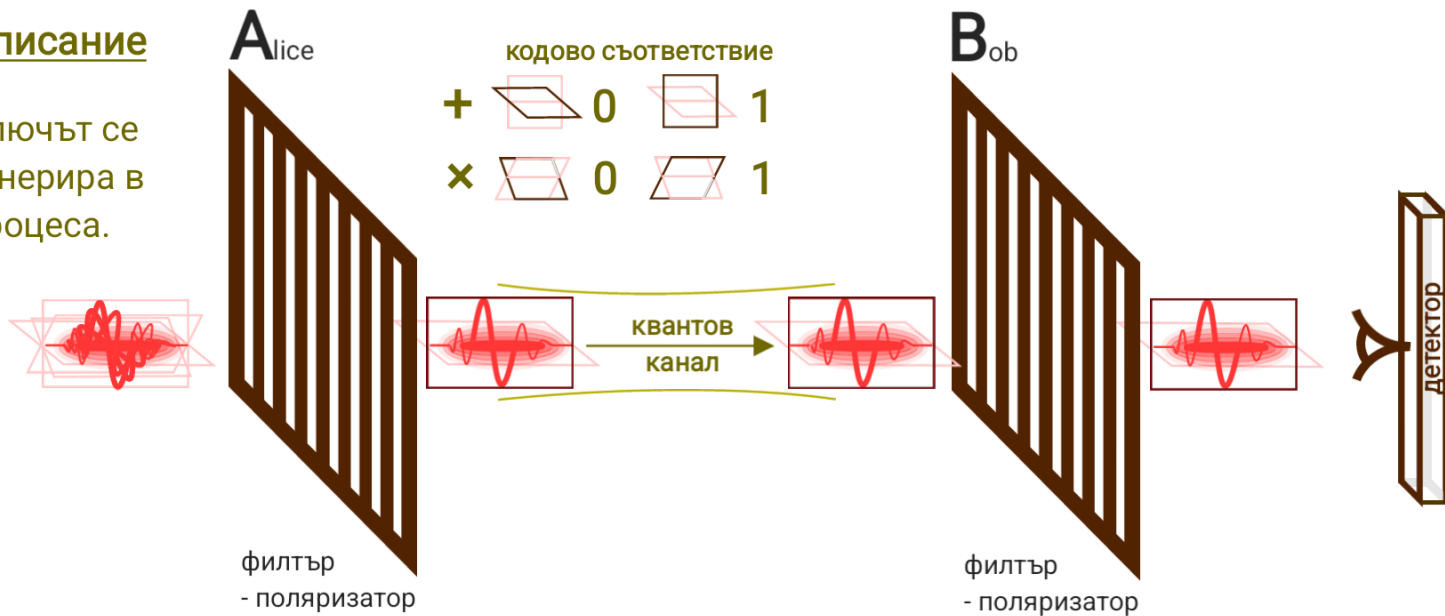
ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

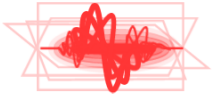
Ключът се генерира в процеса.



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



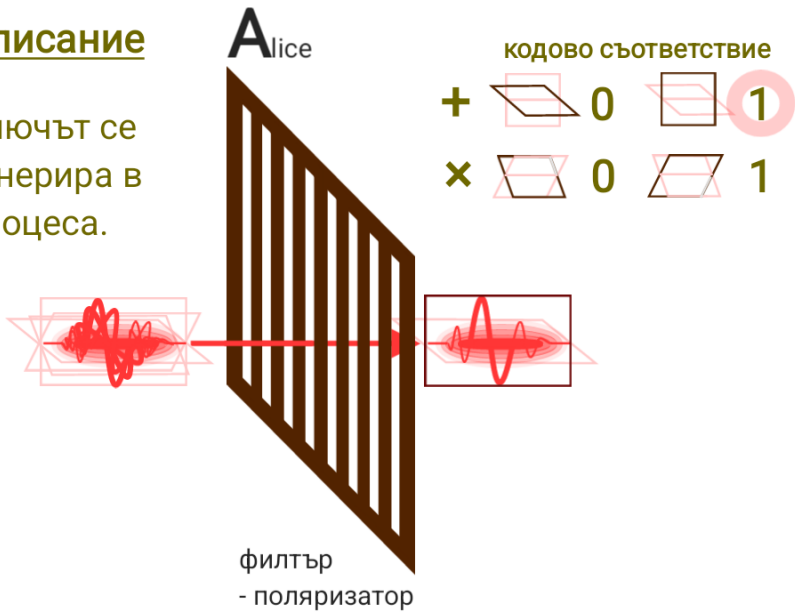
кодово съответствие

+		0		1
x		0		1

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

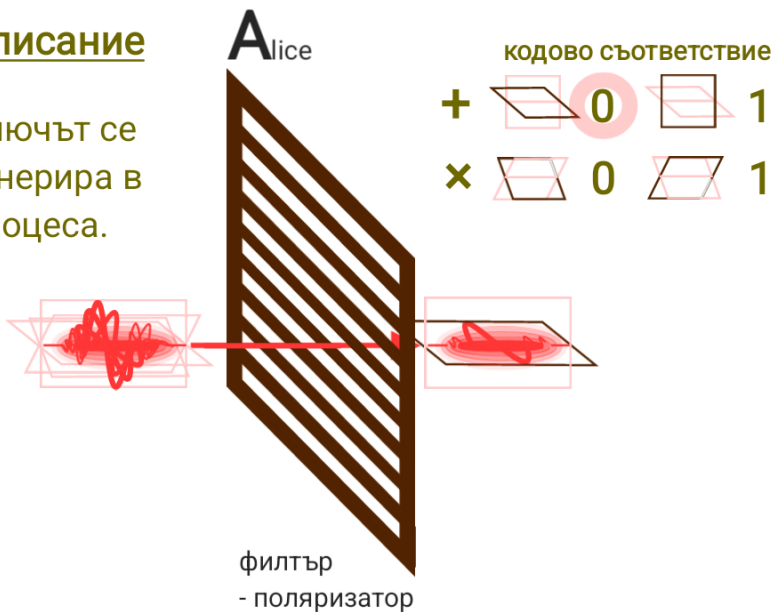
Ключът се генерира в процеса.



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

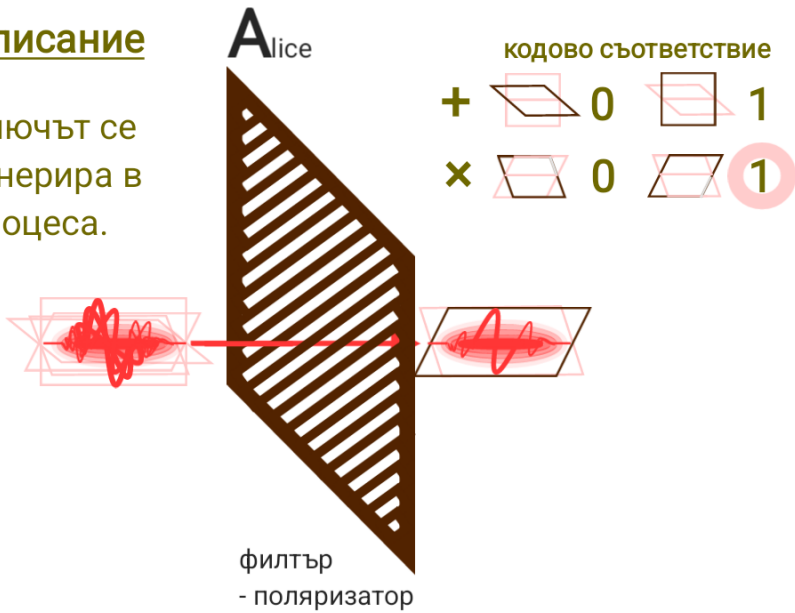
Ключът се генерира в процеса.



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

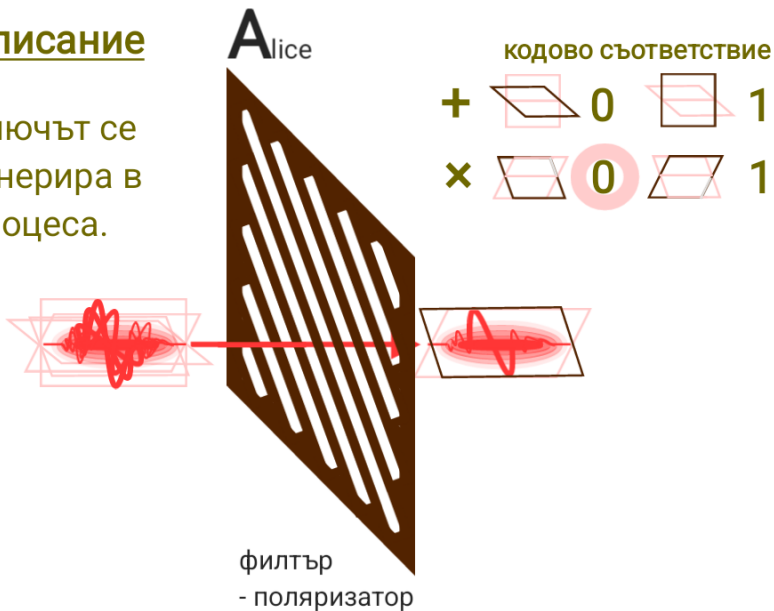
Ключът се генерира в процеса.



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

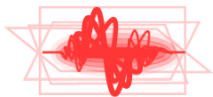
Ключът се генерира в процеса.



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Alice



филтър
- поляризатор

кодово съответствие



Bob



филтър
- поляризатор



Стъпка 1

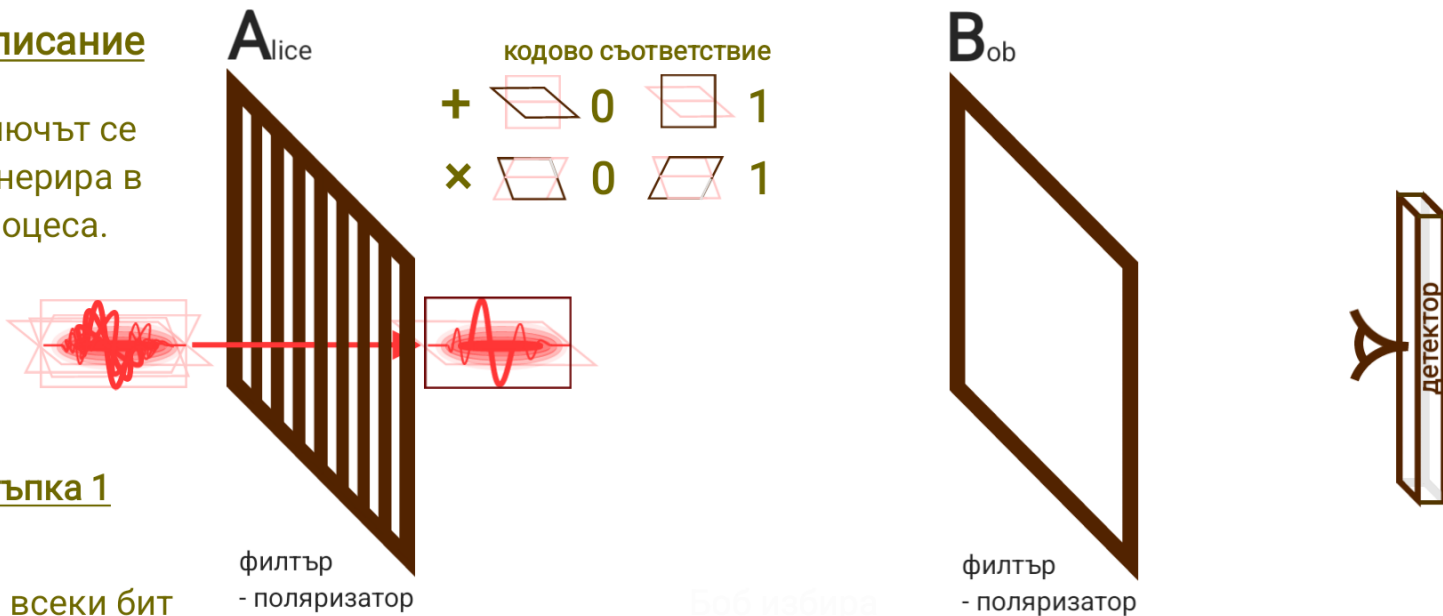
За всеки бит

Алис избира: базис +/x
и филтър
(кодвия символ)

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 1

За всеки бит

Алис избира: базис +/×
и филтър
(кодovia символ)

+ + × + × +
1 0 1 1 0 1

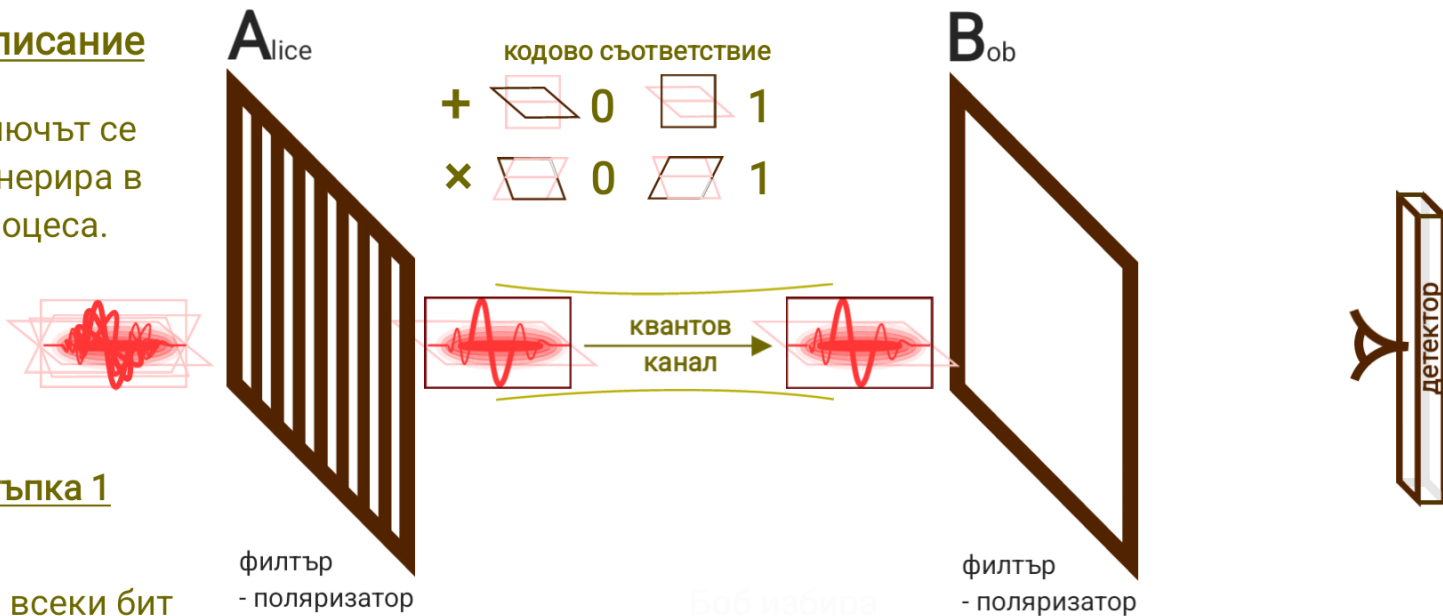
Боб избира
измерване
и получава

филтър
- поляризатор
+ + × + × +
1 0 1 1 0 1

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 1

За всеки бит

Алис избира: базис +/x
и филтър
(кодovия символ)

+ + x + x +
1 0 1 1 0 1

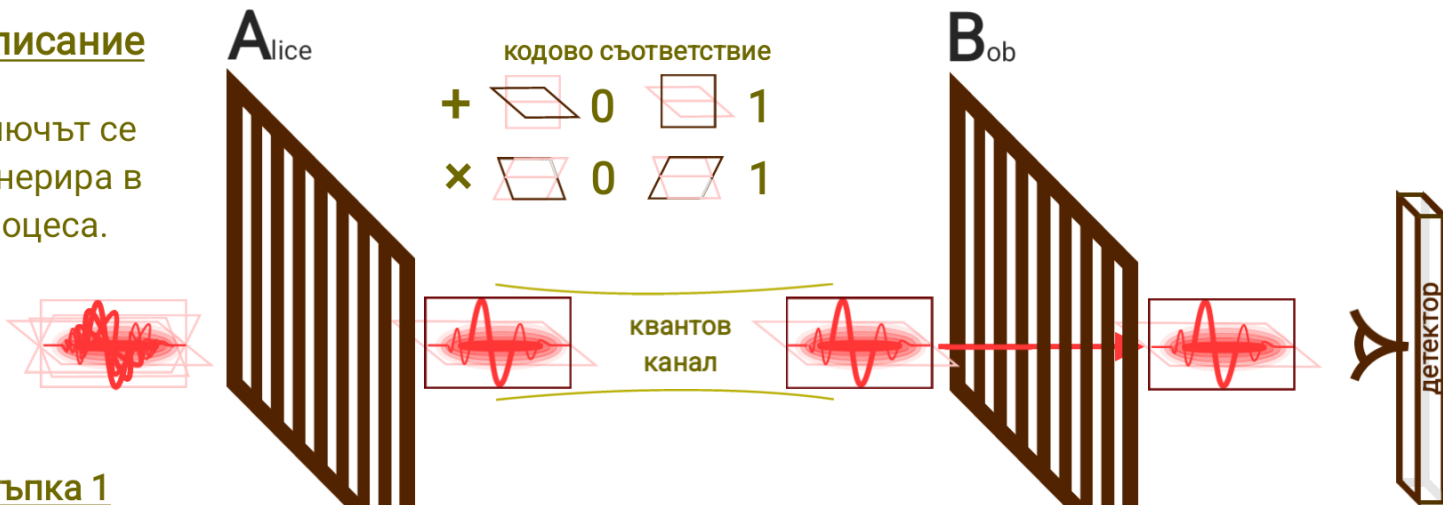
Боб избира
измерване
и получава

филтър - поляризатор
+ + x + x +
1 0 1 1 0 1

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 1

За всеки бит

Алис избира: базис +/x
и филтър
(кодovия символ)

филтър
- поляризатор

+ + x + x +
1 0 1 1 0 1

Боб избира
измерване
и получава

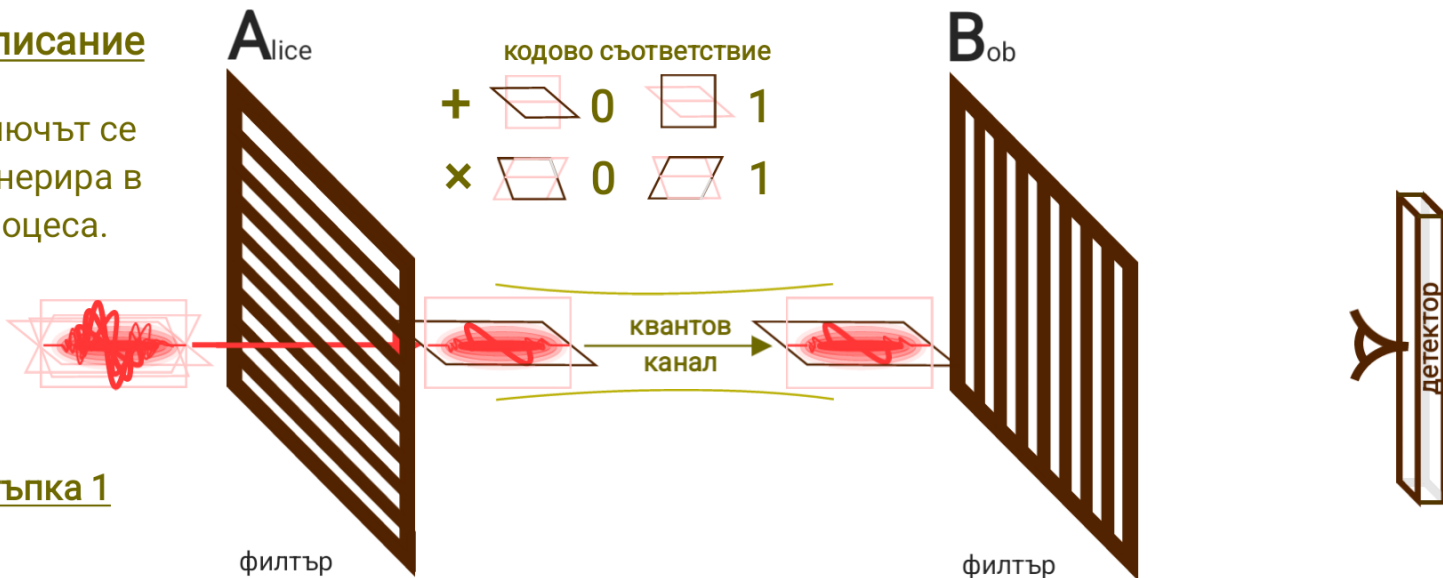
филтър
- поляризатор

+ + x + x +
1 0 1 1 0 1

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 1

За всеки бит

Алис избира: базис +/x
и филтър
(кодoвия символ)

филтър
- поляризатор

++	+x	x+	xx
10	101	101	101

Боб избира
измерване
и получава

филтър
- поляризатор

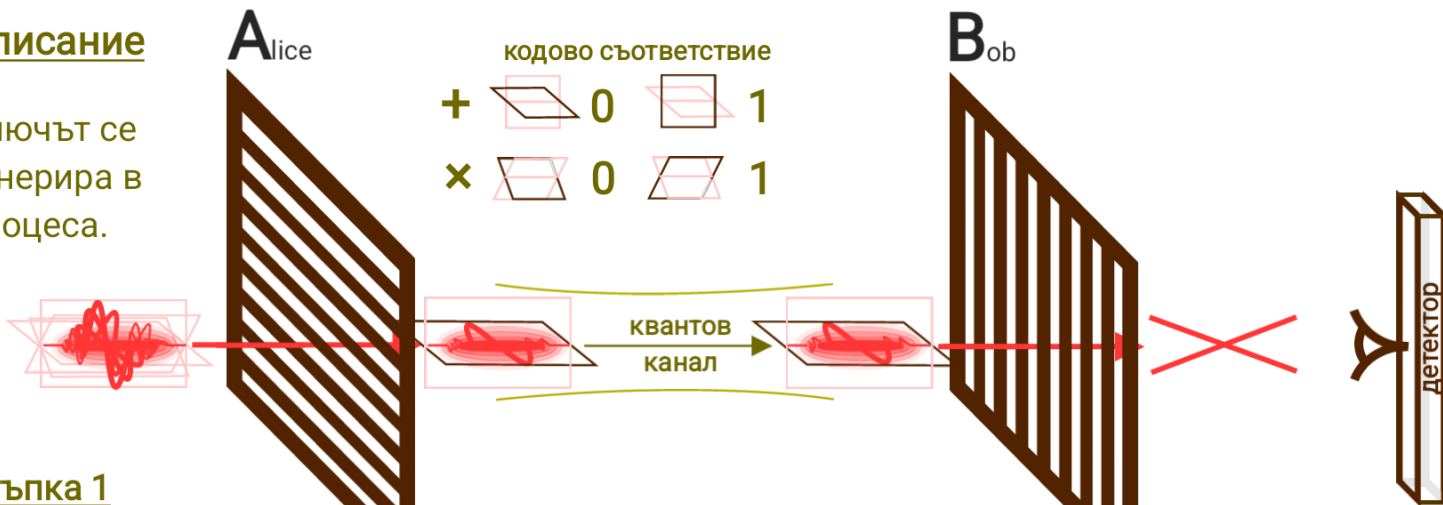
++	+x	x+	xx
10	101	101	101



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 1

За всеки бит

Алис избира: базис +/x
и филтър
(кодovия символ)

филтър
- поляризатор

++ +x+
10 101

Боб избира
измерване
и получава

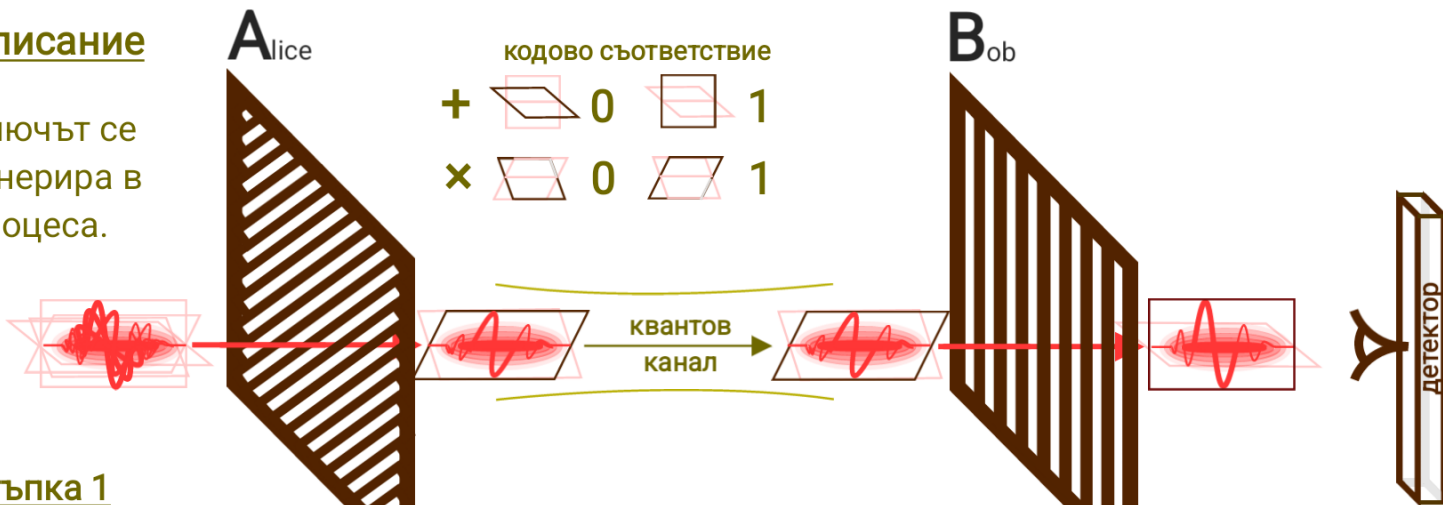
филтър
- поляризатор

++ +x+
10 1101

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 1

За всеки бит

Алис избира: базис +/x
и филтър
(кодoвия символ)

филтър
- поляризатор

++ x -- x
1 0 1 1 0 1

Боб избира
измерване
и получава

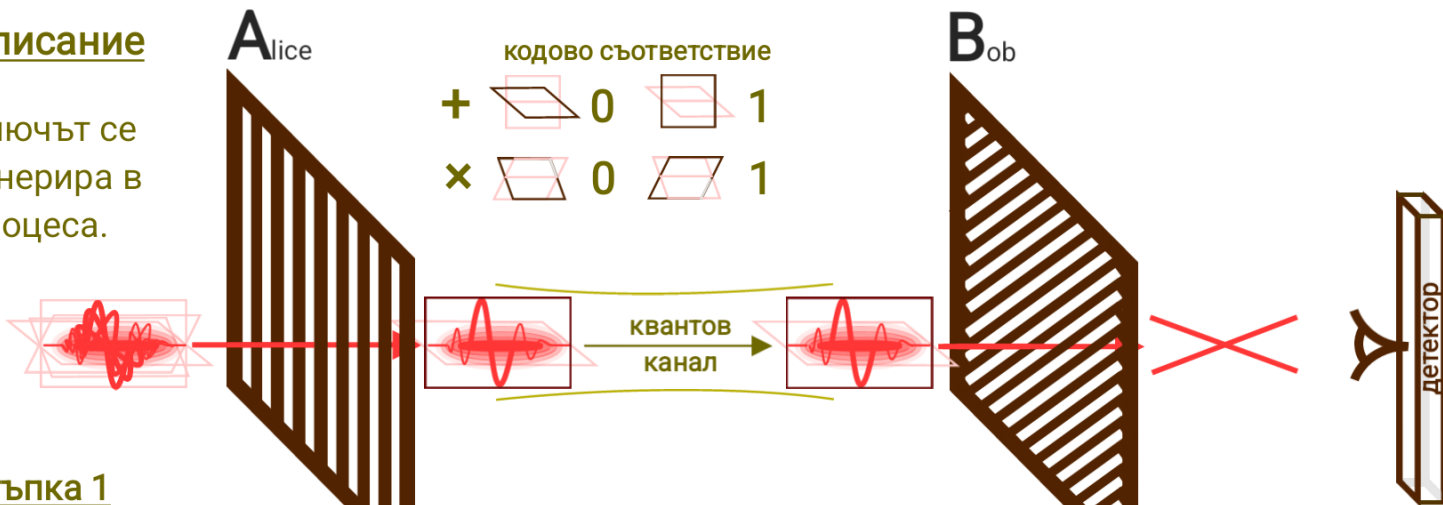
филтър
- поляризатор

+++ -- x
1 0 1 0 0 1

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 1

За всеки бит

Алис избира: базис +/x
и филтър
(кодoвия символ)

филтър
- поляризатор

++ x+ x-
1 0 1 1 0 1

Боб избира
измерване
и получава

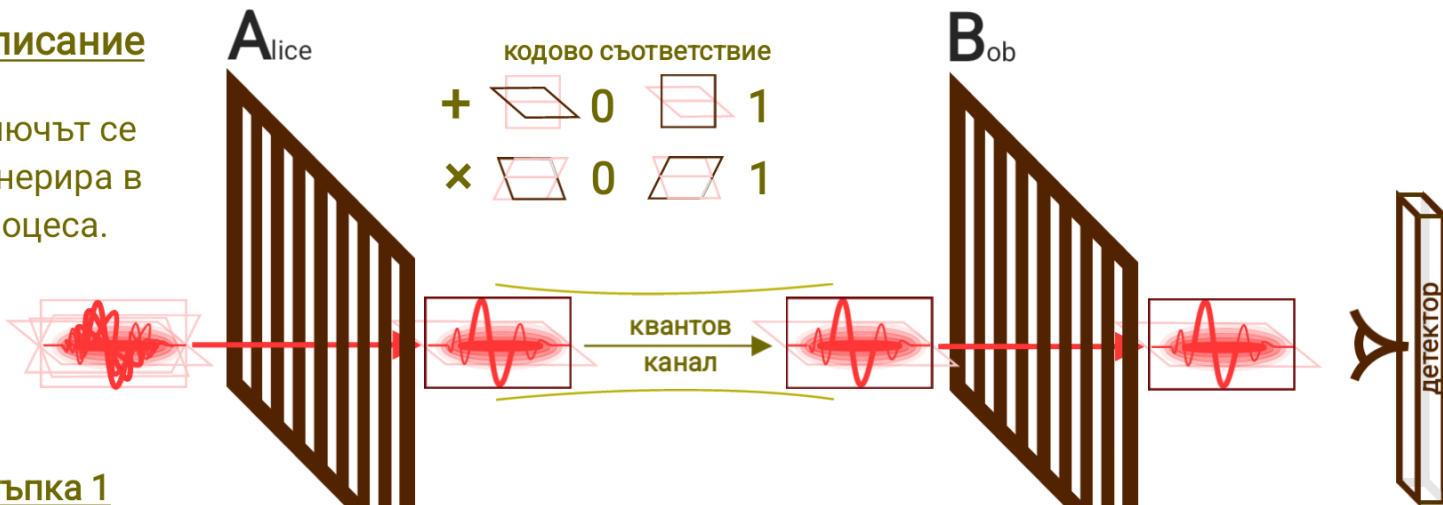
филтър
- поляризатор

+++ x- x-
1 0 1 0 1 1

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 1

За всеки бит

Алис избира: базис +/x
и филтър
(кодovия символ)

филтър
- поляризатор

++ x + x
1 0 1 1 0

Боб избира
измерване
и получава

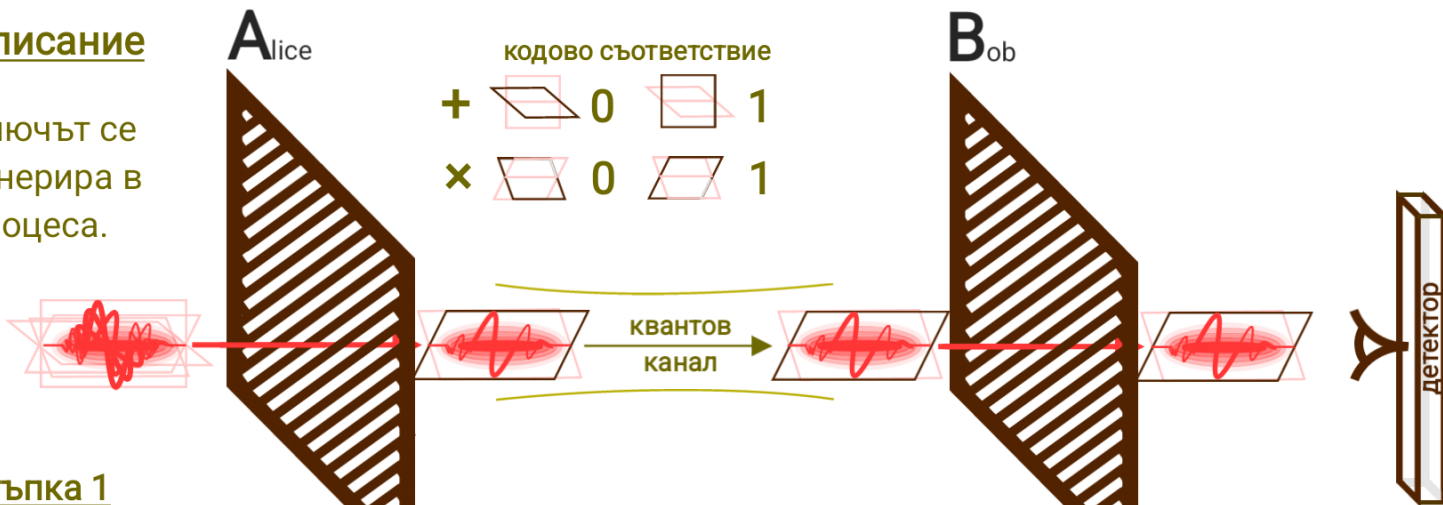
филтър
- поляризатор

++ + x +
1 0 1 0 0

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "B_{ennett} B_{rassard}-1984"

Описание

Ключът се генерира в процеса.



Стъпка 1

За всеки бит

Алис избира: базис +/x
и филтър
(кодoвия символ)

филтър
- поляризатор

++ x + x x
1 0 1 1 0 1

Боб избира
измерване
и получава

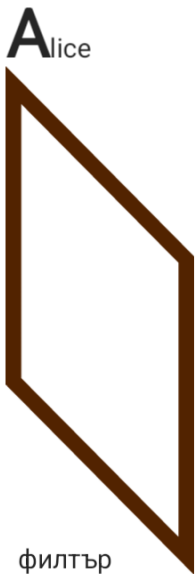
филтър
- поляризатор

++ + x + x
1 0 1 0 0 1

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Аlice
фильтър - поляризатор

кодово съответствие

+		0		1
x		0		1



Bob
фильтър - поляризатор



детектор

Стъпка 2

сравняване по публичен канал и пресяване

++ x + x x

1 0 1 1 0 1

++ + x + x

1 0 1 0 0 1

За всеки бит

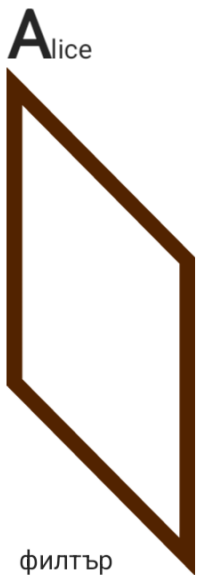
Алис избира базис +/x и филтър (кодovия символ)

Боб избира измерване и получава

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.

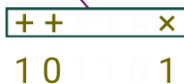


Аlice
филтър - поляризатор



Bob
филтър - поляризатор

сравняване по публичен канал и пресяване



Стъпка 2

За всеки бит

Алис избира базис +/x и филтър (кодovия символ)

Боб избира

измерване и получава

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.

Alice



филтър
- поляризатор

кодово съответствие



Bob



филтър
- поляризатор



детектор

сравняване по публичен канал
и пресяване

За всеки бит

Алис избира

Резултат:

пресят ключ:

1 0 1

(кодovия символ)

Боб избира

измерване

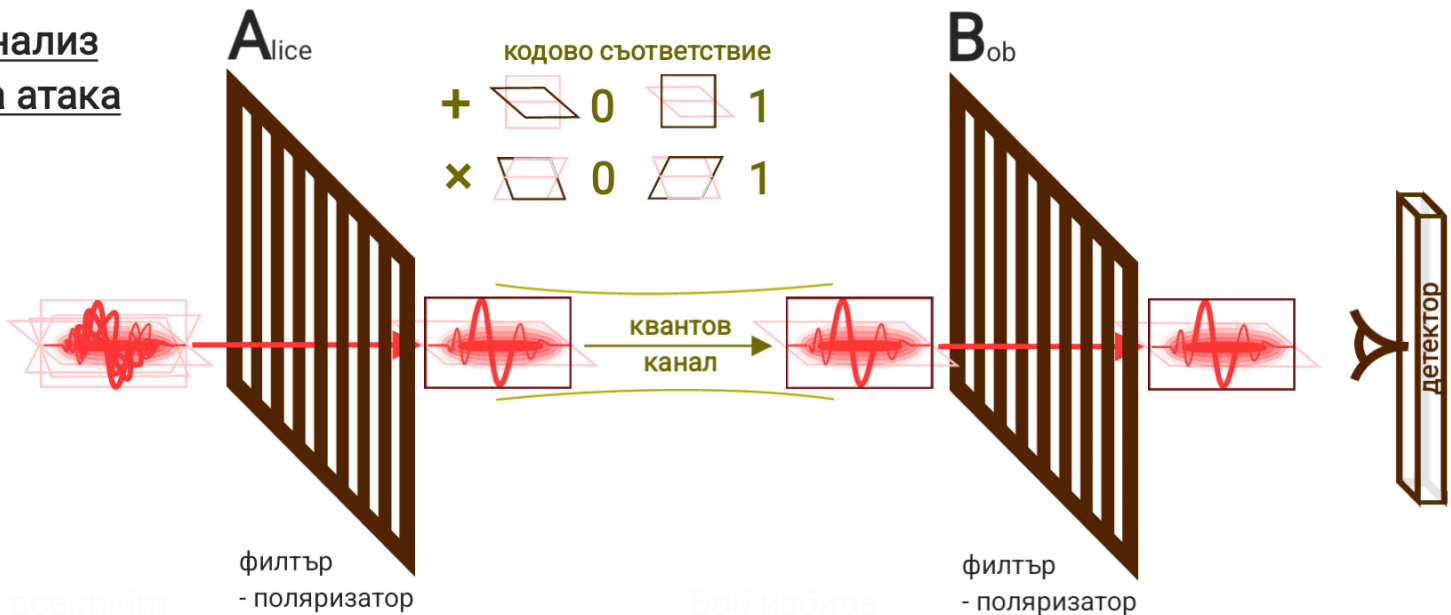
и получава

1 0 1

100% съвпадение при липса на вмшательство

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ на атака



За всеки бит

Алис избира базис +/x и филтър (кодovия символ)

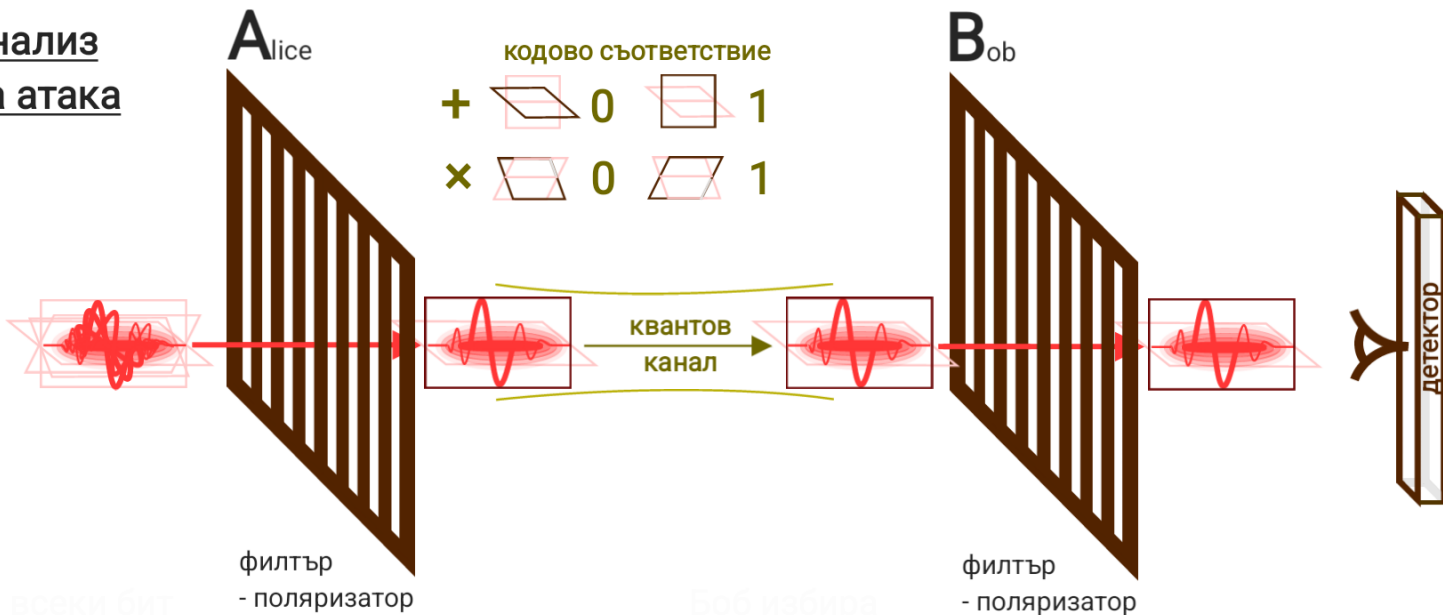
++ x+ x+
10 11 01

Боб избира измерване и получава

++ +x +x
10 10 01

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ на атака



За всеки бит

Алис избира: базис +/x и филтър (кодovия символ)

A: +
1 0 1 1 0 1

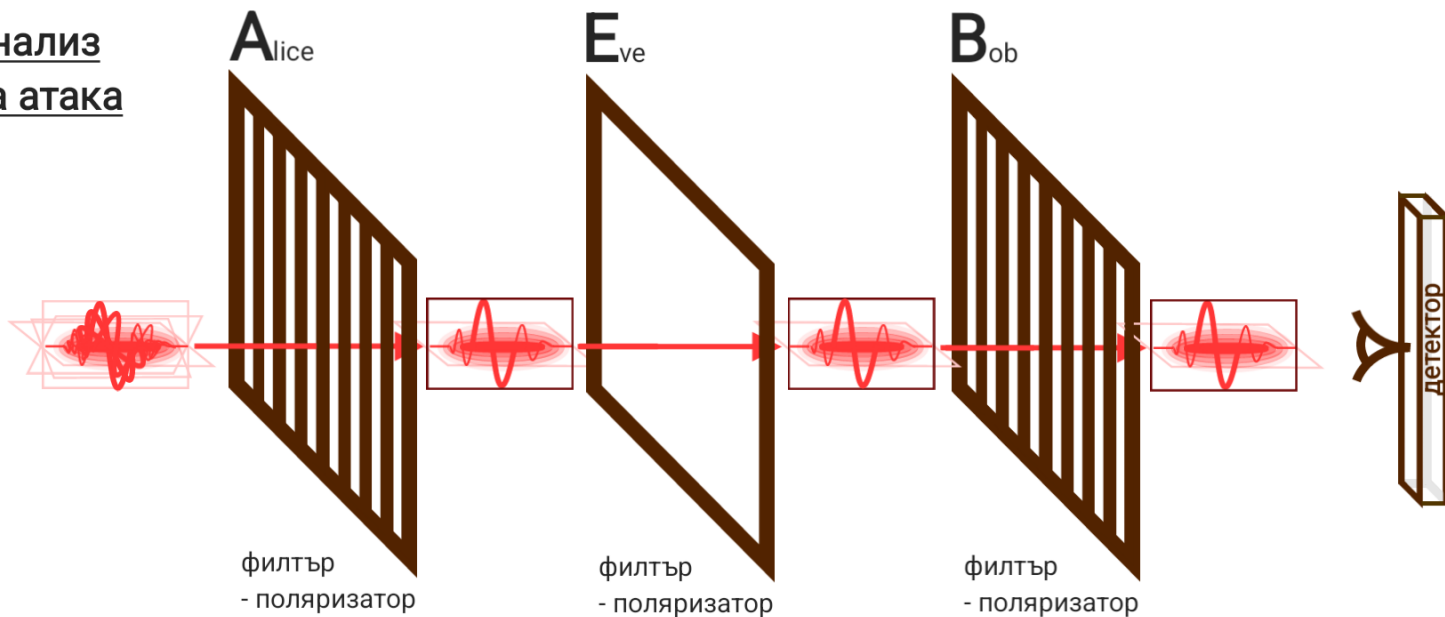
Боб избира

измерване и получава

B: +
1 0 1 0 0 1

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ
на атака



и
Алис избира: базис +/x
и филтър
(кодovия символ)

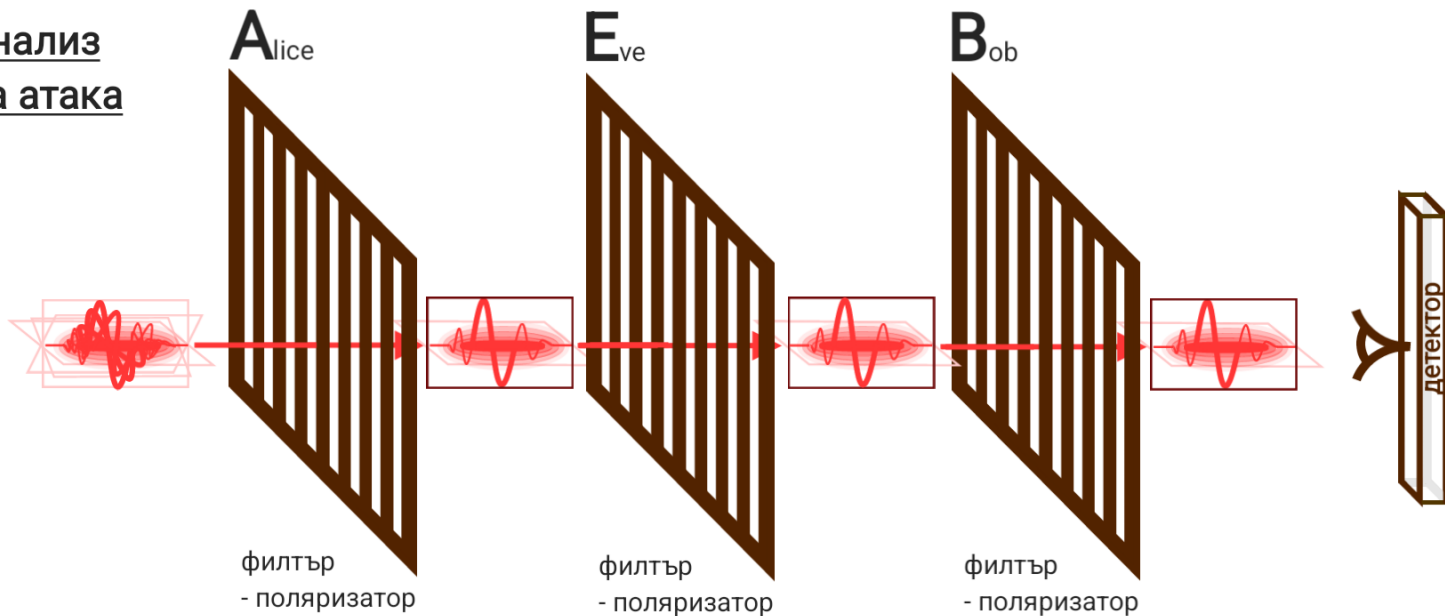
A: +
1 0 1 1 0 1

x
и тролучава

B: +
1 0 1 0 0 1

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ
на атака



и
Алис избира: базис $+/x$
и филтър
(кодovia символ)

A: +

1 0 1 1 0 1

E: + \rightarrow 50%

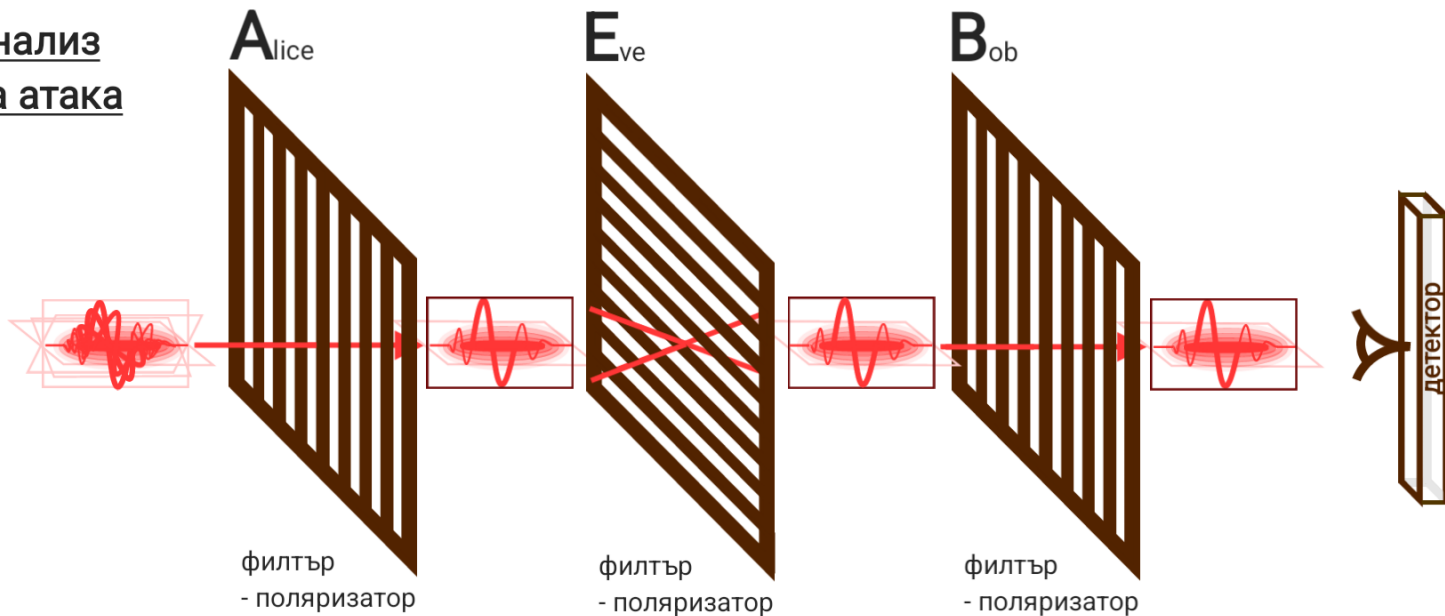
1/0

B: +

1 0 1 0 0 1

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ
на атака



фильтър
- поляризатор

фильтър
- поляризатор

фильтър
- поляризатор

детектор

и
Алис избира: базис +/x
и филтър
(кодovia символ)

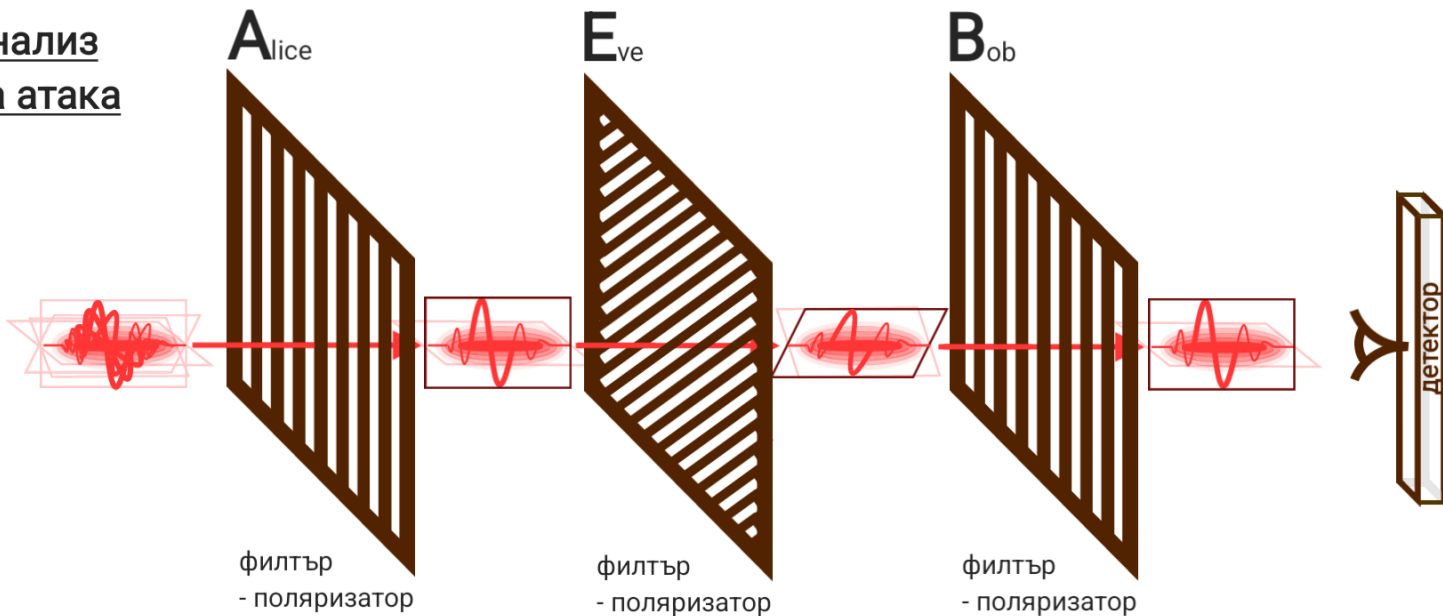
A: +
1 0 1 1 0 1

E: + -> 50%
1/0

B: +
1 0 1 0 0 1

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ на атака



и
 Алис избира базис +/x
 и филтър
 (кодovia символ)

A: +

1 0 1 1 0 1

E: x -> 50%

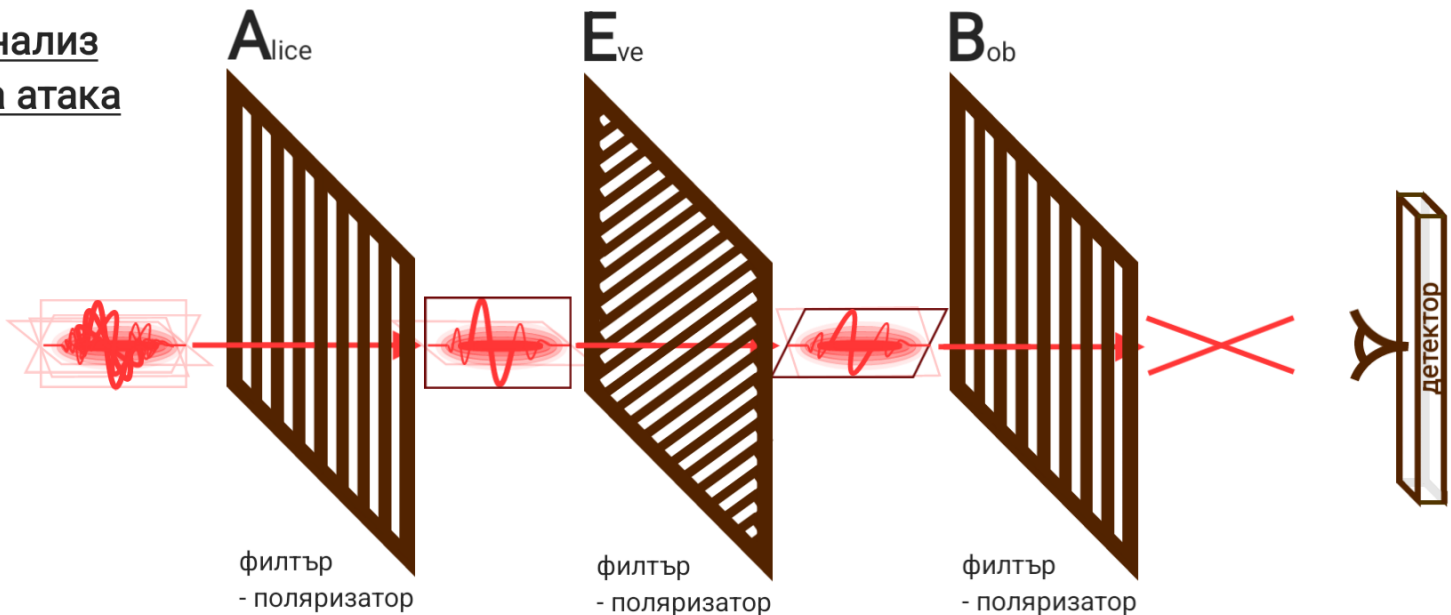
1/0

B: +

1 -> 25%

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ на атака



фильтър - поляризатор

фильтър - поляризатор

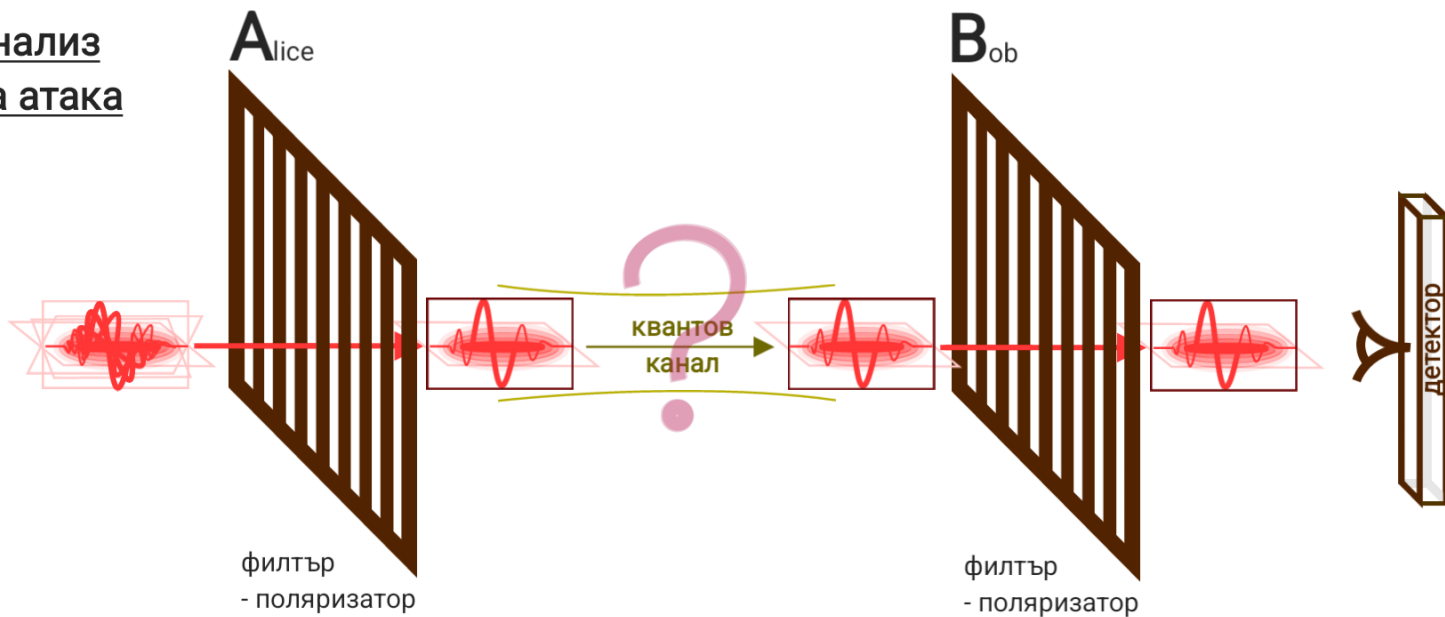
фильтър - поляризатор

детектор

и
 Алис избира: базис +/x **A: +** **E: x** -> 50% **B: +**
 и филтър 1 0 1 1 0 1 1/0 0 -> 25% **РАЗКРИТА АТАКА**
 (кодovia символ)

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ
на атака



Извод: ако грешките в пресетия ключ надхвърлят 25%, то това е индикация за подслушване