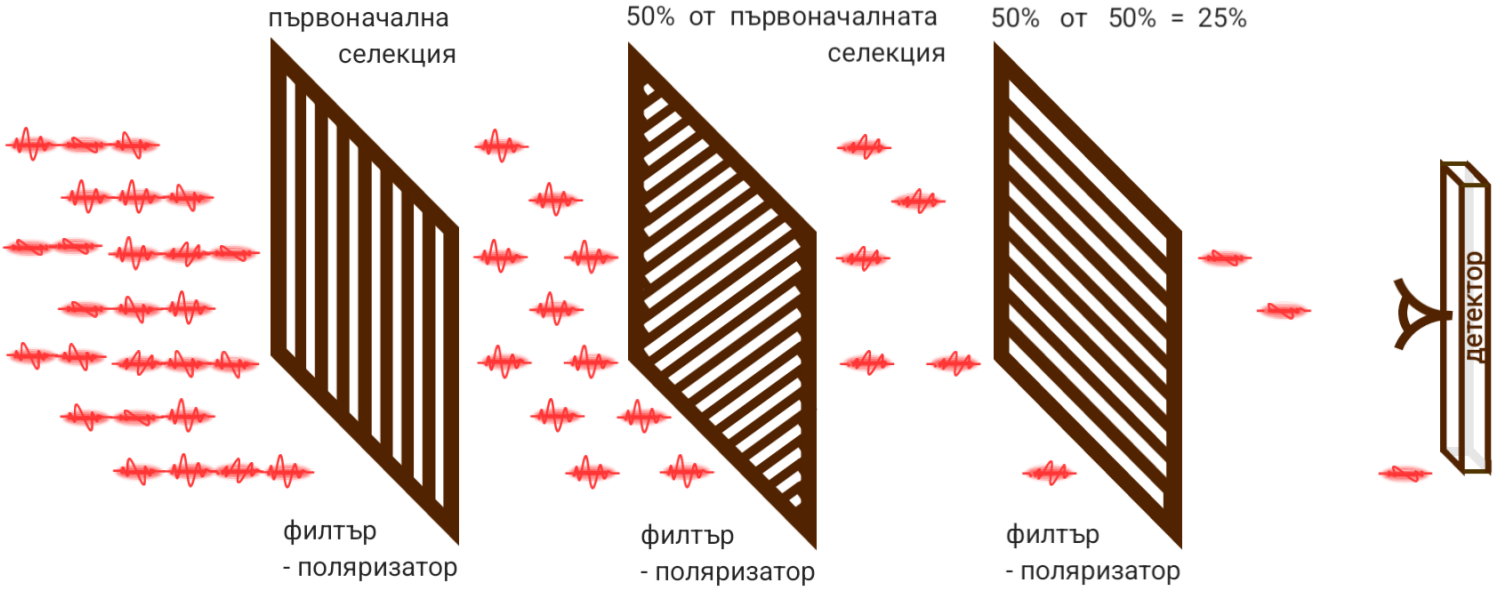
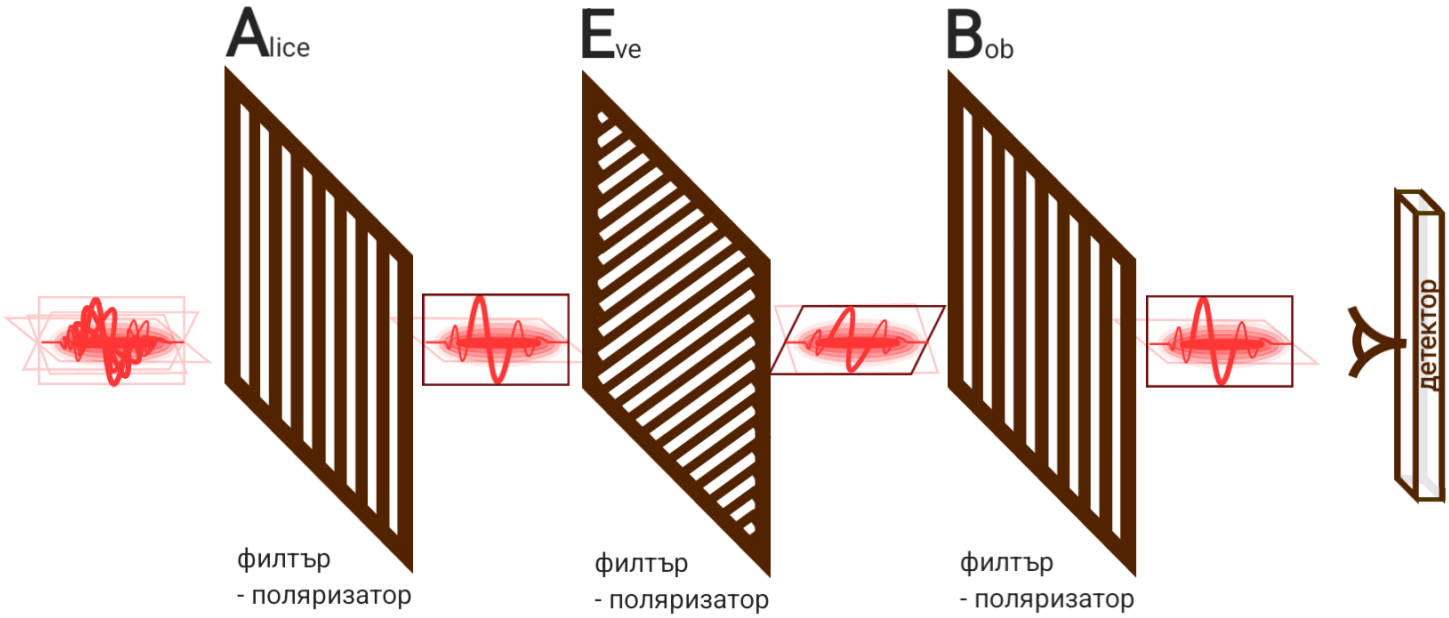
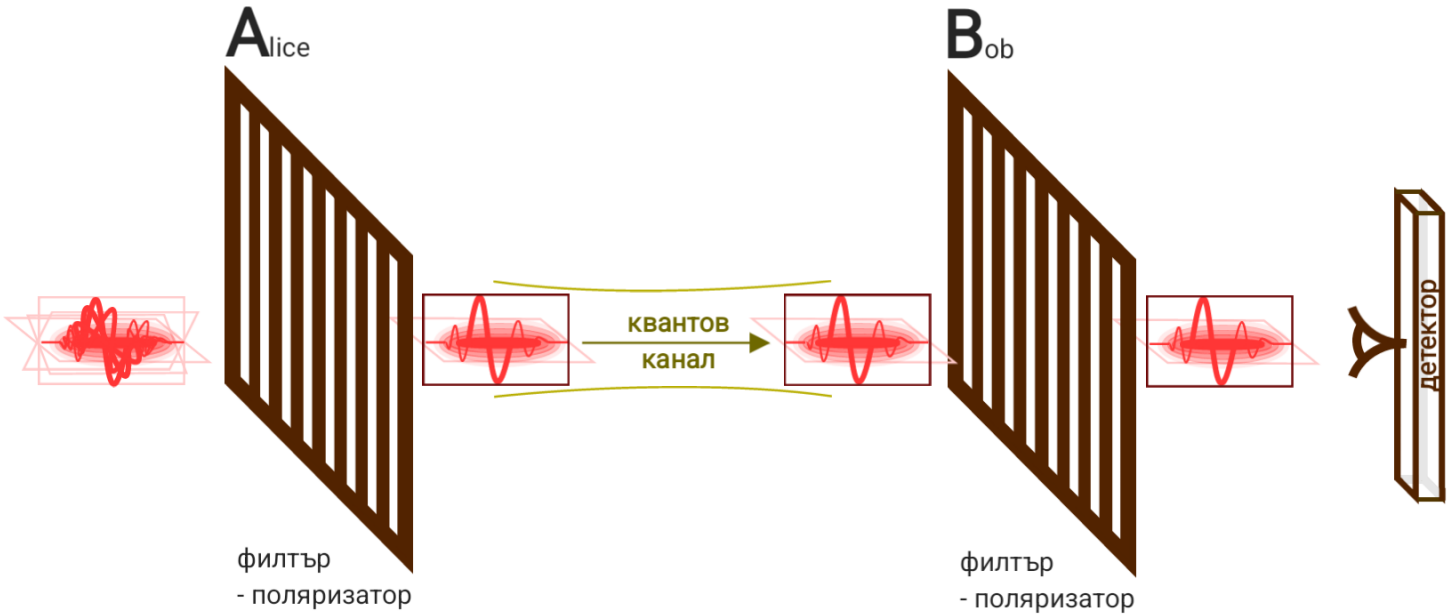
ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"



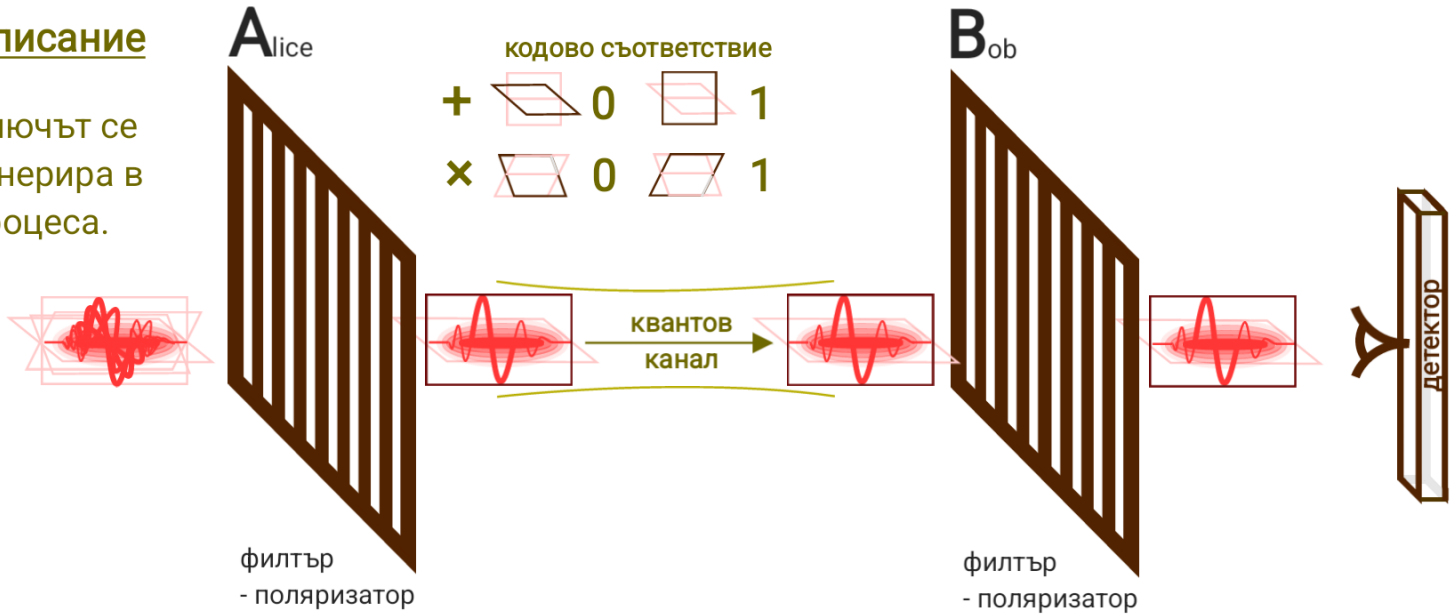
ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

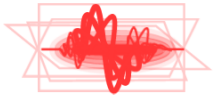
Ключът се генерира в процеса.

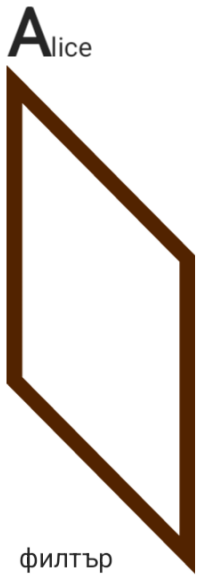


ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

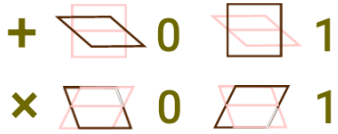
Описание

Ключът се генерира в процеса.





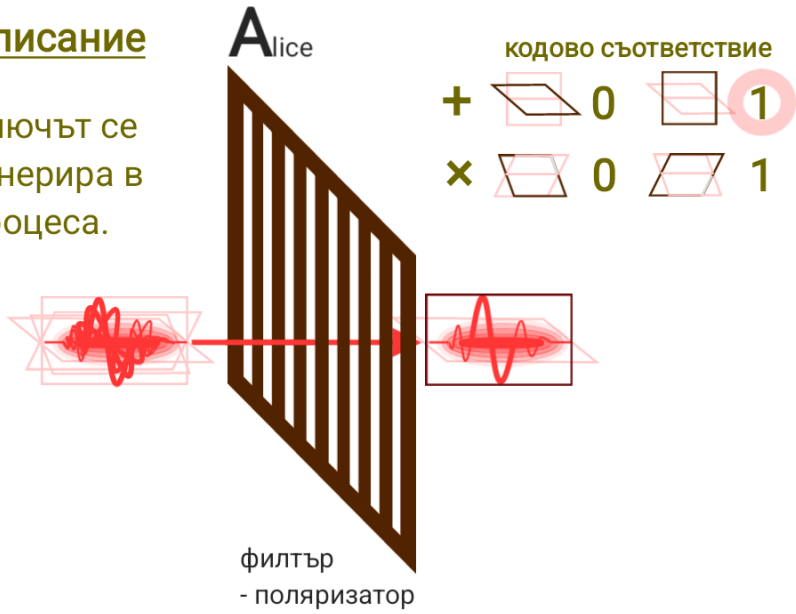
кодово съответствие



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

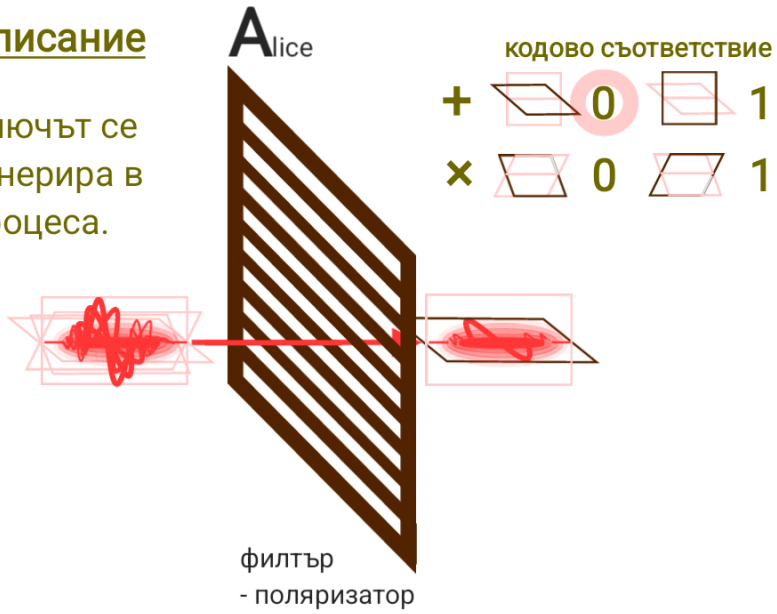
Ключът се генерира в процеса.



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

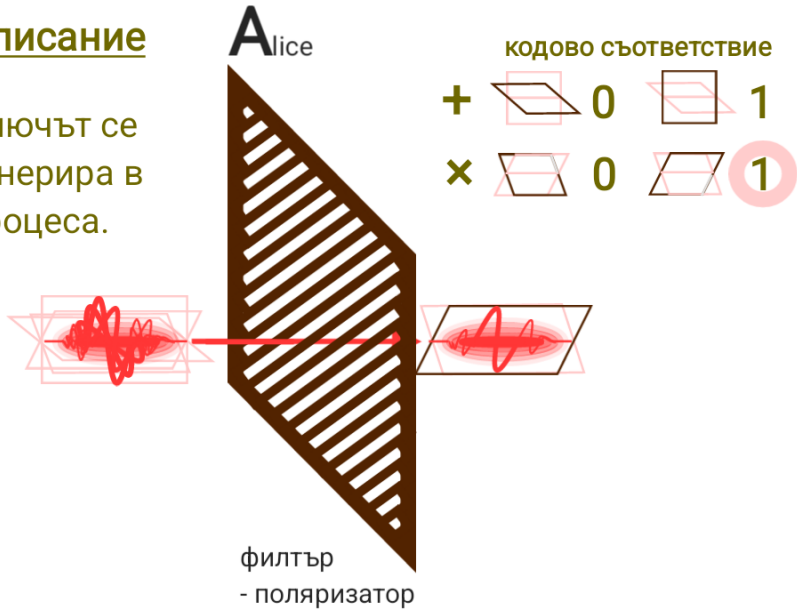
Ключът се генерира в процеса.



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

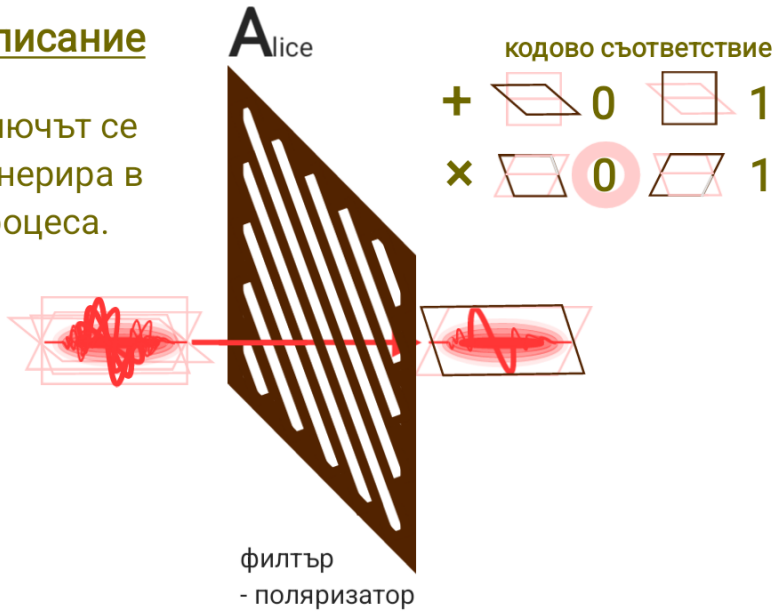
Ключът се генерира в процеса.



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

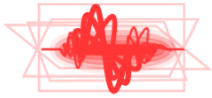
Ключът се генерира в процеса.



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

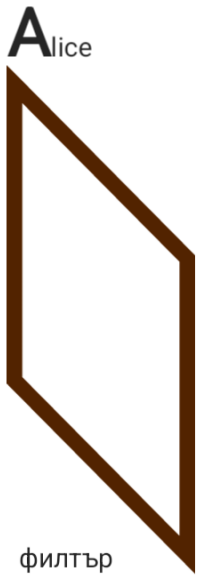
Описание

Ключът се генерира в процеса.

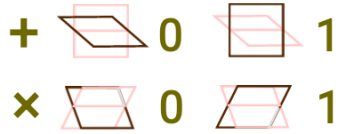


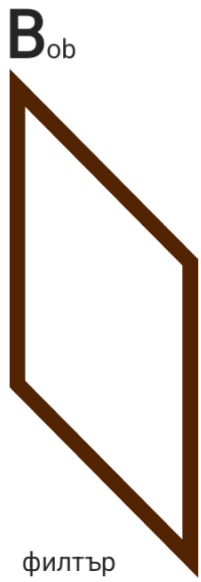
Стъпка 1

За всеки бит
Алис избира: базис +/× и филтър
(кодовия символ)



кодово съответствие

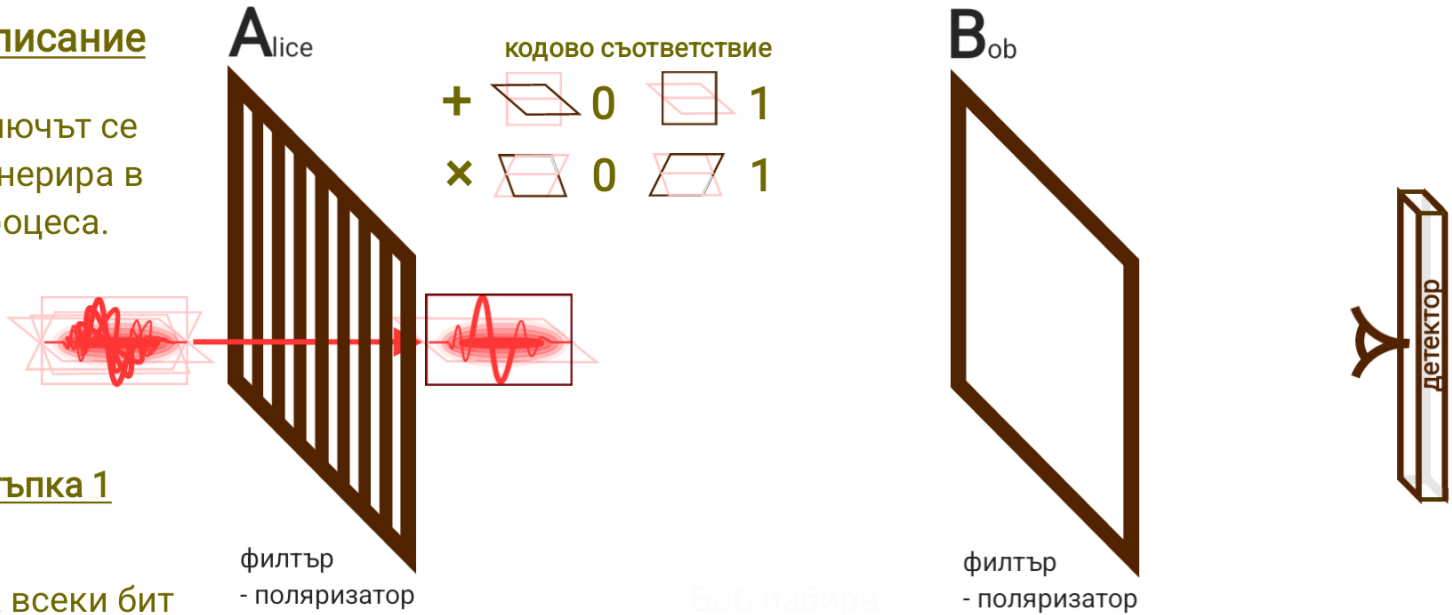




ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 1

За всеки бит

Алис избира: базис +/× + + × + × +

и филтър 1 0 1 1 0 1

(кодовия символ)

Боб избира + + × + × +

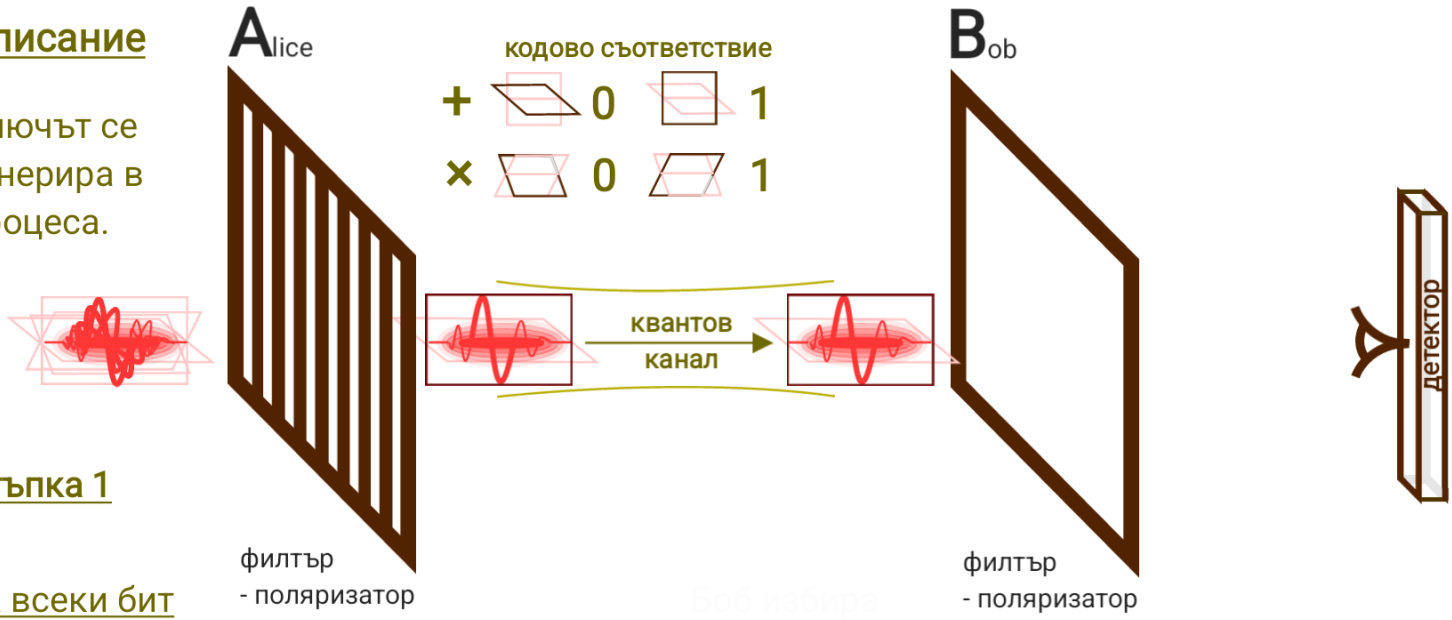
измерване

и получава 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 +/× + + × + × +

и филтър 1 0 1 1 0 1

(кодовия символ)

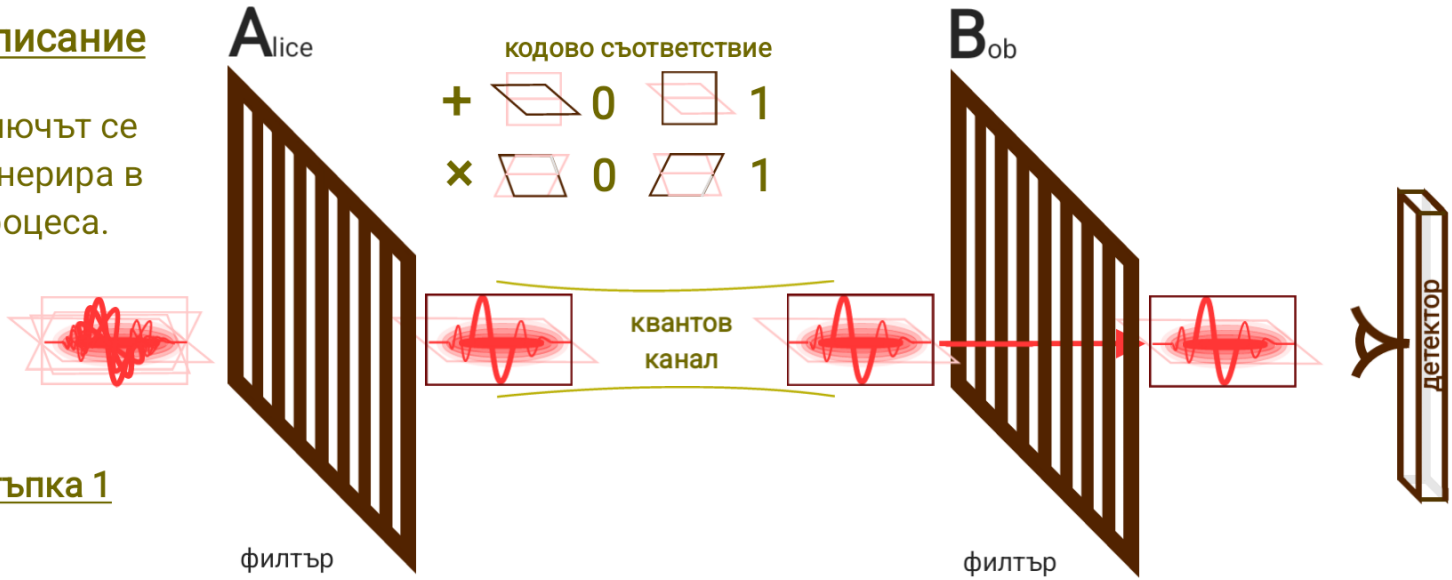
Боб избира + + × + × +

измерване и получава 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 +/× + + × + × +

и филтър 1 0 1 1 0 1

(кодовия символ)

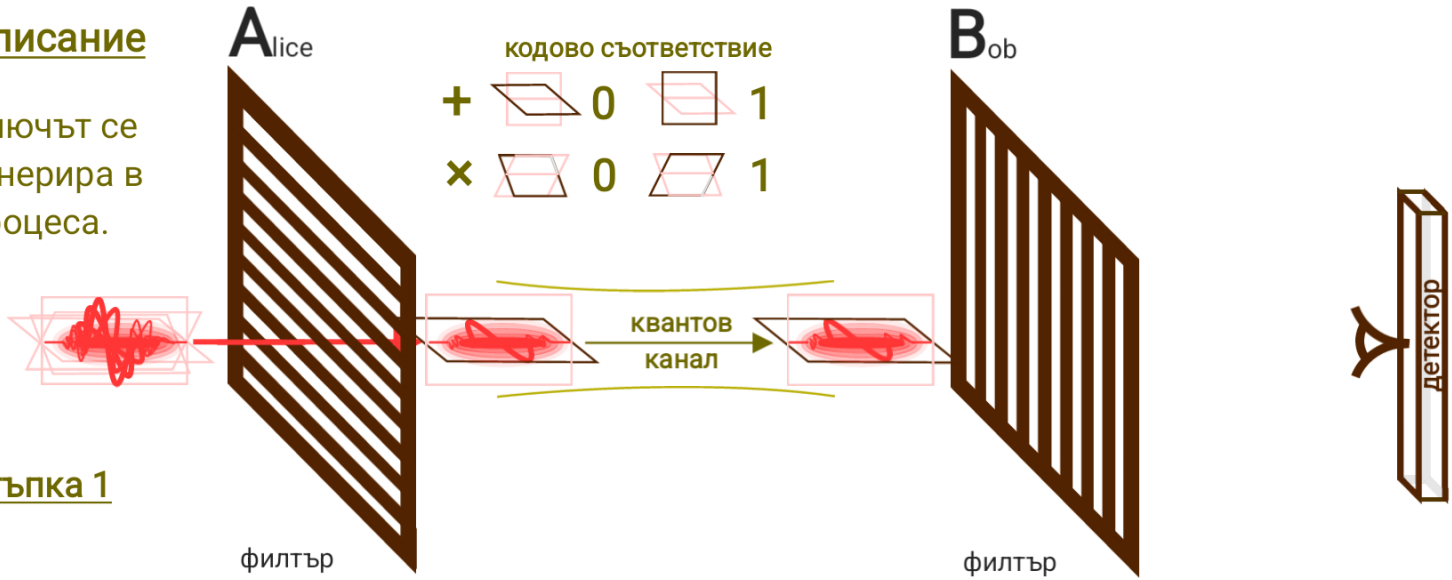
Боб избира измерване + + × + × +

и получава 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 +/× + + × + × +

и филтър 1 0 1 1 0 1

(кодовия символ)

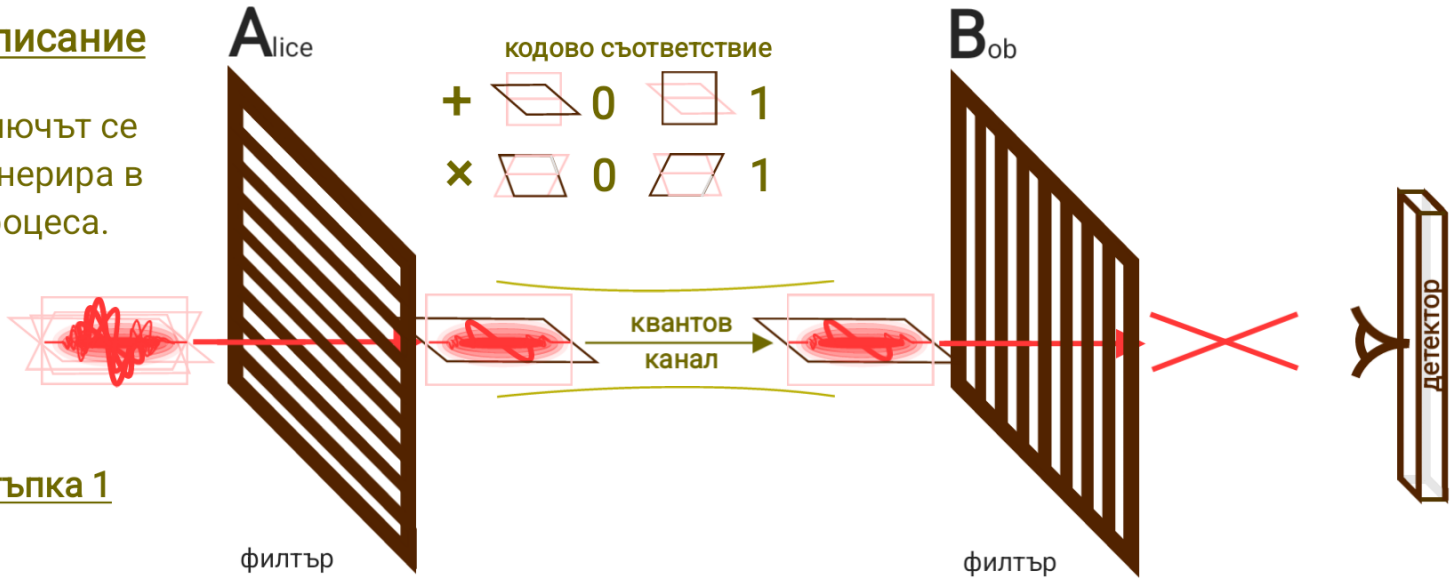
Боб избира измерване + + × + × +

и получава 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 +/× + + × + × +

и филтър 1 0 1 1 0 1

(кодовия символ)

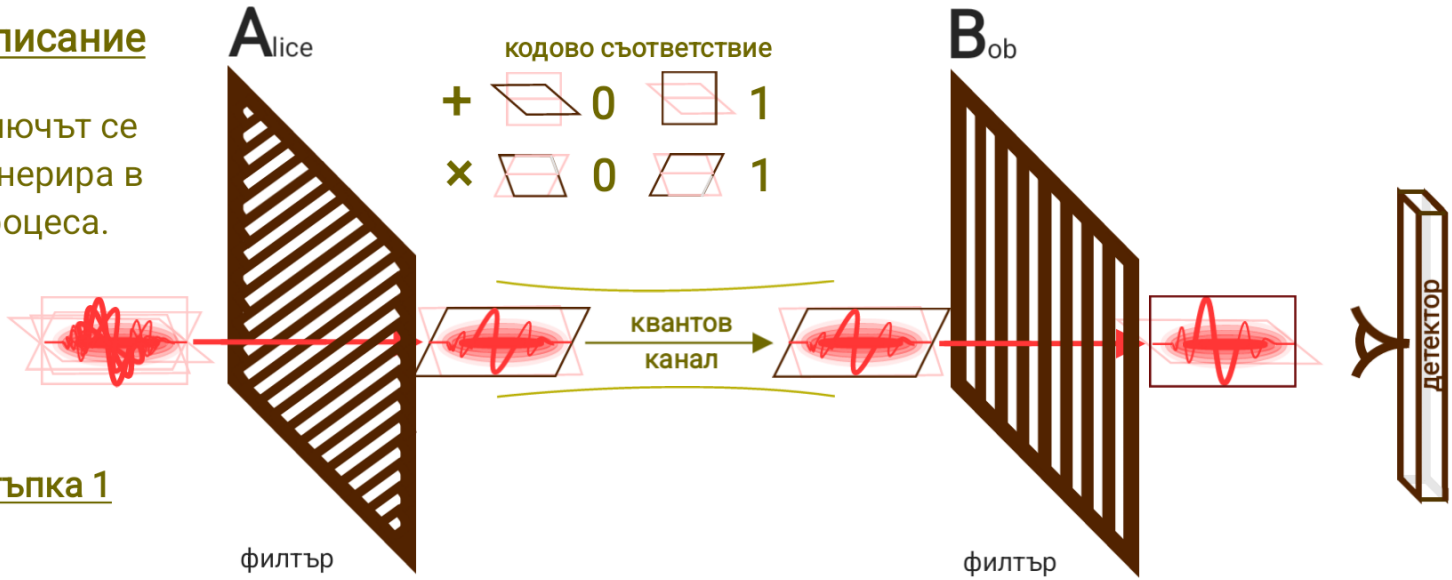
Боб избира измерване + + × + × +

и получава 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 +/× + + × × × ×

и филтър 1 0 1 1 0 1

(кодовия символ)

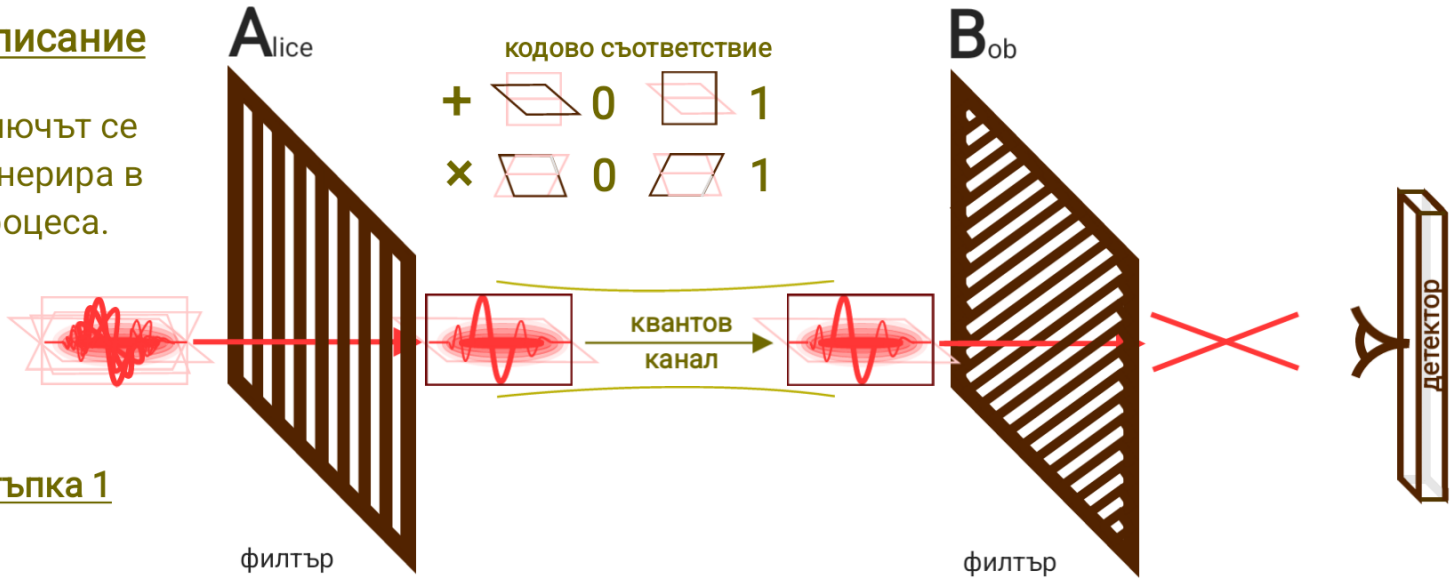
Боб избира измерване + + + × + ×

и получава 1 0 1 0 0 1

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 1

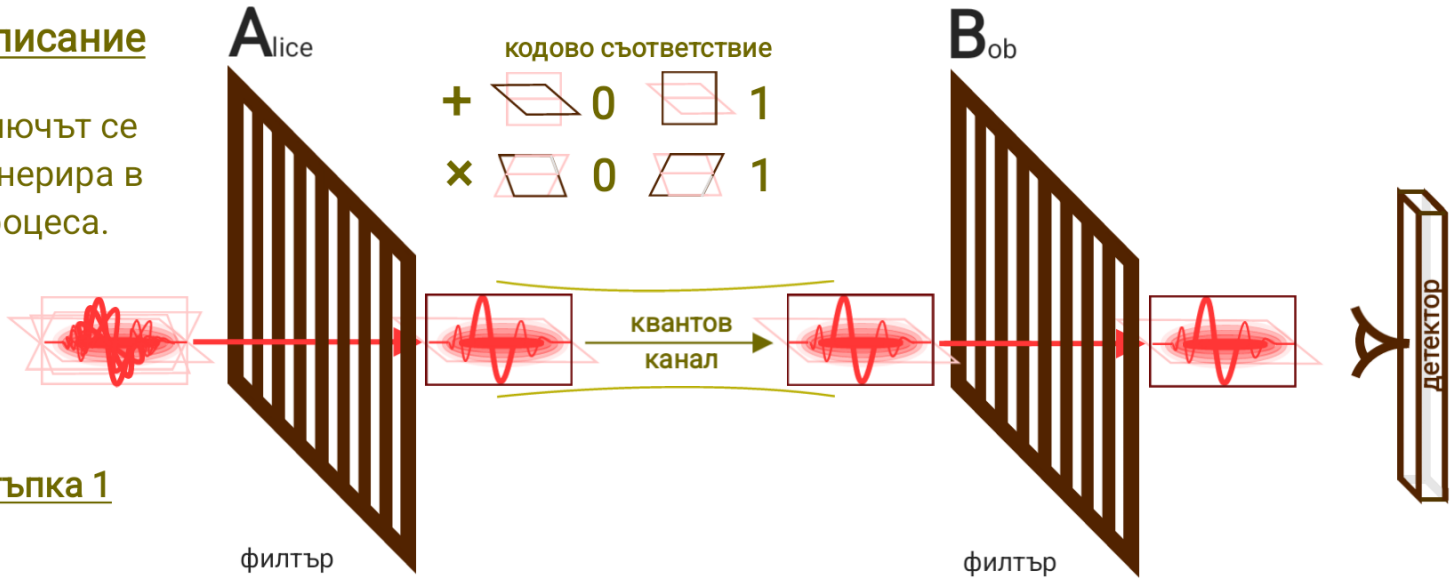
За всеки бит

Алис избира:	базис +/×	+ + × +		Боб избира	измерване	+ + + ×
	и филтър	1 0 1 1			и получава	1 0 1 0
	(кодовия символ)					

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 1

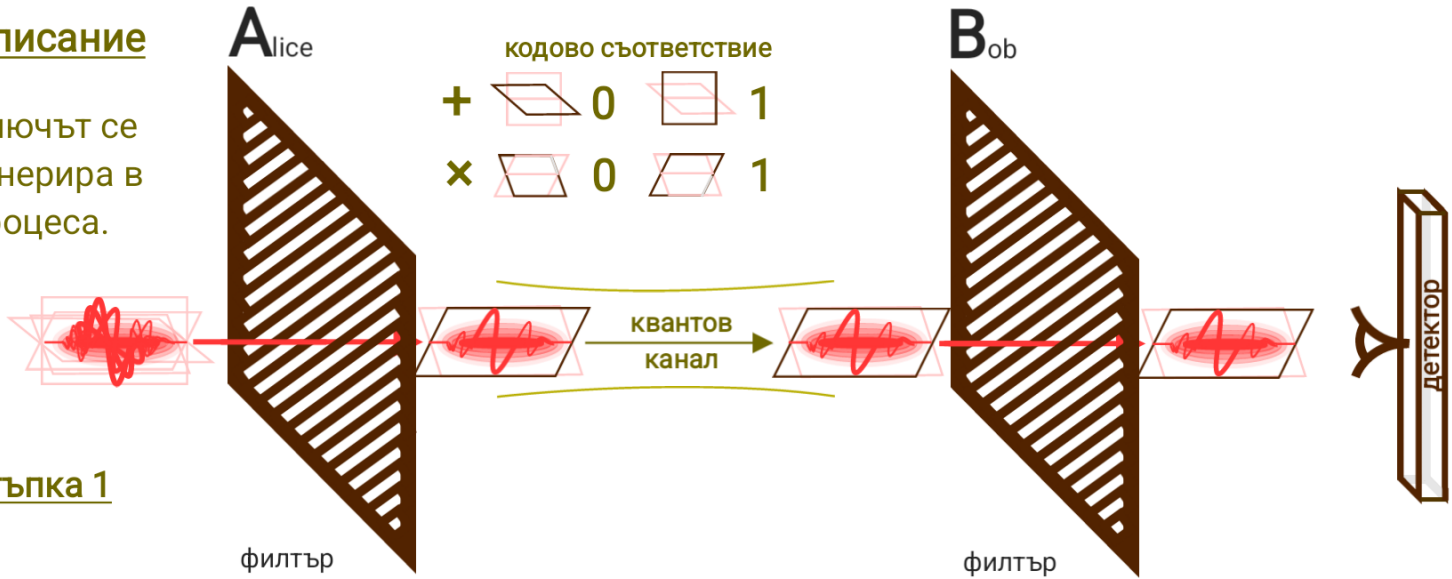
За всеки бит

Алис избира:	базис +/×	+ + × + ×	Боб избира	+ + + × +
	и филтър	1 0 1 1 0	измерване и получава	1 0 1 0 0
	(кодовия символ)			

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 1

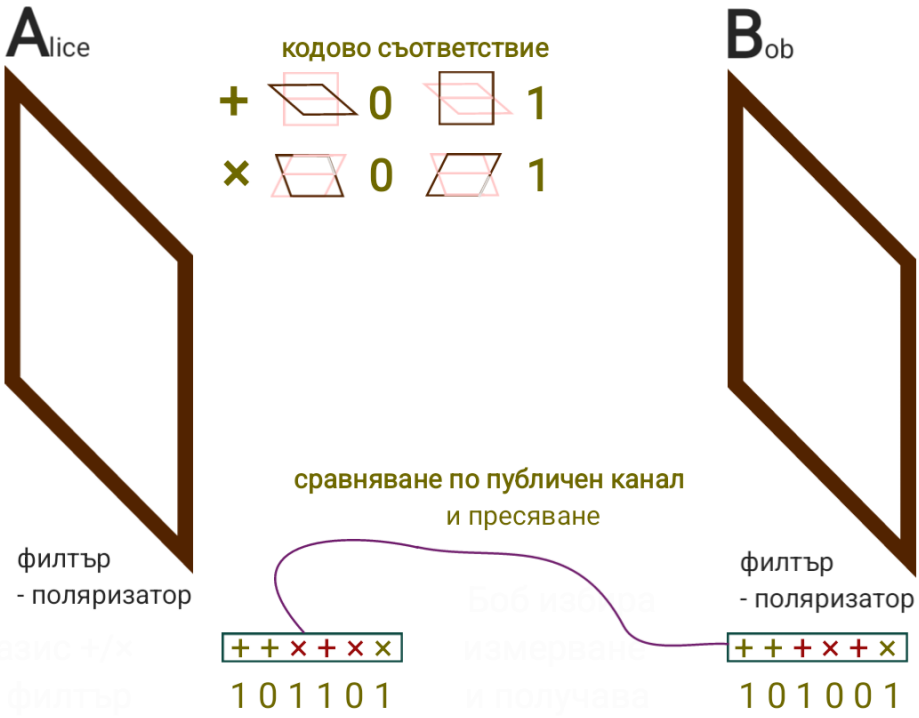
За всеки бит

Алис избира:	базис +/×	+ + × + × ×	Боб избира	+ + + × + ×
	и филтър	1 0 1 1 0 1	измерване и получава	1 0 1 0 0 1
	(кодовия символ)			

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 2

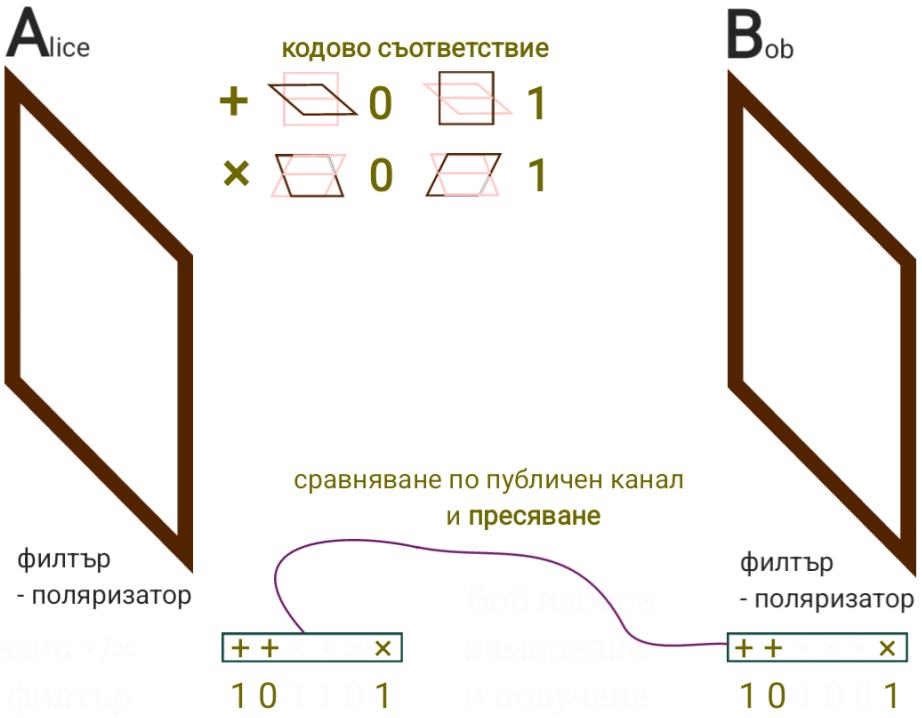
За всеки бит Алис избира базис +/× и филтър (кодовия символ)

Боб избира измерване и получава

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.



Стъпка 2

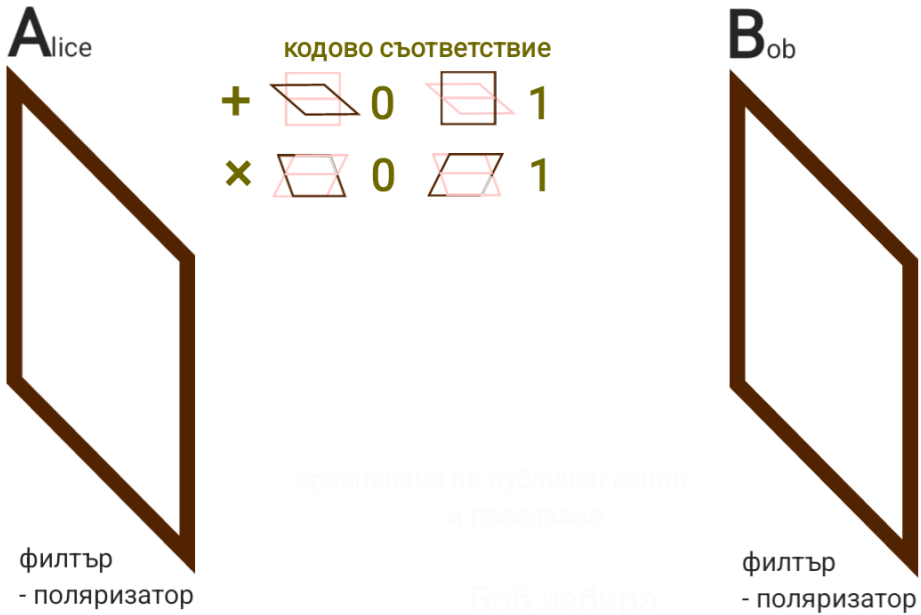
За всеки бит Алис избира базис +/× и филтър (кодовия символ)

Боб избира измерване и получава

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Описание

Ключът се генерира в процеса.

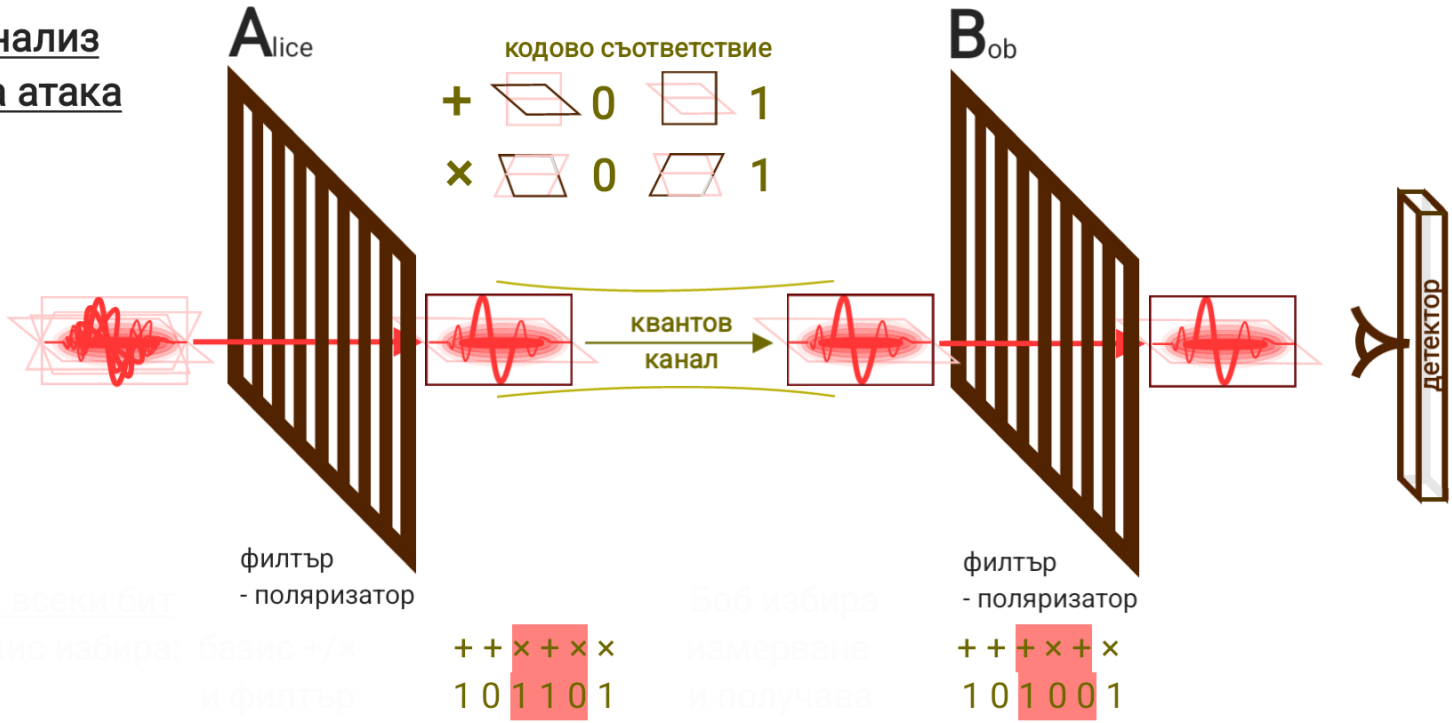


Резултат: пресят ключ: 1 0 1 1 | 1 0 1 1

100% съвпадение при липса на вмвшателство

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ на атака

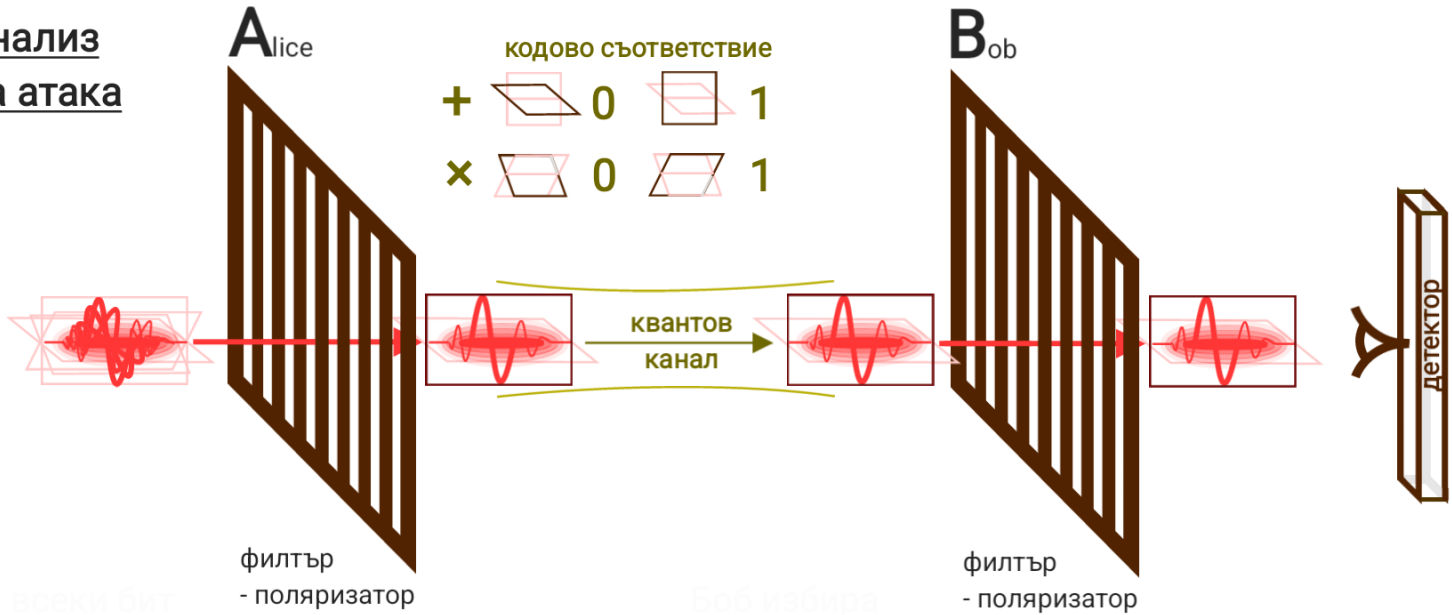


За всеки бит Алис избира: базис +/× и филтър (кодовия символ)

Боб избира измерване и получава

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

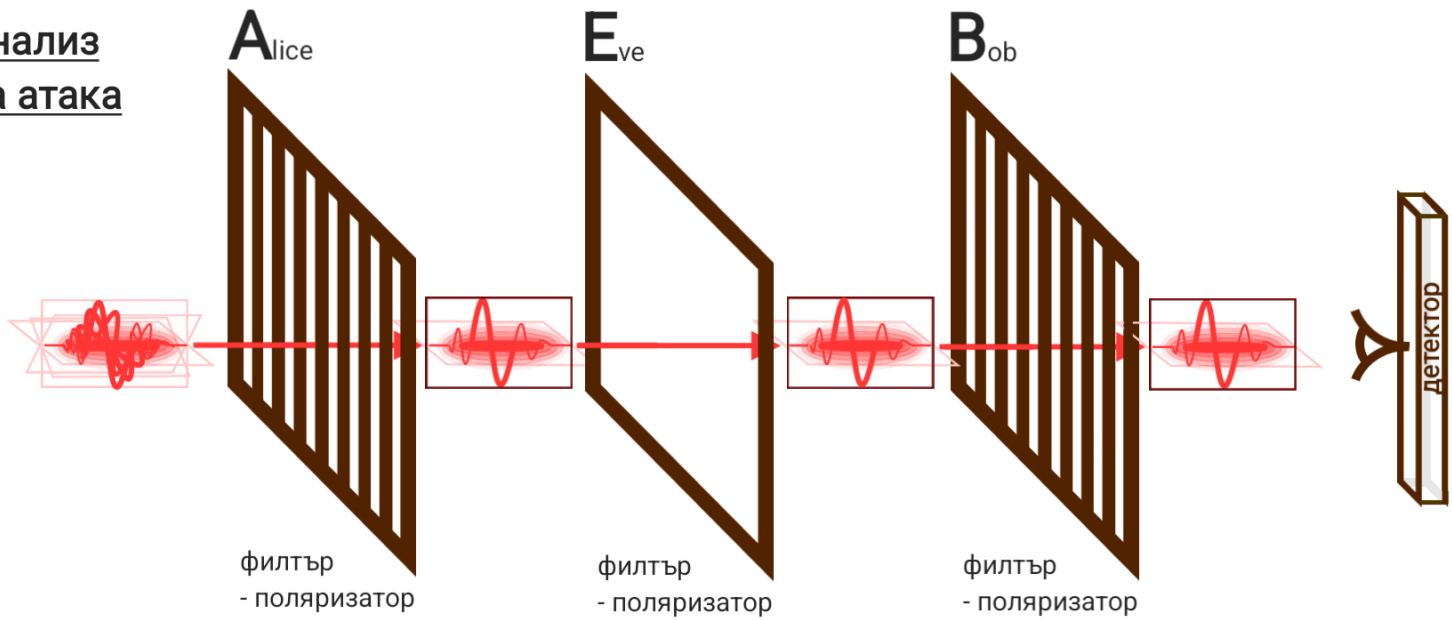
Анализ на атака



За всеки бит
Алис избира: базис +/× и филтър (кодовия символ)
Боб избира измерване и получава

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ на атака



A: + × + + × × + × + ×

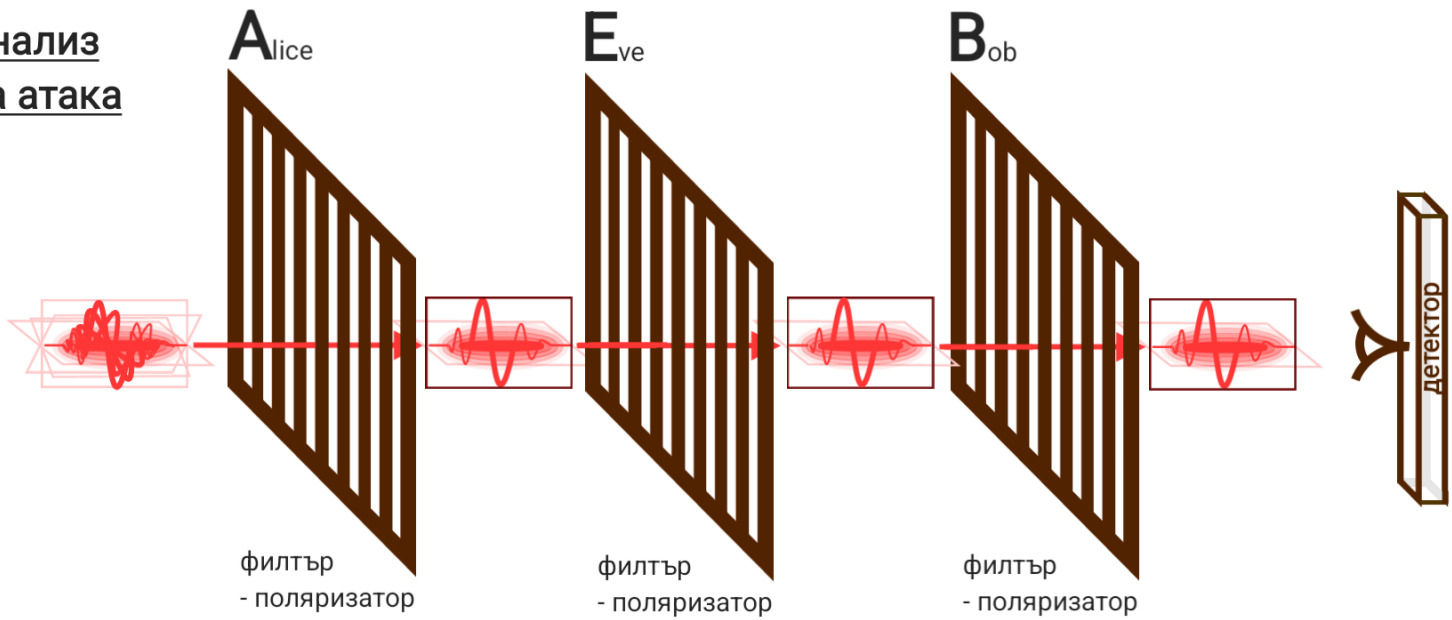
1 0 1 1 0 1

B: + × + × + × + × + ×

1 0 1 0 0 1

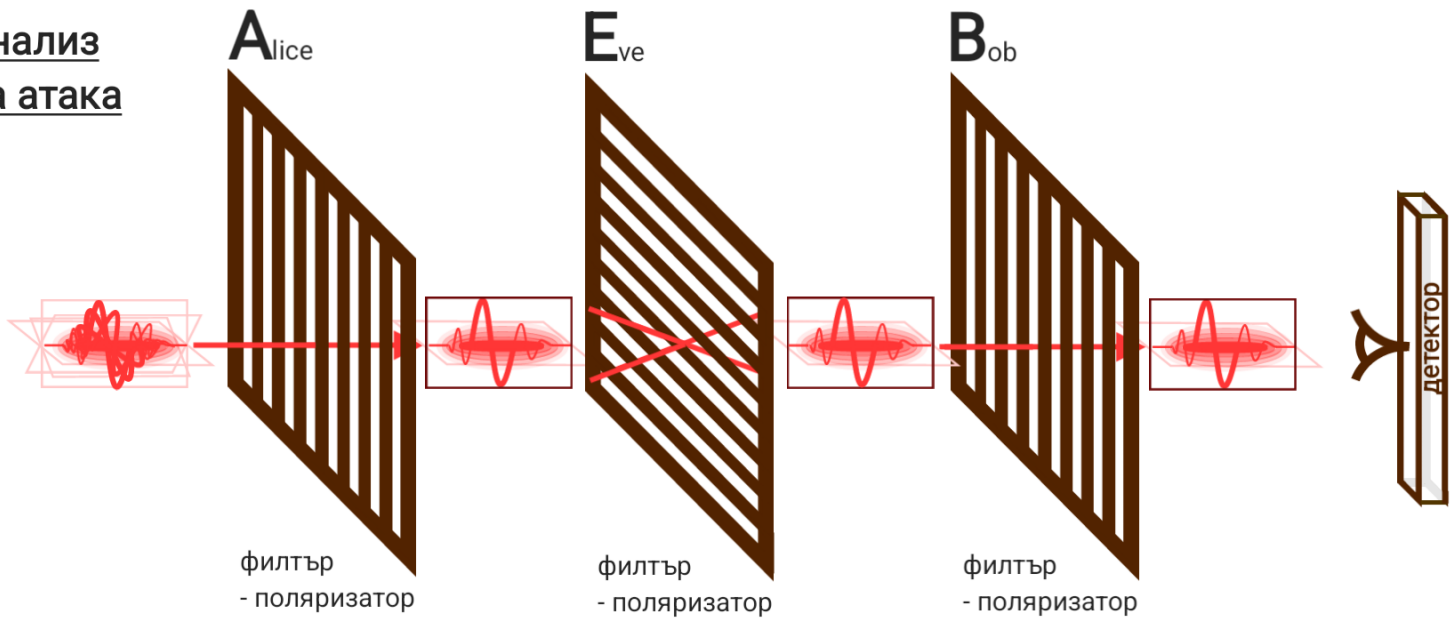
ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ на атака



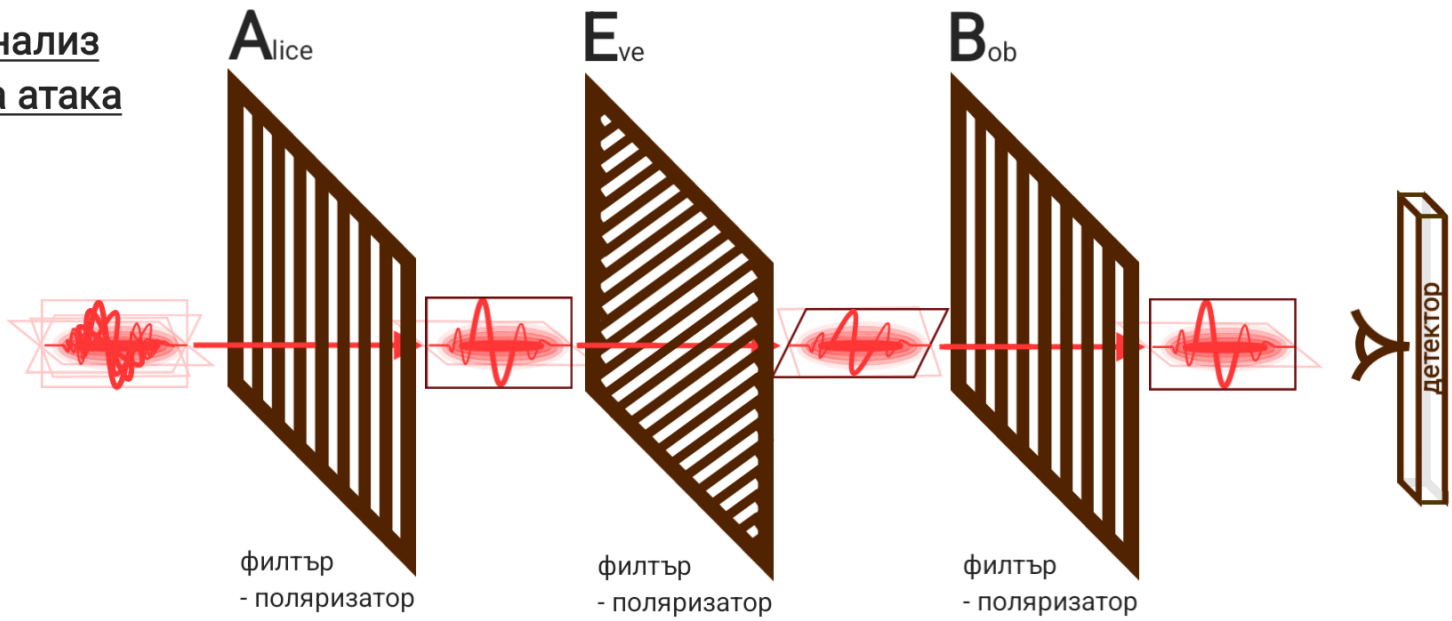
ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ на атака



ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ на атака



A: + + × + × + + × + ×

E: × -> 50%

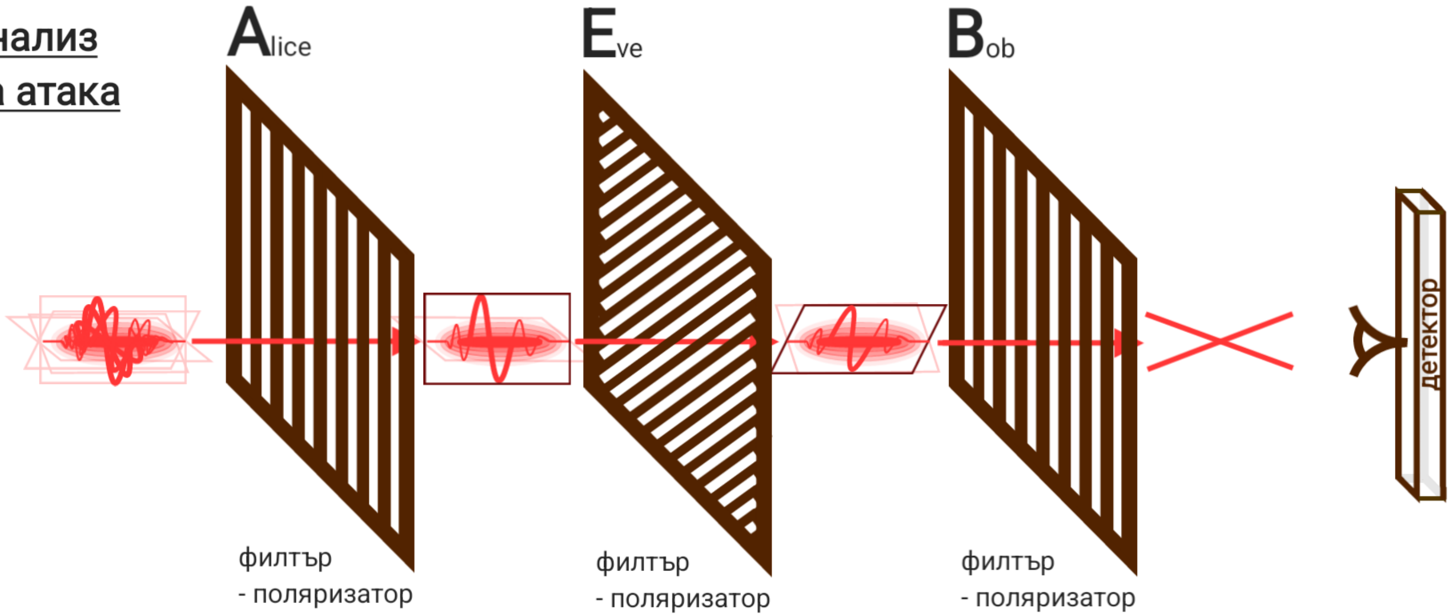
1 0 1 1 0 1 1/0

B: + + × + ×

1 -> 25%

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ на атака



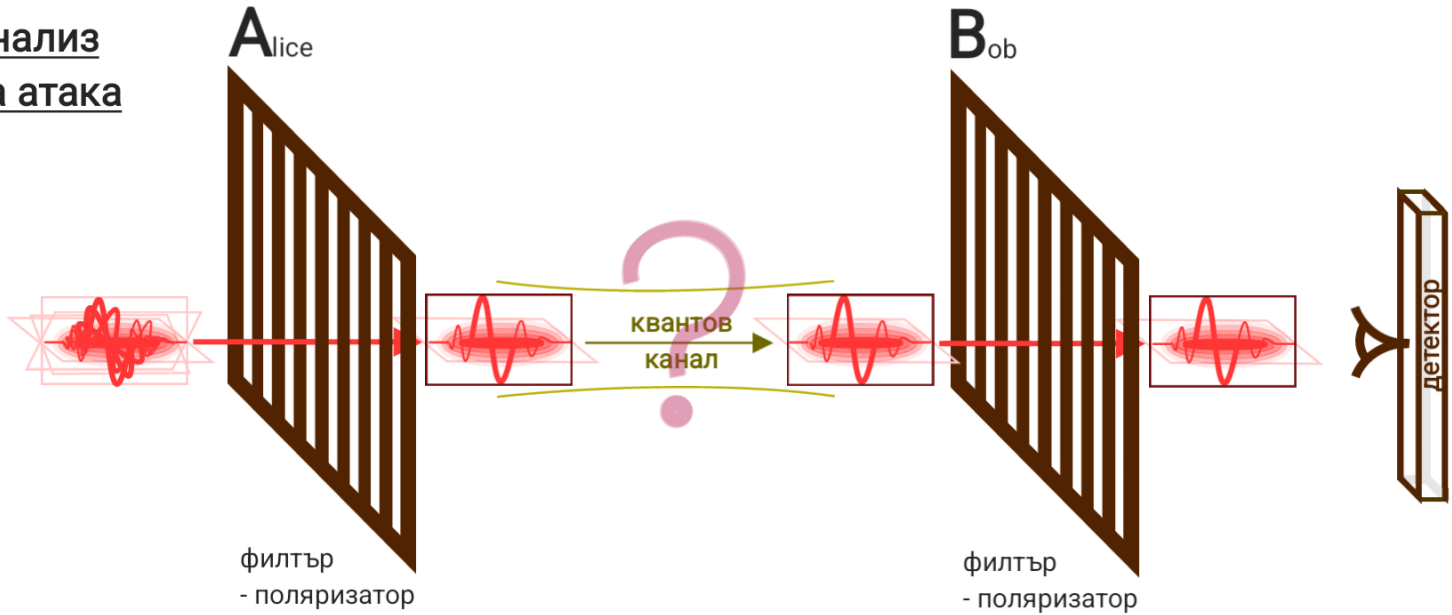
A: + 1

E: × -> 50% 1/0

B: + 0 -> 25% РАЗКРИТА АТАКА

ПРИЛОЖЕНИЕ: ПРОТОКОЛ "Bennett Brassard-1984"

Анализ на атака



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