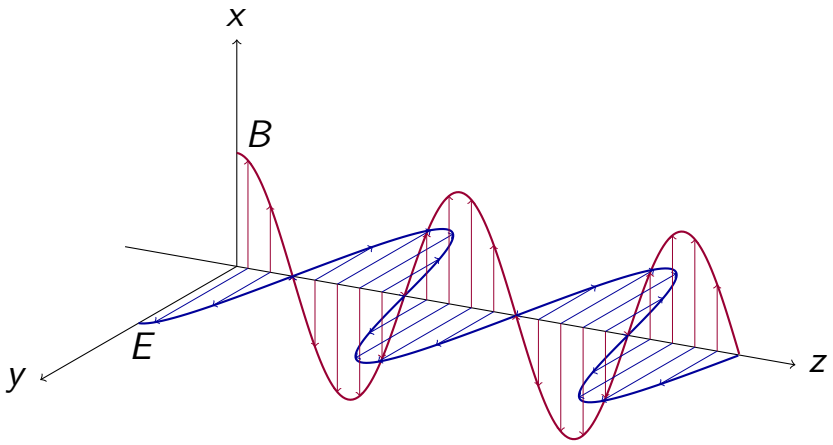
Aula 15: Física Quântica

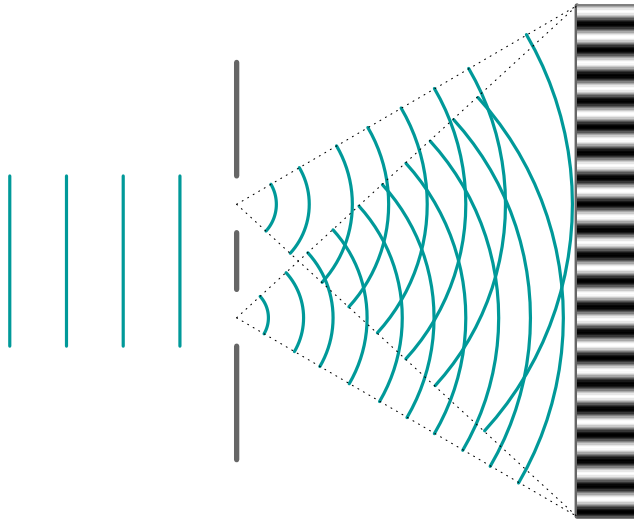
Bárbara Amaral
Instituto de Física da USP

O Bit Quântico

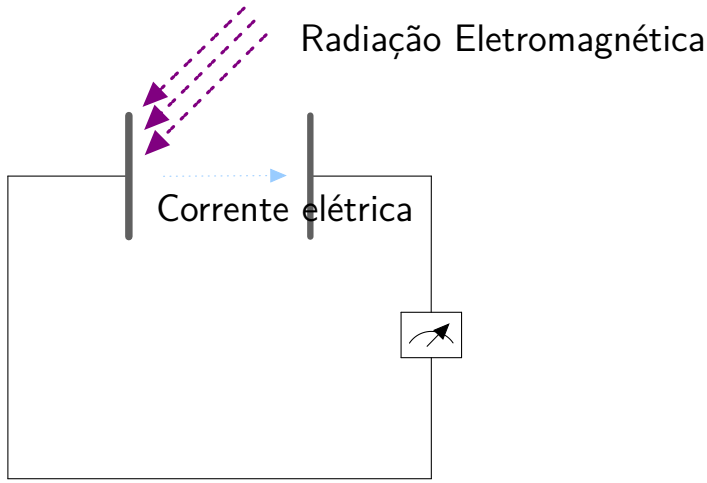
A Física

A Polarização da Luz


x
B
E
y
z



O efeito fotoelétrico

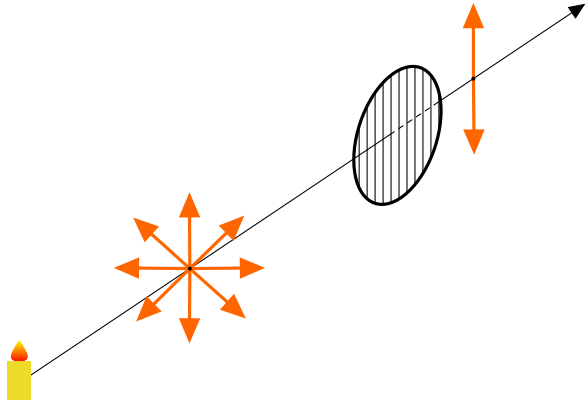


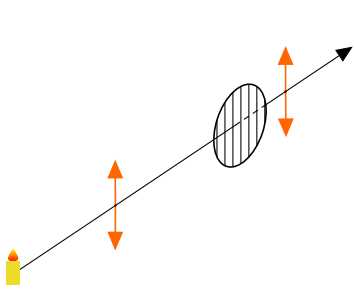
Dualidade Onda-Partícula

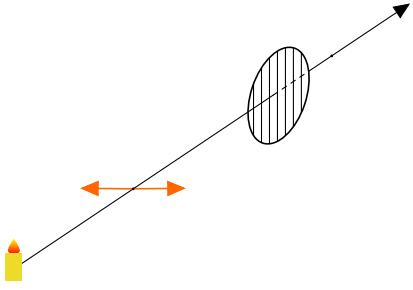
Dualidade onda-partícula

A radiação eletromagnética algumas vezes se comporta como onda e algumas vezes se comporta como partícula.

A polarização é uma característica dos fótons.



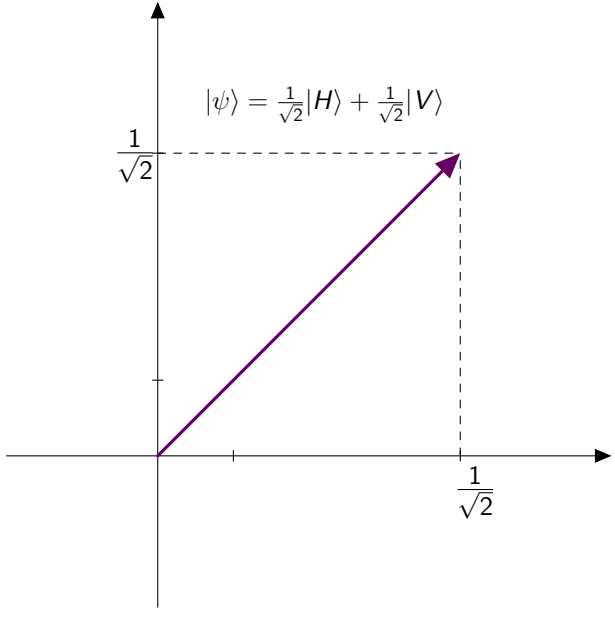




Fóton polarizado horizontalmente: $|H\rangle$.

Fóton polarizado verticalmente: $|V\rangle$.

Os fótons podem estar polarizados em outras direções além das direções x e y.


$|\psi\rangle = \frac{1}{\sqrt{2}}|H\rangle + \frac{1}{\sqrt{2}}|V\rangle$
$\frac{1}{\sqrt{2}}$
$\frac{1}{\sqrt{2}}$

Os estados extremais são associados a vetores ortogonais.

$$|H\rangle = (1, 0)$$
$$|V\rangle = (0, 1)$$

Um fóton polarizado em outras direções pode ser representado por uma combinação dos símbolos $|H\rangle$ e $|V\rangle$:

$$|\phi\rangle = \alpha|H\rangle + \beta|V\rangle.$$

A probabilidade do fóton ser absorvido é $|\alpha|^2$ e a probabilidade do fóton ser transmitido é $|\beta|^2$.

Os estados de polarização podem ser adequadamente descritos se utilizarmos $\mathbb{C}^2$.

Por convenção , associamos os estados de polarização $|H\rangle$ e $|V\rangle$ à base ortonormal

$$|H\rangle = (1,0), \quad |V\rangle = (0,1).$$

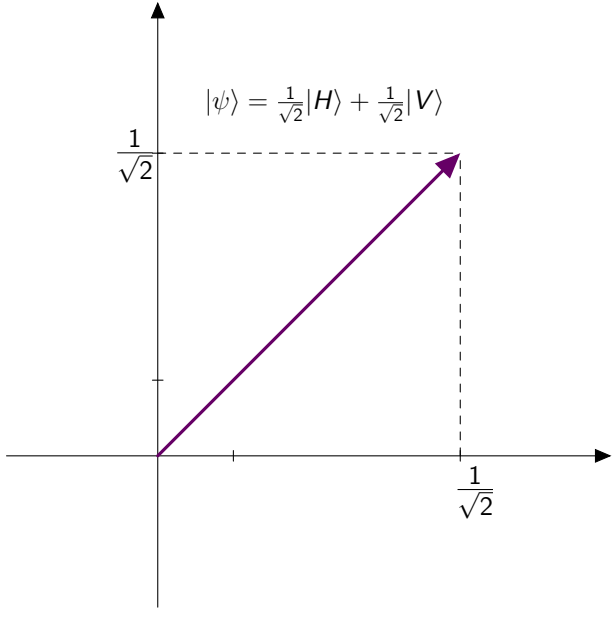
Luz Linearmente Polarizada

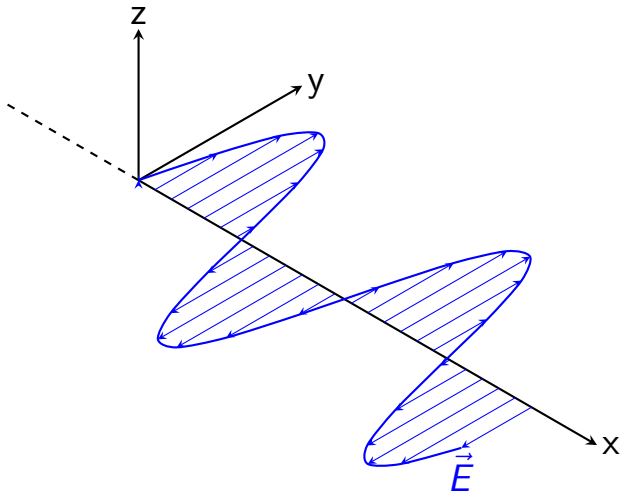
α e β são números reais.

Luz Linearmente Polarizada

α e β são números reais.

A direção do campo elétrico é constante no tempo e é determinada pelos valores de α e β.


$|\psi\rangle = \frac{1}{\sqrt{2}}|H\rangle + \frac{1}{\sqrt{2}}|V\rangle$
$\frac{1}{\sqrt{2}}$
$\frac{1}{\sqrt{2}}$


z
y
x
$\vec{E}$

Luz circularmente polarizada

α ou β possuem parte imaginária diferente de zero.

Luz circularmente polarizada

α ou β possuem parte imaginária diferente de zero.

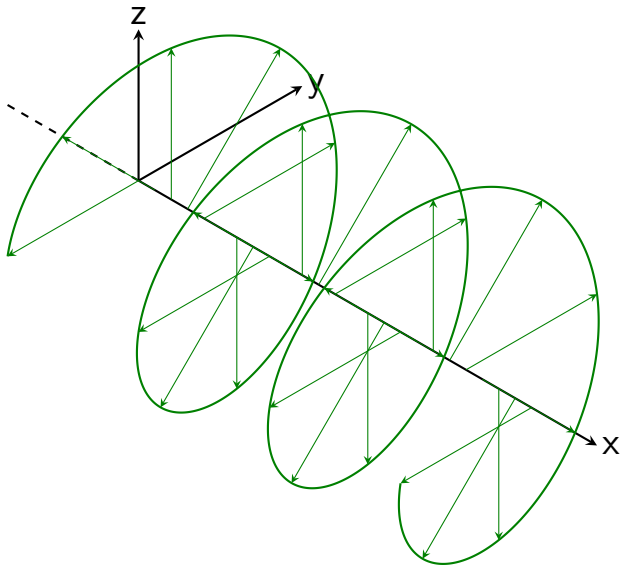
As componentes do campo elétrico nas direções x e y oscilam *fora de fase* e a direção do campo elétrico varia com o tempo.

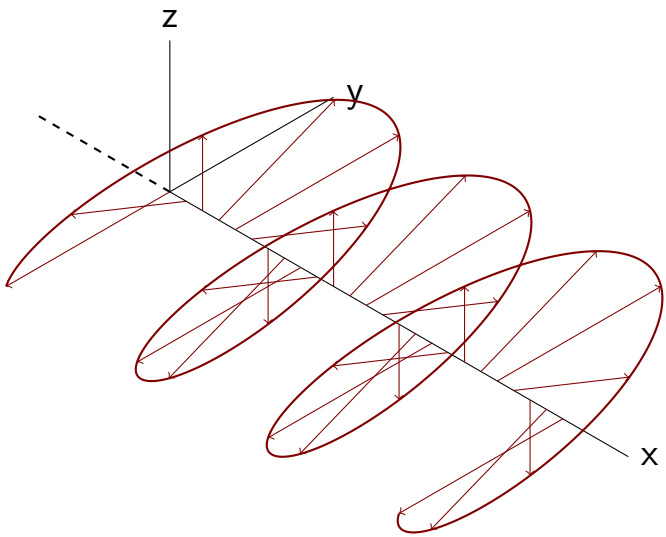
Luz circularmente polarizada

α ou β possuem parte imaginária diferente de zero.

As componentes do campo elétrico nas direções x e y oscilam *fora de fase* e a direção do campo elétrico varia com o tempo.

Nesse caso temos estados de polarização chamados de polarização *circular* e *elíptica*.

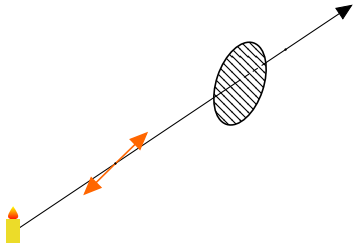

z
y
x

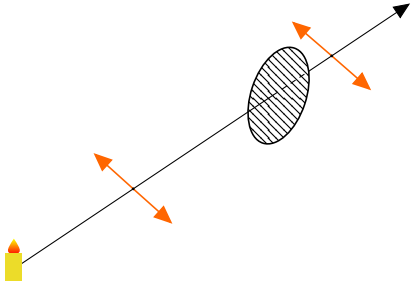

z
y
x

Outros teste

$$|+\rangle = \frac{1}{\sqrt{2}}|H\rangle + \frac{1}{\sqrt{2}}|V\rangle$$

$$|-\rangle = \frac{1}{\sqrt{2}}|H\rangle - \frac{1}{\sqrt{2}}|V\rangle$$





$$|\phi\rangle = \gamma|+\rangle + \delta|-\rangle.$$

$$|\phi\rangle = \gamma|+\rangle + \delta|-\rangle.$$

A probabilidade do fóton ser absorvido é igual a $|\gamma|^2$ e a probabilidade do fóton ser transmitido é $|\delta|^2$.

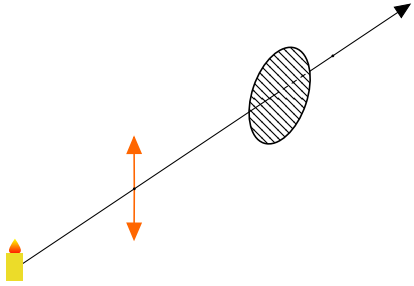
Exemplo

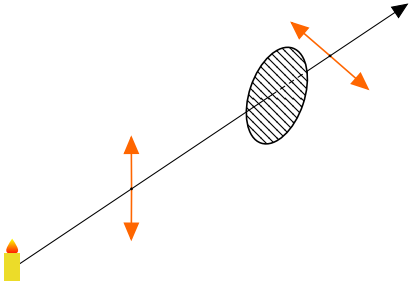
Por exemplo, o estado de polarização $|H\rangle$ pode ser escrito na forma

$$|H\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$$

e o estado de polarização $|V\rangle$ pode ser escrito na forma

$$|V\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle.$$





A Matemática

O Bit Clássico

O bit clássico

Variável que pode assumir dois valores: 0 e 1.

O bit clássico

Variável que pode assumir dois valores: 0 e 1.

O Bit Quântico

O bit quântico

Temos dois estados extremais $|0\rangle$ e $|1\rangle$.

O bit quântico

Temos dois estados extremais $|0\rangle$ e $|1\rangle$.

O sistema pode estar em *superposição* desses dois estados.

O bit quântico

Temos dois estados extremais $|0\rangle$ e $|1\rangle$.

O sistema pode estar em *superposição* desses dois estados.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

Feynman

We shall tackle immediately the basic element of the mysterious behavior in its most strange form. We choose to examine a phenomenon which is impossible, absolutely impossible, to explain in any classical way, and which has in it the heart of quantum mechanics. In reality, it contains the only mystery. We cannot make the mystery go away by "explaining" how it works. We will just tell you how it works. In telling you how it works we will have told you about the basic peculiarities of all quantum mechanics.

Em um teste podemos apenas distinguir entre os estados $|0\rangle$ e $|1\rangle$.

A probabilidade da resposta 0 é

$$p(0) = |\alpha|^2$$

e a probabilidade da resposta 1 é

$$p(1) = |\beta|^2.$$

A probabilidade da resposta 0 é

$$p(0) = |\alpha|^2$$

e a probabilidade da resposta 1 é

$$p(1) = |\beta|^2.$$

$$|\alpha|^2 + |\beta|^2 = 1$$

Probabilística *a priori*.

Após a realização do teste:

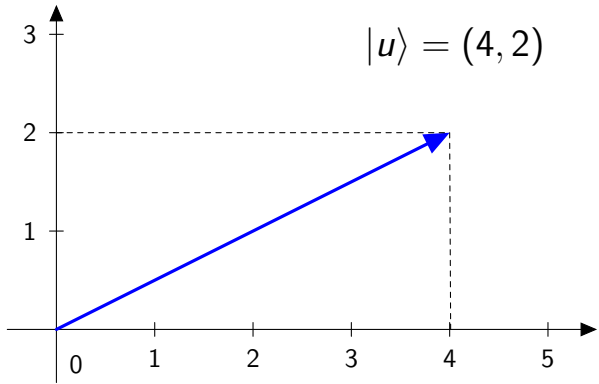
Após a realização do teste:

- Se a resposta foi 0 o estado final do sistema é $|0\rangle$.

Após a realização do teste:

- Se a resposta foi 0 o estado final do sistema é $|0\rangle$.
- Se a resposta foi 1, o estado final do sistema é $|1\rangle$.

A descrição matemática do *estado* de um bit quântico pode ser feita através de vetores.

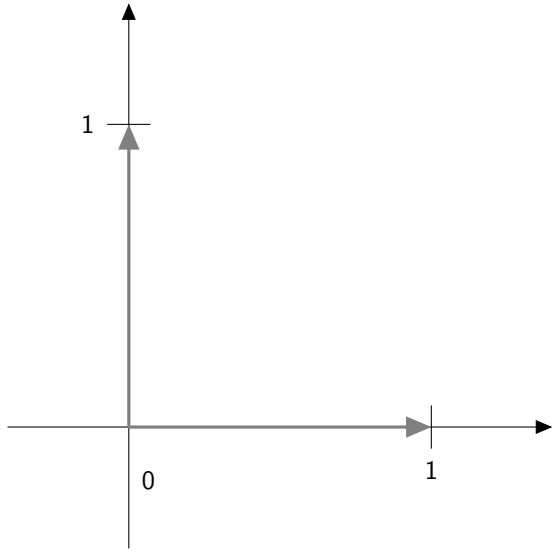

$|u\rangle = (4, 2)$
3
2
1
0
1
2
3
4
5

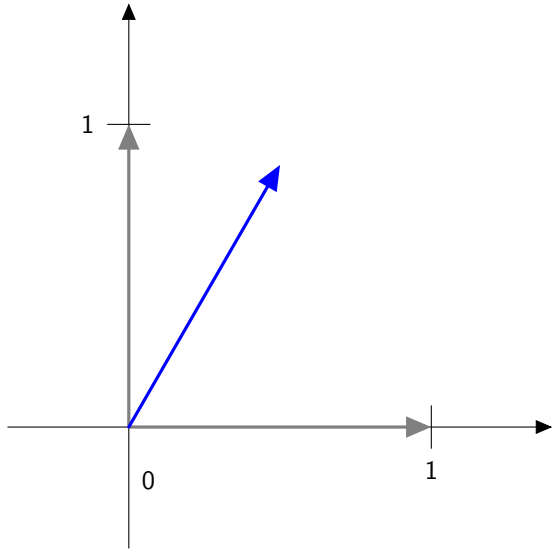
O bit quântico

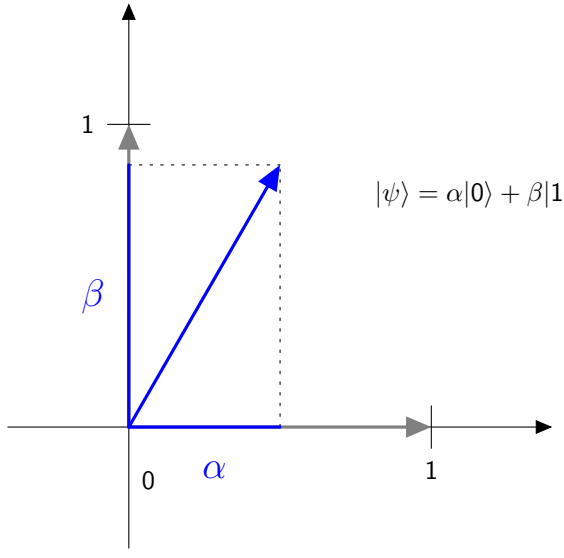
Os estados extremais são associados a vetores ortogonais.

$$|0\rangle = (1, 0)$$

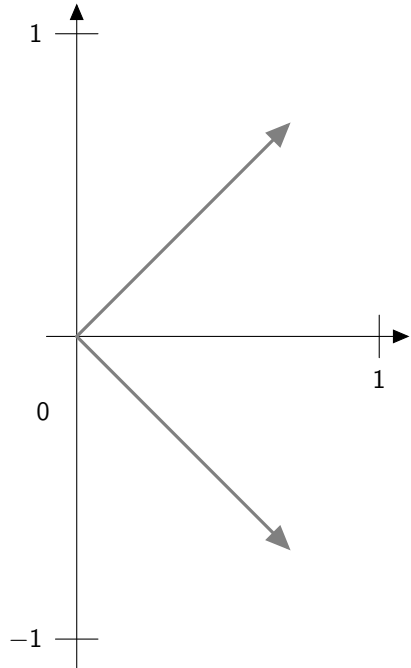
$$|1\rangle = (0, 1)$$


1
0
1


1
0
1

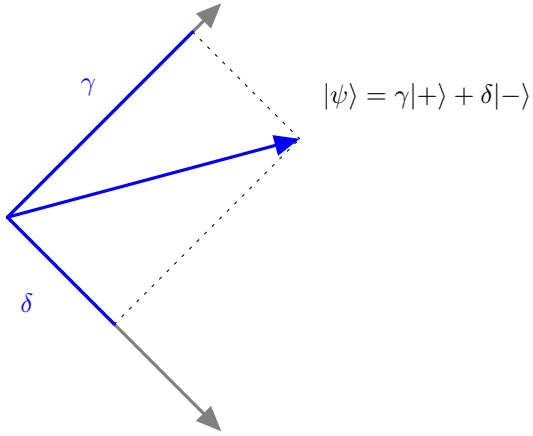

1
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
β
0
α
1

Existem outros pares de vetores ortogonais...


1
1
0
−1

$$|+\rangle = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$$

$$|-\rangle = \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)$$


γ
δ
$|\psi\rangle = \gamma|+\rangle + \delta|-\rangle$

O Bit Quântico

$$|\psi\rangle = \gamma|+\rangle + \delta|-\rangle.$$

A probabilidade da resposta $+$ é

$$p(+) = |\gamma|^2$$

e a probabilidade da $-$ é

$$p(-) = |\delta|^2.$$

Após a realização do teste:

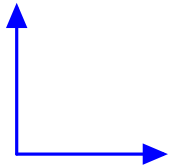
Após a realização do teste:

- Se a resposta foi $+$ o estado final do sistema é $|+\rangle$.

Após a realização do teste:

- Se a resposta foi $+$ o estado final do sistema é $|+\rangle$.
- Se a resposta foi $-$, o estado final do sistema é $|-\rangle$.

Teste Z

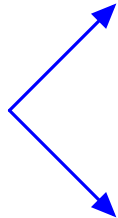


$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$p(0) = |\alpha|^2, \quad |\psi\rangle_f = |0\rangle$

$p(1) = |\beta|^2, \quad |\psi\rangle_f = |1\rangle$

Teste X



$|\psi\rangle = \gamma|+\rangle + \delta|-\rangle$

$p(+) = |\gamma|^2, \quad |\psi\rangle_f = |+\rangle$

$p(-) = |\delta|^2, \quad |\psi\rangle_f = |-\rangle$

Exercício

Teste Z aplicado ao estado $|0\rangle$

Teste Z aplicado ao estado $|0\rangle$

$$p(0) = 1$$

$$|\psi\rangle_f = |0\rangle$$

Teste Z aplicado ao estado $|1\rangle$

Teste Z aplicado ao estado $|1\rangle$

$$p(1) = 1$$

$$|\psi\rangle_f = |1\rangle$$

Teste Z aplicado ao estado

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Teste Z aplicado ao estado

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$p(0) = \frac{1}{2}$$

$$|\psi\rangle_f = |0\rangle$$

Teste Z aplicado ao estado

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Teste Z aplicado ao estado

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$p(1) = \frac{1}{2}$$

$$|\psi\rangle_f = |1\rangle$$

Teste Z aplicado ao estado

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Teste Z aplicado ao estado

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$p(0) = \frac{1}{2}$$

$$|\psi\rangle_f = |0\rangle$$

Teste Z aplicado ao estado

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Teste Z aplicado ao estado

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$p(1) = \frac{1}{2}$$

$$|\psi\rangle_f = |1\rangle$$

Teste X aplicado ao estado

$$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$$

Teste X aplicado ao estado

$$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$$

$$p(+) = \frac{1}{2}$$

$$|\psi\rangle_f = |+\rangle$$

Teste X aplicado ao estado

$$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$$

Teste X aplicado ao estado

$$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$$

$$p(-) = \frac{1}{2}$$

$$|\psi\rangle_f = |-\rangle$$

Teste X aplicado ao estado

$$|1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle$$

Teste X aplicado ao estado

$$|1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle$$

$$p(+) = \frac{1}{2}$$

$$|\psi\rangle_f = |+\rangle$$

Teste X aplicado ao estado

$$|1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle$$

Teste X aplicado ao estado

$$|1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle$$

$$p(-) = \frac{1}{2}$$

$$|\psi\rangle_f = |-\rangle$$

Teste X aplicado ao estado $|+\rangle$

Teste X aplicado ao estado $|+\rangle$

$$p(+) = 1$$

$$|\psi\rangle_f = |+\rangle$$

Teste X aplicado ao estado $|-\rangle$

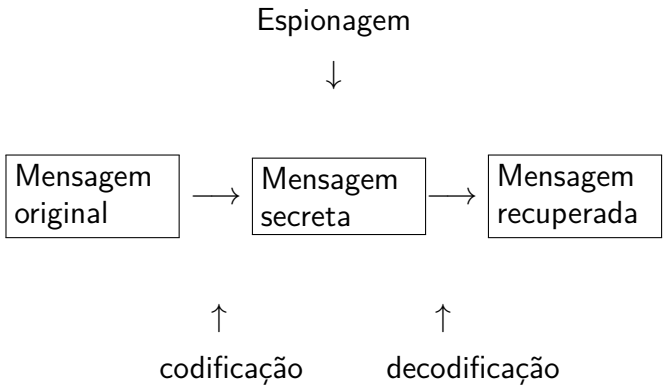
Teste X aplicado ao estado $|-\rangle$

$$p(-) = 1$$

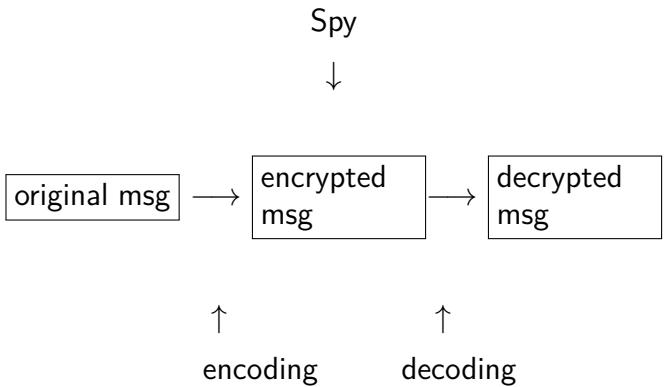
$$|\psi\rangle_f = |-\rangle$$

Criptografia

Criptografia de chave privada



Criptografia de chave privada



Criptografia de Júlio César

Deslocamos o alfabeto e substituímos cada letra pela letra correspondente.

Criptografia de Júlio César

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Q	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
T	U	V	W	X	Y	Z	A	B	C

Criptografia de Júlio César

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Q	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
T	U	V	W	X	Y	Z	A	B	C

MATEMÁTICA $\longrightarrow$ PDWHPDWLFD

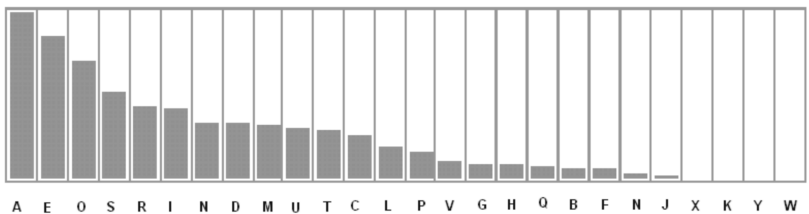
Como quebrar a criptografia de Júlio César

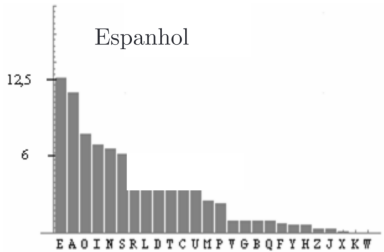
A	B	C	D	E	F	G	H	I	J	K	L
14,6	1,0	3,8	4,9	12,5	1,0	1,3	1,2	6,1	0,4	0,02	2,7

M	N	O	P	Q	R	S	T	U	V	W	X
4,7	5,0	10,7	2,5	1,2	6,5	7,8	4,3	4,6	1,6	0,01	0,2

Y	Z
0,01	0,4

Frequência aproximada das letras em português (%)




Espanhol
12,5
6
EAOINSRLDTCUMPVGBQFYHZJXKW


Inglês
12.7
12
10
8
6
4
2
e t a o i n s h r d l c u m w f g y p b v k j x q z

(53±±+305))6; 4826) 4±.)4±);806*;48+8π*

*60))85;1±(;:±*8+83(88)5*+;46(;88*96*?;8)*±(;485);5*+2:*±(;4956* 2*

(5-4)8π8* ; 4069285);)6+8)4±±;1(±9;48081 ; 8:8±1;48+85;4) 485 +*

528806 81(±9;48; (88;4 (± ? 34;48) 4 ± ; 161 ; : 188; ±?;*

A good glass in the bishop's hostel in the devil's seat forty-one degrees and thirteen minutes north-east and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line form the tree through the shot fifty feet out.

Enigma

$$158.962.555.217.826.360.000 \approx 2^{67}$$

100.000

A única forma de tornar a criptografia de chave privada segura é trocar de chave com frequência.

Informação codificada em bits

$$\mathbb{Z}_2 = \{0, 1\}$$

$$\mathbb{Z}_2 = \{0, 1\}$$

$$0 + 0 = 0$$

$$0 + 1 = 1$$

$$1 + 0 = 1$$

$$1 + 1 = 0$$

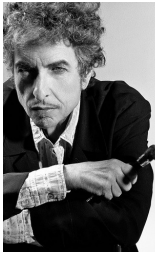
Para mandar uma mensagem com n bits, precisamos de uma chave também com n bits.

$$
\begin{array}{rll}
 & 011011101001 & \text{msg original} \\
+ & 101100011010 & \text{chave} \\
\hline
 & 110111110011 & \text{msg criptografada}
\end{array}
$$

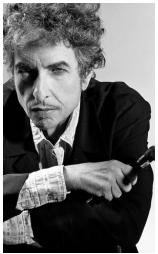
Para que a comunicação seja segura, devemos trocar a chave a cada uso.

A criptografia quântica permite o estabelecimento de chaves para a criptografia de chave privada.

Distribuição de chave quântica



101100011010



101100011010

Protocolo BB84

As duas partes envolvidas no protocolo, Alice e Bob, devem compartilhar um canal quântico de modo que Alice possa enviar bits quânticos para Bob;

Protocolo BB84

Alice deve possuir um gerador de bits quânticos;

Protocolo BB84

Alice e Bob devem possuir aparatos de medição de bits quânticos devidamente calibrados para que os testes X e Z sejam os mesmos para os dois.

Primeiro passo

Alice gera uma sequência de bits quânticos e os mede escolhendo aleatoriamente entre os testes X e Z.

Segundo passo

Alice envia os bits quânticos para Bob após a medição.

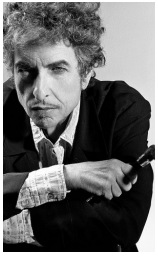
Terceiro passo

Bob recebe os bits quânticos enviados por Alice e os mede escolhendo aleatoriamente entre os testes X e Z.

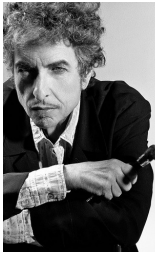
Ao final desse processo, Alice e Bob possuem uma sequência de bits.

Quando Alice e Bob têm certeza de que seus bits são iguais?

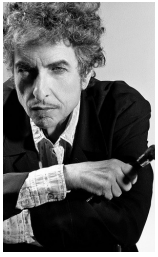
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$



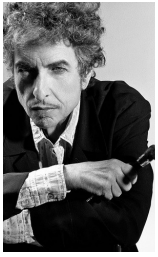
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	$+$			



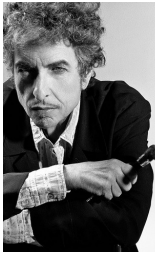
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	$+$	$\|+\rangle$		



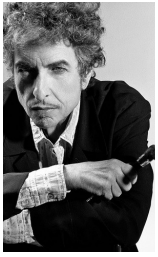
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	$+$	$\|+\rangle$	$\mathcal{Z}$	o



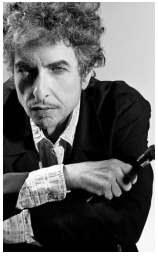
T	R		T	R
X	+		Z	o
Z	o			



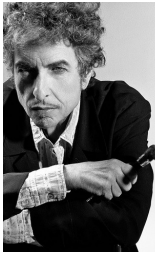
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	$+$		$\mathcal{Z}$	o
$\mathcal{Z}$	o	$\|0\rangle$		



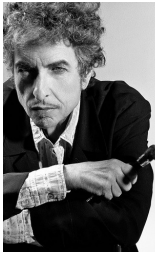
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	$+$		$\mathcal{Z}$	o
$\mathcal{Z}$	o	$\|0\rangle$	$\mathcal{X}$	-



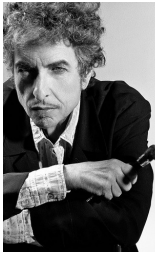
T	R		T	R
X	+		Z	o
Z	o		X	-
Z	1			



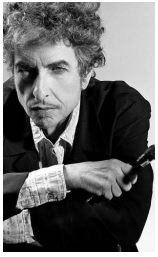
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	+		$\mathcal{Z}$	o
$\mathcal{Z}$	o		$\mathcal{X}$	-
$\mathcal{Z}$	1	$\|1\rangle$		



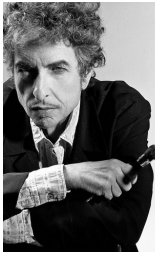
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	+		$\mathcal{Z}$	o
$\mathcal{Z}$	o		$\mathcal{X}$	-
$\mathcal{Z}$	1	$\|1\rangle$	$\mathcal{Z}$	1



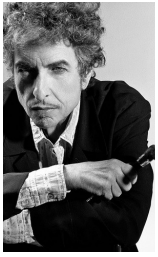
T	R		T	R
X	+		Z	0
Z	0		X	-
Z	1		Z	1
X	+			



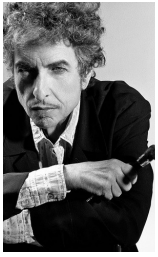
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	+		$\mathcal{Z}$	0
$\mathcal{Z}$	0		$\mathcal{X}$	-
$\mathcal{Z}$	1		$\mathcal{Z}$	1
$\mathcal{X}$	+	$\|+\rangle$		



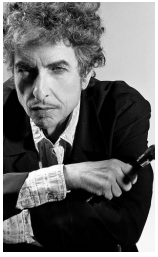
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	$+$		$\mathcal{Z}$	0
$\mathcal{Z}$	0		$\mathcal{X}$	$-$
$\mathcal{Z}$	1		$\mathcal{Z}$	1
$\mathcal{X}$	$+$	$\|+\rangle$	$\mathcal{Z}$	1



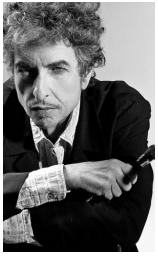
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	+		$\mathcal{Z}$	0
$\mathcal{Z}$	0		$\mathcal{X}$	-
$\mathcal{Z}$	1		$\mathcal{Z}$	1
$\mathcal{X}$	+		$\mathcal{Z}$	1
$\mathcal{X}$	-			



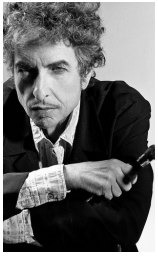
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
X	+		Z	0
Z	0		X	-
Z	1		Z	1
X	+		Z	1
X	-	$\|-\rangle$		



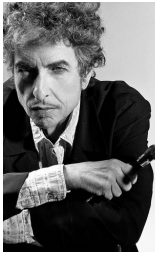
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	+		$\mathcal{Z}$	0
$\mathcal{Z}$	0		$\mathcal{X}$	-
$\mathcal{Z}$	1		$\mathcal{Z}$	1
$\mathcal{X}$	+		$\mathcal{Z}$	1
$\mathcal{X}$	-	$\lvert - \rangle$	$\mathcal{X}$	-



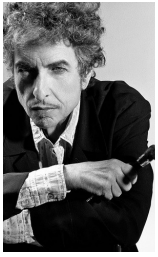
T	R		T	R
X	+		Z	0
Z	0		X	-
Z	1		Z	1
X	+		Z	1
X	-		X	-
Z	1			



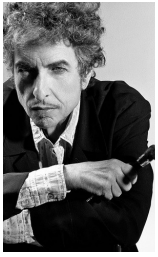
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	+		$\mathcal{Z}$	0
$\mathcal{Z}$	0		$\mathcal{X}$	-
$\mathcal{Z}$	1		$\mathcal{Z}$	1
$\mathcal{X}$	+		$\mathcal{Z}$	1
$\mathcal{X}$	-		$\mathcal{X}$	-
$\mathcal{Z}$	1	$\|1\rangle$		



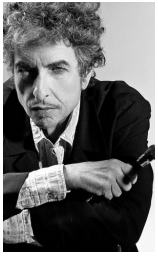
$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	+		$\mathcal{Z}$	0
$\mathcal{Z}$	0		$\mathcal{X}$	-
$\mathcal{Z}$	1		$\mathcal{Z}$	1
$\mathcal{X}$	+		$\mathcal{Z}$	1
$\mathcal{X}$	-		$\mathcal{X}$	-
$\mathcal{Z}$	1	$\|1\rangle$	$\mathcal{Z}$	1



$\mathcal{T}$	$\mathcal{R}$		$\mathcal{T}$	$\mathcal{R}$
$\mathcal{X}$	+		$\mathcal{Z}$	0
$\mathcal{Z}$	0		$\mathcal{X}$	-
$\mathcal{Z}$	1		$\mathcal{Z}$	1
$\mathcal{X}$	+		$\mathcal{Z}$	1
$\mathcal{X}$	-		$\mathcal{X}$	-
$\mathcal{Z}$	1		$\mathcal{Z}$	1



T	R		T	R
X	+		Z	0
Z	0		X	-
Z	1		Z	1
X	+		Z	1
X	-		X	-
Z	1		Z	1



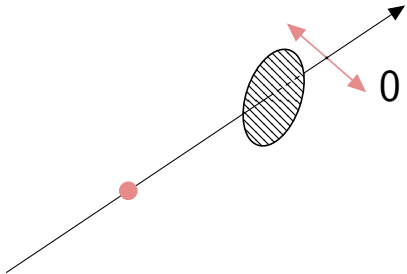
Quando os testes escolhidos são iguais!

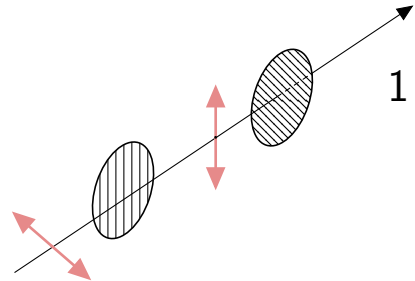
Terceiro Passo

Alice e Bob anunciam que teste realizaram. Eles descartam os bits em que os testes foram diferentes e guardam os bits em que os testes foram iguais.

Alice e Bob possuem agora uma sequência perfeitamente correlacionada de bits, ou seja, uma chave criptográfica.

Por que esse protocolo é seguro?


0


1

Verificação de erros

Quarto Passo

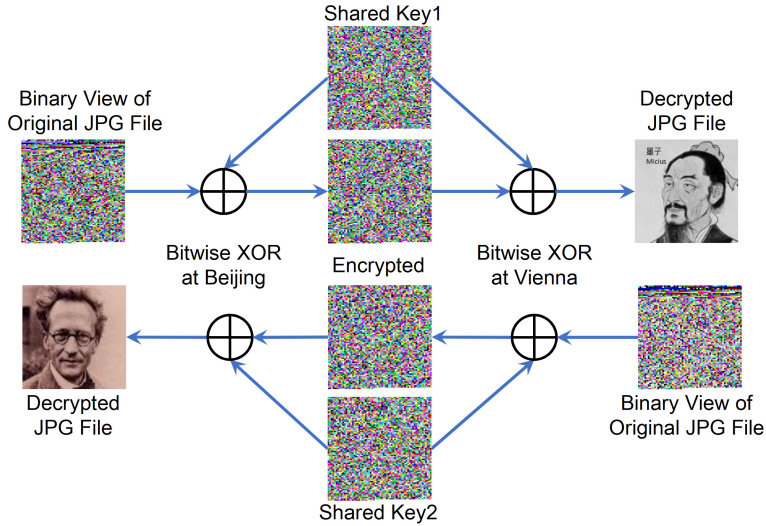
Bob envia a Alice uma fração dos bits correlacionados obtidos nesse processo.

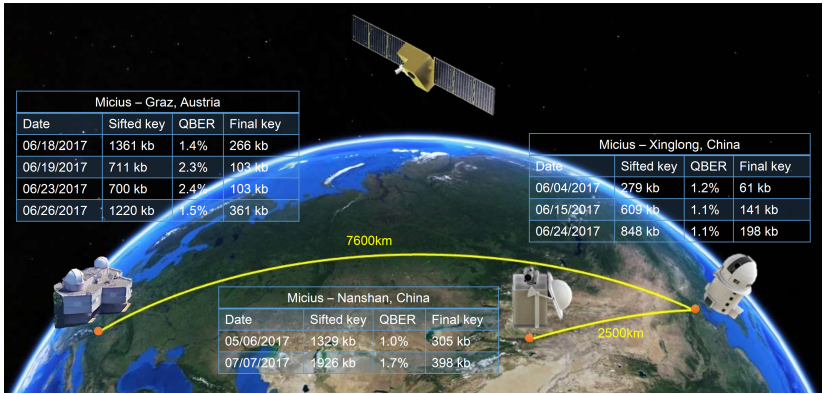
Qualquer erro pode ser detectado por Alice se ela comparar seus bits com os bits enviados por Bob!

Se temos uma espiã tentando obter a informação sobre o bit enviado por Alice, os bits de Bob não estarão mais perfeitamente correlacionados os bits de Alice!

Satellite-relayed intercontinental quantum network

Sheng-Kai Liao[1,2], Wen-Qi Cai[1,2], Johannes Handsteiner[3,4], Bo Liu[4,5], Juan Yin[1,2], Liang Zhang[2,6], Dominik Rauch[3,4], Matthias Fink[4], Ji-Gang Ren[1,2], Wei-Yue Liu[1,2], Yang Li[1,2], Qi Shen[1,2], Yuan Cao[1,2], Feng-Zhi Li[1,2], Jian-Feng Wang[7], Yong-Mei Huang[8], Lei Deng[9], Tao Xi[10], Lu Ma[11], Tai Hu[12], Li Li[1,2], Nai-Le Liu[1,2], Franz Koidl[13], Peiyuan Wang[13], Yu-Ao Chen[1,2], Xiang-Bin Wang[2], Michael Steindorfer[13], Georg Kirchner[13], Chao-Yang Lu[1,2], Rong Shu[2,6], Rupert Ursin[3,4], Thomas Scheidl[3,4], Cheng-Zhi Peng[1,2], Jian-Yu Wang[2,6], Anton Zeilinger[3,4], Jian-Wei Pan[1,2]


Shared Key1
Binary View of
Original JPG File
Decrypted
JPG File
墨子
Micius
Bitwise XOR
at Beijing
Encrypted
Bitwise XOR
at Vienna
Decrypted
JPG File
Binary View of
Original JPG File
Shared Key2


Micius – Graz, Austria
Date | Sifted key | QBER | Final key
06/18/2017 | 1361 kb | 1.4% | 266 kb
06/19/2017 | 711 kb | 2.3% | 103 kb
06/23/2017 | 700 kb | 2.4% | 103 kb
06/26/2017 | 1220 kb | 1.5% | 361 kb
Micius – Xinglong, China
Date | Sifted key | QBER | Final key
06/04/2017 | 279 kb | 1.2% | 61 kb
06/15/2017 | 609 kb | 1.1% | 141 kb
06/24/2017 | 848 kb | 1.1% | 198 kb
7600km
Micius – Nanshan, China
Date | Sifted key | QBER | Final key
05/06/2017 | 1329 kb | 1.0% | 305 kb
07/07/2017 | 1926 kb | 1.7% | 398 kb
2500km

Long-distance transmission of quantum key distribution coexisting with classical optical communication over weakly-coupled few-mode fiber

Bi-Xiao Wang,[1,2] Yingqiu Mao,[1,2] Lei Shen,[3] Lei Zhang,[3] Xiao-Bo Lan,[3] Dawei Ge,[4] Yuyang Gao,[4] Juhao Li,[4] Yan-Lin Tang,[5] Shi-Biao Tang,[5] Jun Zhang,[1,2] Teng-Yun Chen,[1,2,*] and Jian-Wei Pan[1,2,†]

[1] *Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, P. R. China*

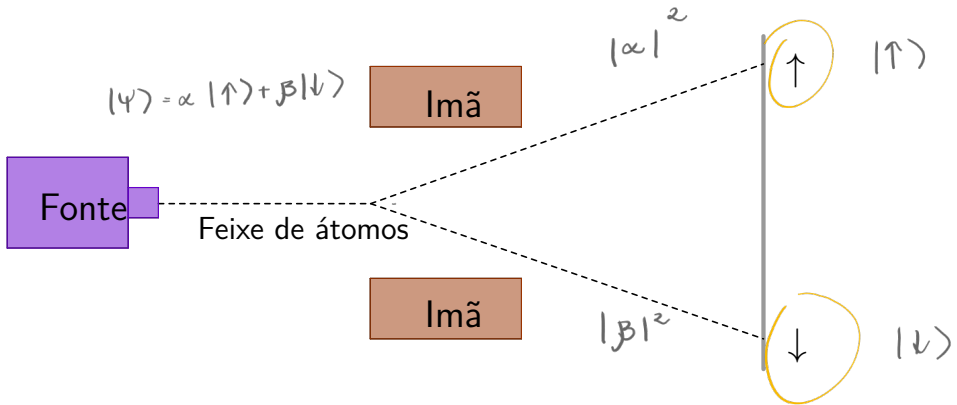
[2] *CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, P. R. China*

[3] *State Key Laboratory of Optical Fiber and Cable Manufacture Technology, Yangtze Optical Fiber and Cable Joint Stock Limited Company, Wuhan, 430070, P. R. China*

[4] *State Key Laboratory of Advanced Optical Communication Systems and Networks, Peking University, Beijing 100871, P. R. China*

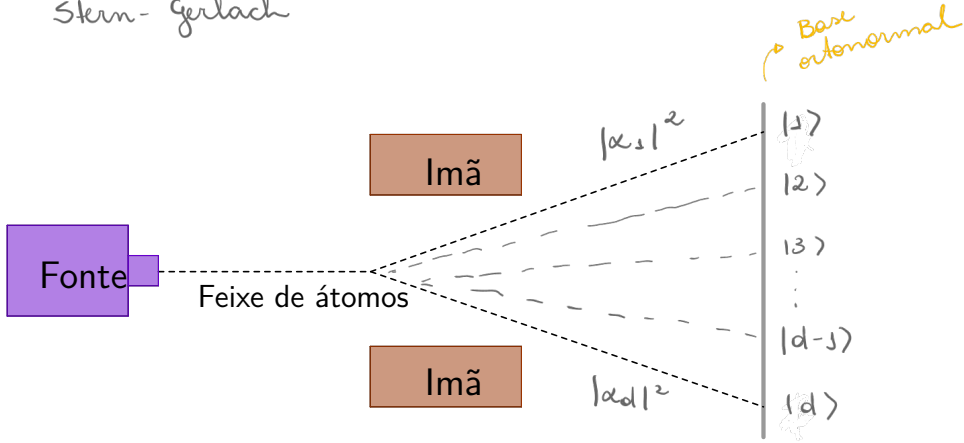
[5] *QuantumCTek Corporation Limited, Hefei, Anhui 230088, P. R. China*

Spin


$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$
Imã
Fonte
Feixe de átomos
Imã
$|\alpha|^2$
$|\uparrow\rangle$
$|\beta|^2$
$|\downarrow\rangle$

$$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$$

Stern - Gerlach



$$|\psi\rangle = \alpha_1 |1\rangle + \alpha_2 |2\rangle + \dots + \alpha_d |d\rangle$$