Protocol E91

Isabelle Viarouge
isabelle.viarouge@usherbrooke.ca

26th of February, 2026

UNIVERSITÉ DE SHERBROOKE

Who are we?

Quantum algorithm laboratory

INSTITUT QUANTIQUE

UdS Université de Sherbrooke

Quantum AlgoLab

Get started with Quantum

QUANTUM ALGOLAB

RESEARCH

Scientific collaborations
Quantum programming support
Access to *IBM Quantum Network* systems

COMMUNITY

Acces to talent
Quantum events
Technical communities of practice

TRAINING

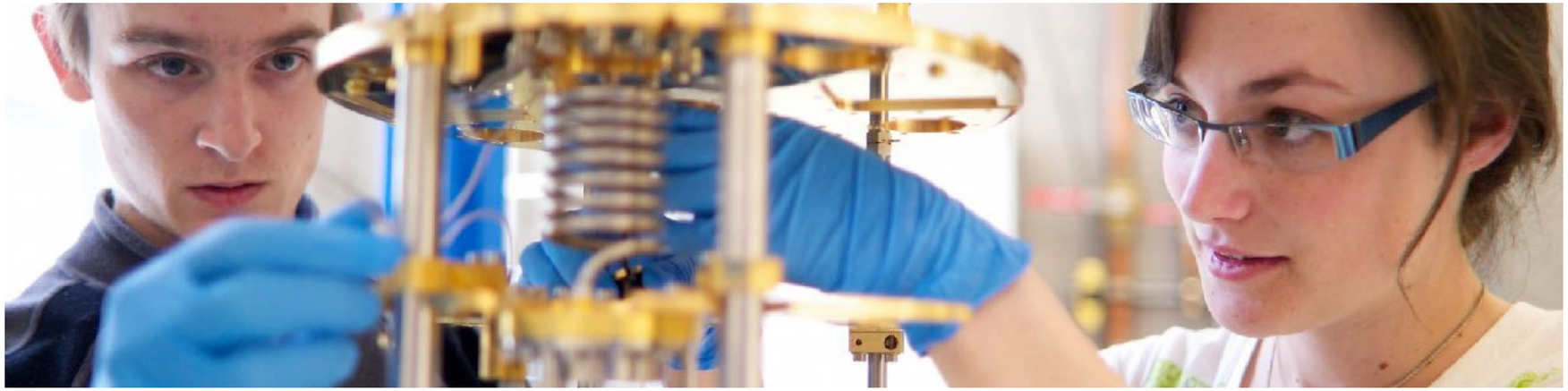
Institut quantique expertise
Unique quantum programming workshops
In-house seminars

Nous contacter : AlgoLabquantique@usherbrooke.ca

INSTITUT QUANTIQUE
UNIVERSITÉ DE SHERBROOKE

Institut quantique

We place our 250 students and postdocs at the center of research in an open and collaborative environment to accelerate the transition from science to quantum technologies



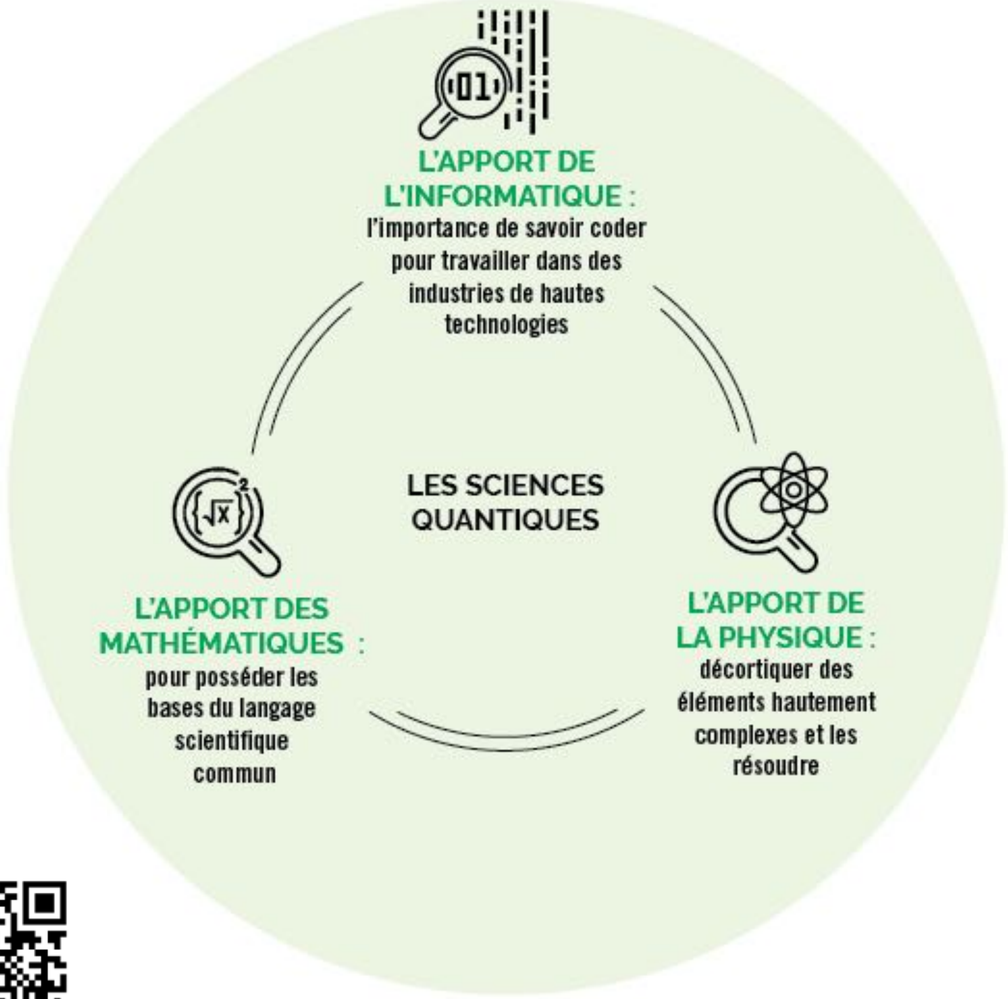
Our 32 faculty members come from 4 faculties and 7 departments
$80M invested in 10 years and a new building is now open

Bachelor’s degree in Quantum information sciences

Nouvelle cohorte à l’automne 2026

<u>Formation professionnalisante</u>

- Programme interdisciplinaire
- Parcours coop
- Projets intégrateurs



Pour en savoir plus

Université de Sherbrooke

Institut quantique

Cooperative R&D environment for Academia and Industry

Quantum tech platforms

Quantum Fab Lab

Quantum computing platform

Plan

- Presentation
- Cryptography
- The qubit
- The photon: messenger of quantum information
- Entanglement and CHSH inequality
- Protocol E91
- Hands-on session

Plan

- ✓ Presentation
- Cryptography
- The qubit
- The photon: messenger of quantum information
- Entanglement and CHSH inequality
- Protocol E91
- Hands-on session

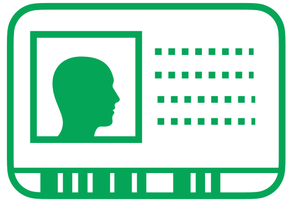
Plan

- ✓ Presentation
- Cryptography
- The qubit
- The photon: messenger of quantum information
- Entanglement and CHSH inequality
- Protocol E91
- Hands-on session

Cryptography

Confidentiality

Authenticity



Message integrity

Cryptography

Confidentiality

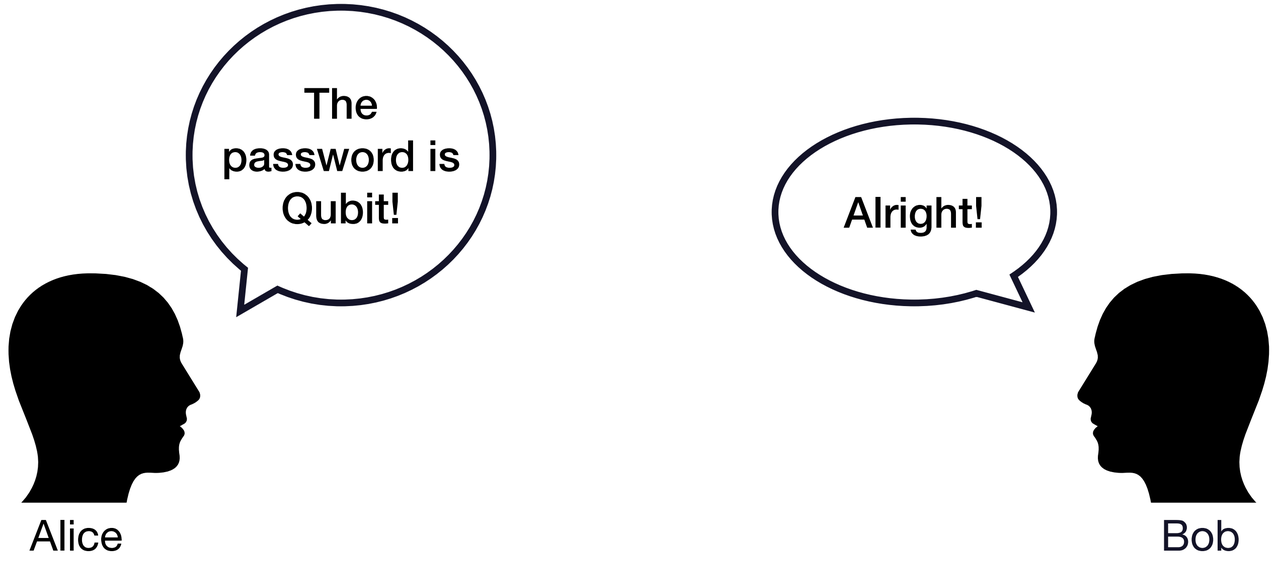
Authenticity

Message integrity

Cryptography

Confidentiality

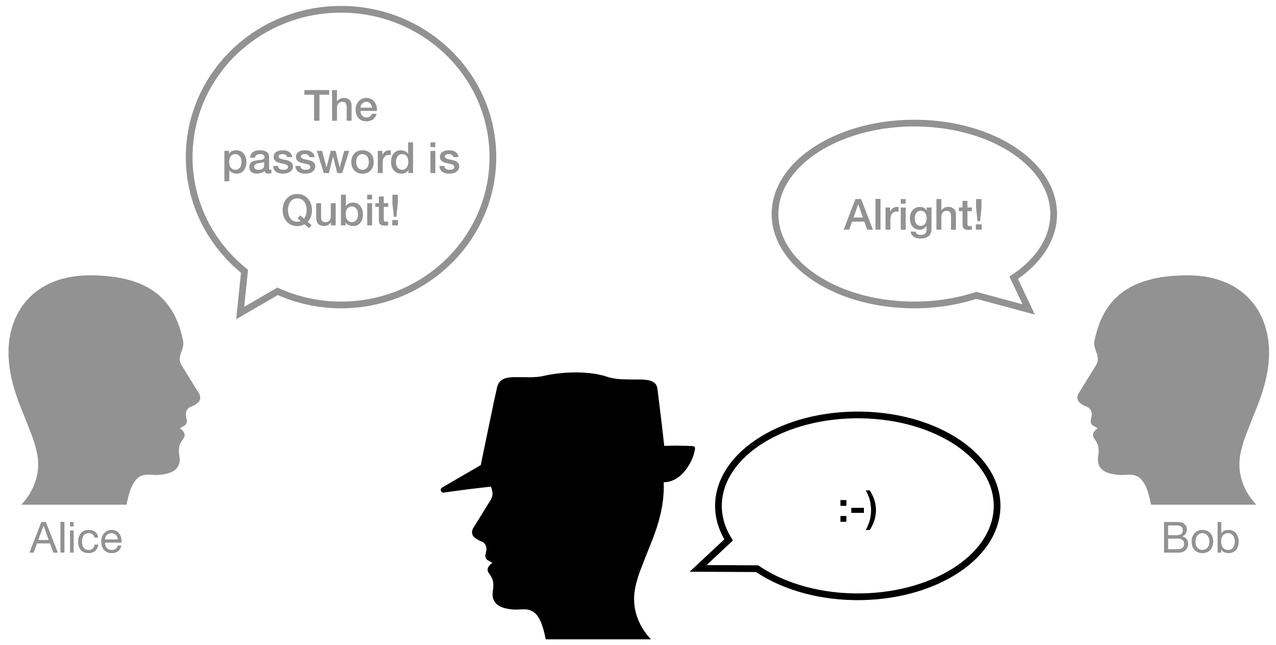
Goal: Ensure that the message is inaccessible to an eavesdropper!



Cryptography

Confidentiality

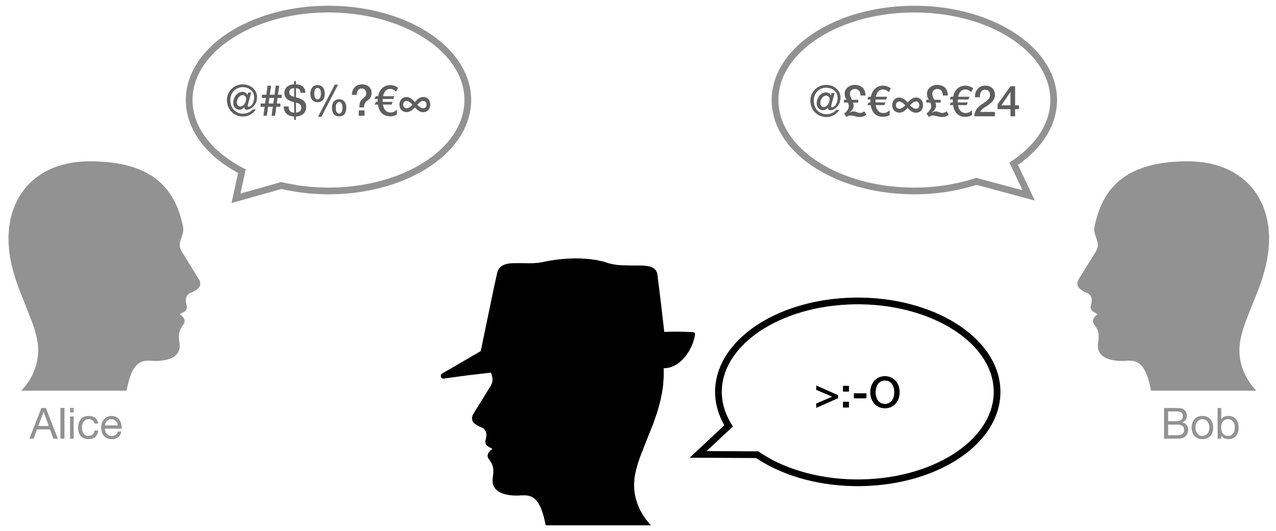
Goal: Ensure that the message is inaccessible to an eavesdropper!



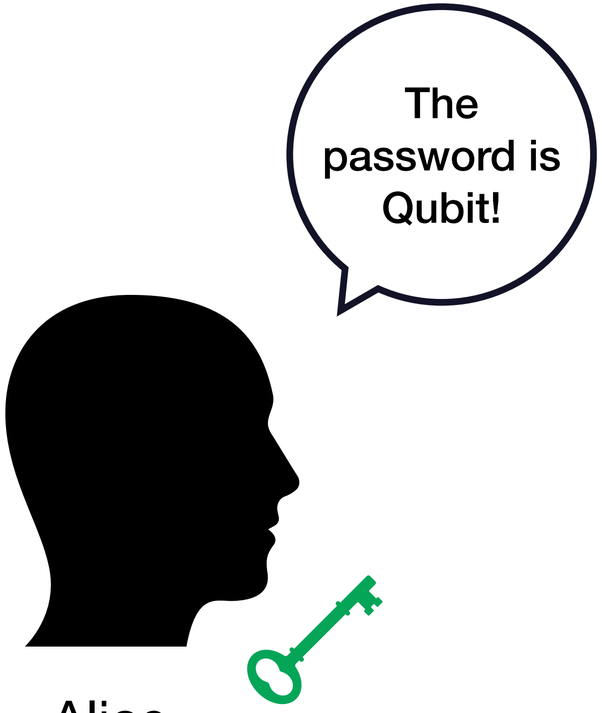
Cryptography

Confidentiality

Goal: Ensure that the message is inaccessible to an eavesdropper!



Symmetric Key



Alice

Bob

Symmetric Key

Alice

Bob

Symmetric Key

Symmetric Key

Symmetric Key

Property

- One private key for encoding and decoding

Symmetric Key

Property

- One private key for encoding and decoding

Pros

- Low computational ressource requirements

Symmetric Key

Property

- One private key for encoding and decoding

Pros

- Low computational ressource requirements

Cons

- Key distribution

Symmetric Key

Property

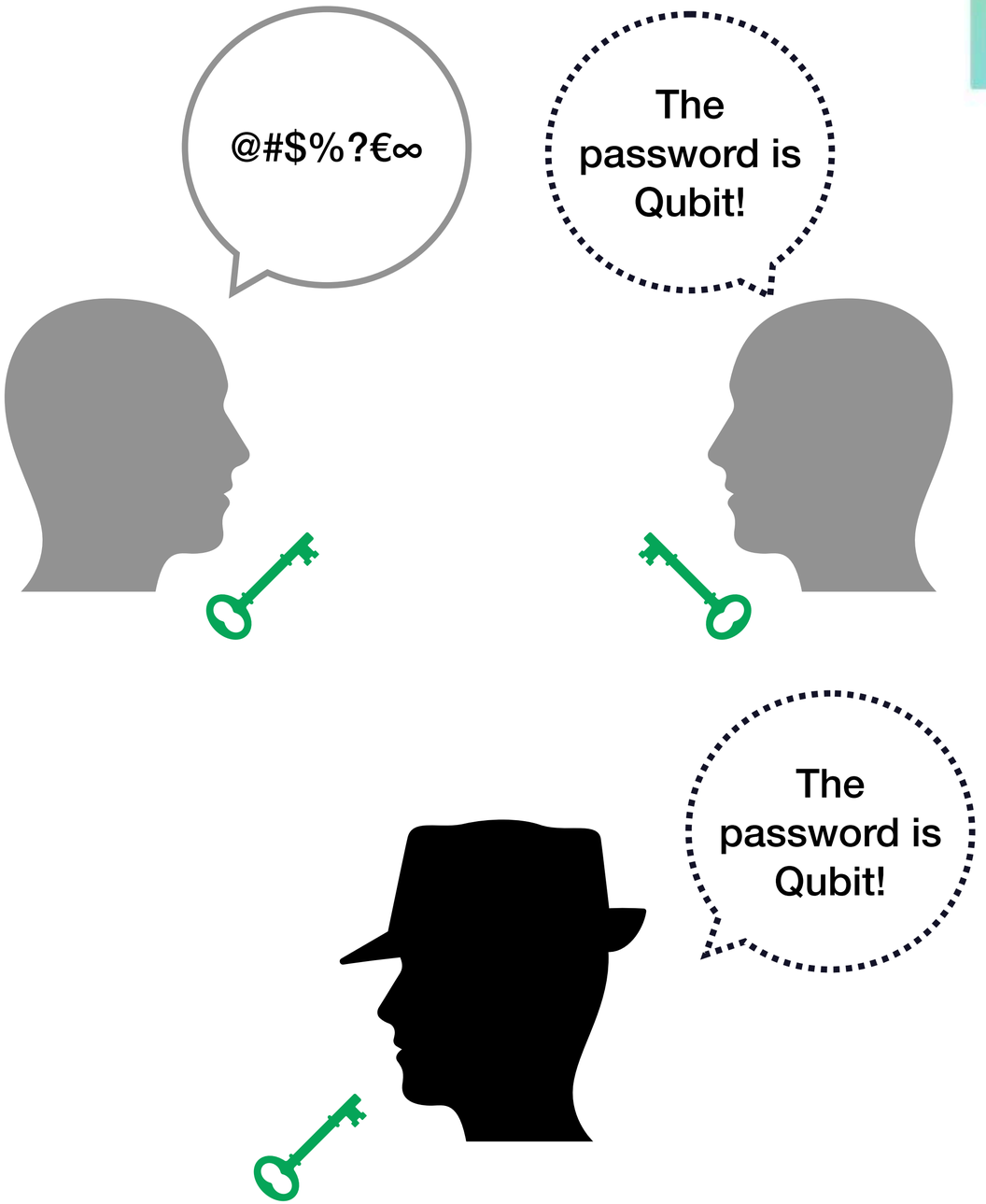
- One private key for encoding and decoding

Pros

- Low computational ressource requirements

Cons

- Key distribution



Asymmetric Key

Properties

- Public key for encryption
- Private key for decryption

Asymmetric Key

Properties

- Public key for encryption
- Private key for decryption

Pros

- Public key distribution

Asymmetric Key

Properties

- Public key for encryption
- Private key for decryption

Pros

- Public key distribution

Cons

- Slow and computationally expensive

Motivation

Quantum cryptography

Motivation

Quantum cryptography

Decrypting messages

- Asymmetric encryption protocols (e.g. RSA with Shor's algorithm)
- Symmetric encryption protocols (e.g. AES with Grover's algorithm)

Motivation

Quantum cryptography

Decrypting messages

- Asymmetric encryption protocols (e.g. RSA with Shor's algorithm)
- Symmetric encryption protocols (e.g. AES with Grover's algorithm)

Quantum cryptography

Quantum Cryptography

Cryptography methods exploiting the properties of quantum mechanics, such as

- Superposition
- No-cloning theorem
- Entanglement

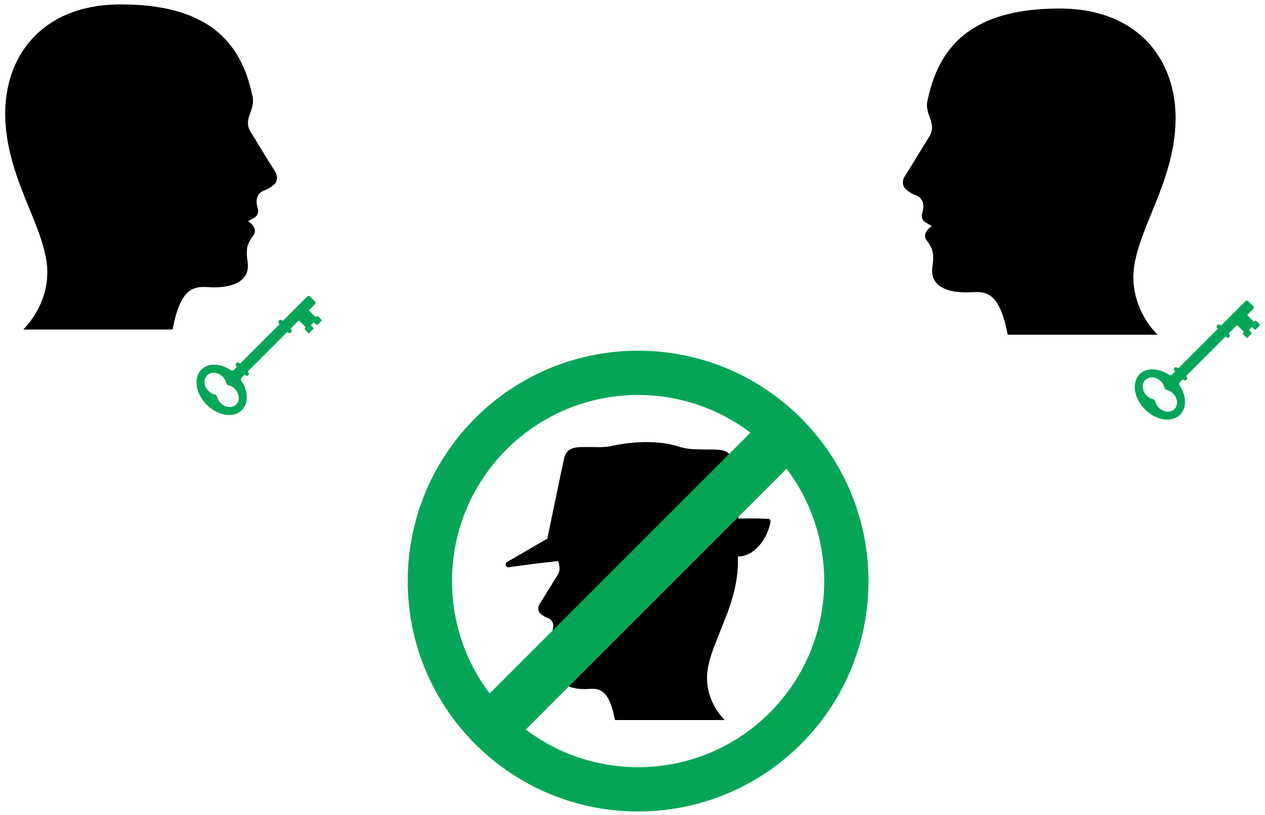
Quantum Key Distribution (QKD)

Quantum Key Distribution

Deploy a symmetric key at Alice's and Bob's using the properties of quantum mechanics

Perfect theoretical security

Spy detection



Protocol E91

APS Journals All Journals Physics Magazine

Physical Review Letters

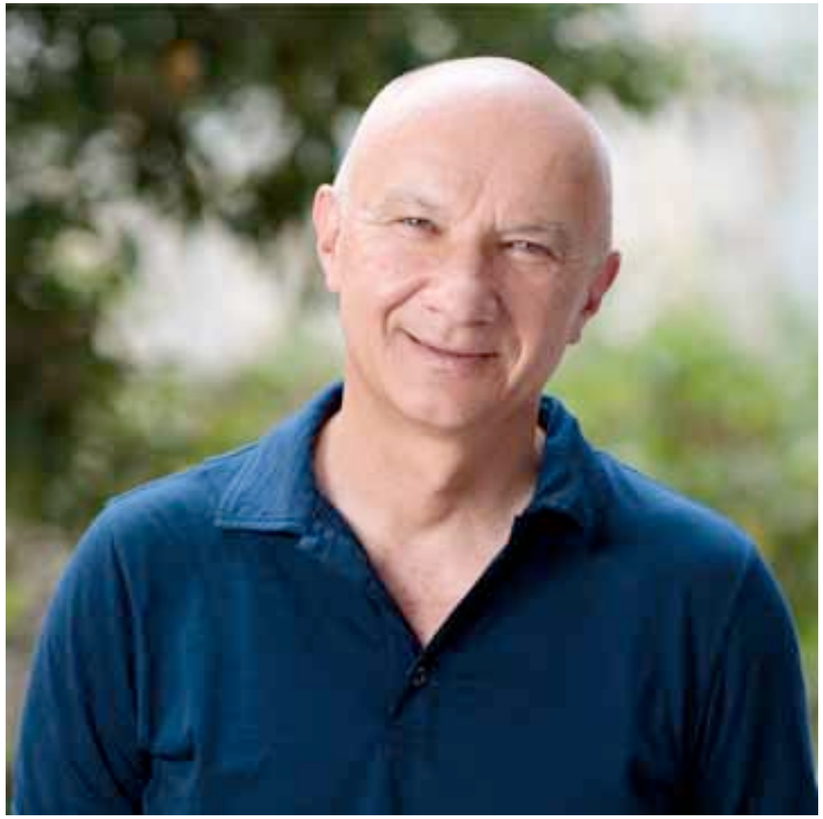
Quantum cryptography based on Bell's theorem

Artur K. Ekert

Show more

Phys. Rev. Lett. **67**, 661 – **Published 5 August, 1991**

DOI: https://doi.org/10.1103/PhysRevLett.67.661



Plan

- ✓ Presentation
- Cryptography
- The qubit
- The photon: messenger of quantum information
- Entanglement and CHSH inequality
- Protocol E91
- Hands-on session

Plan

- ✓ Presentation
- ✓ Cryptography
- The qubit
- The photon: messenger of quantum information
- Entanglement and CHSH inequality
- Protocol E91
- Hands-on session

Plan

- ✓ Presentation
- ✓ Cryptography
- The qubit
- The photon: messenger of quantum information
- Entanglement and CHSH inequality
- Protocol E91
- Hands-on session

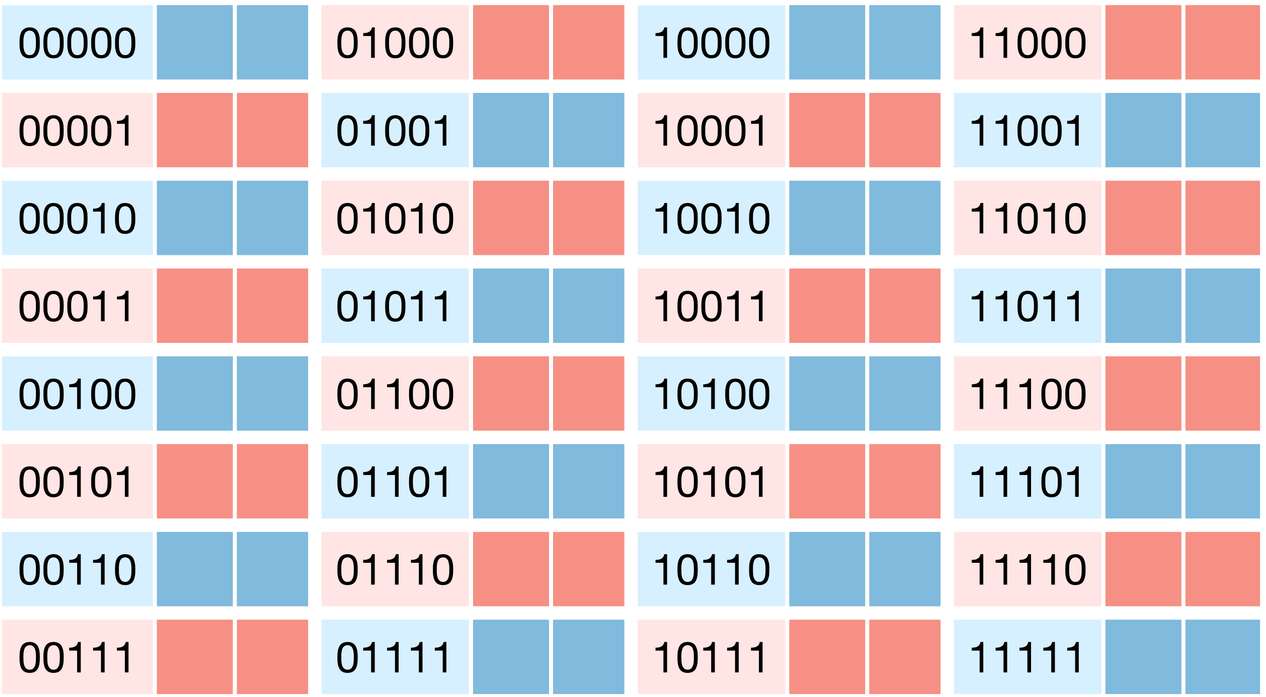
The Classical Bit

Classical information

- The bit = the information unit

  0 or 1

- Information can be encoded in chains of bits.



The Classical Bit

Classical information

- The bit = the information unit

  0 or 1

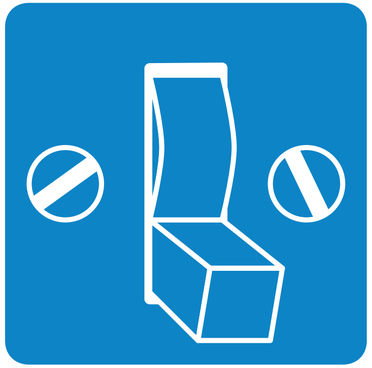
- Information can be encoded in chains of bits.
- With 5 bits we can encode :
  - Numbers from 0 to 31
  - The alphabet

00000	0	a	01000	8	i	10000	16	q	11000	24	y
00001	1	b	01001	9	j	10001	17	r	11001	25	z
00010	2	c	01010	10	k	10010	18	s	11010	26	
00011	3	d	01011	11	l	10011	19	t	11011	27	
00100	4	e	01100	12	m	10100	20	u	11100	28	
00101	5	f	01101	13	n	10101	21	v	11101	29	
00110	6	g	01110	14	o	10110	22	w	11110	30	
00111	7	h	01111	15	p	10111	23	x	11111	31	

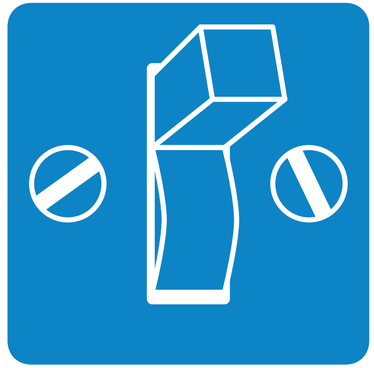
Physical Representation

Classical information

Bit



0



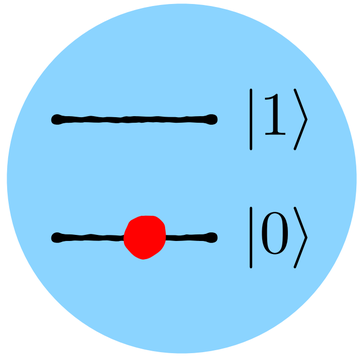
1

Quantum Information

The qubit

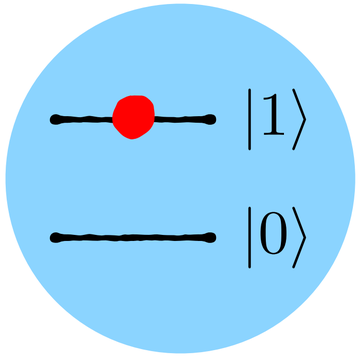
- The qubit = quantum bit
- Takes a continuum of values

0



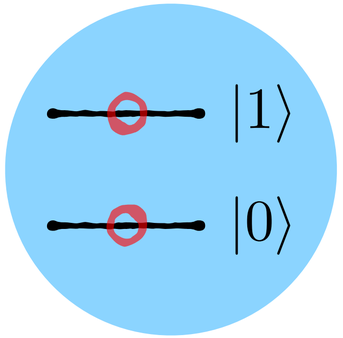
ou

1



ou

"0 and 1"

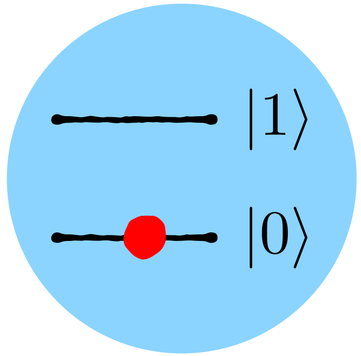


Quantum Information

The qubit

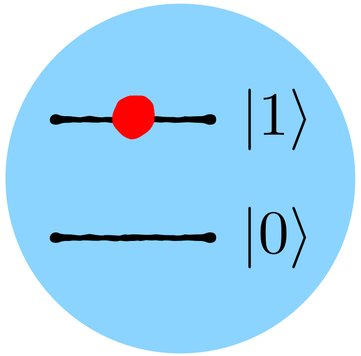
- The qubit = quantum bit
- Takes a continuum of values

0



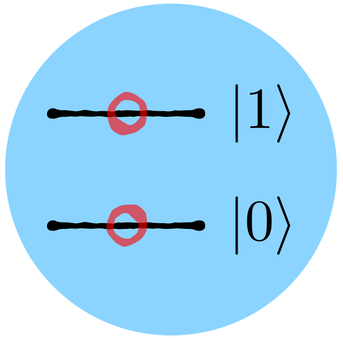
ou

1



ou

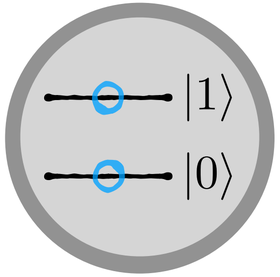
"0 and 1"



Superposition state

Dirac Notation

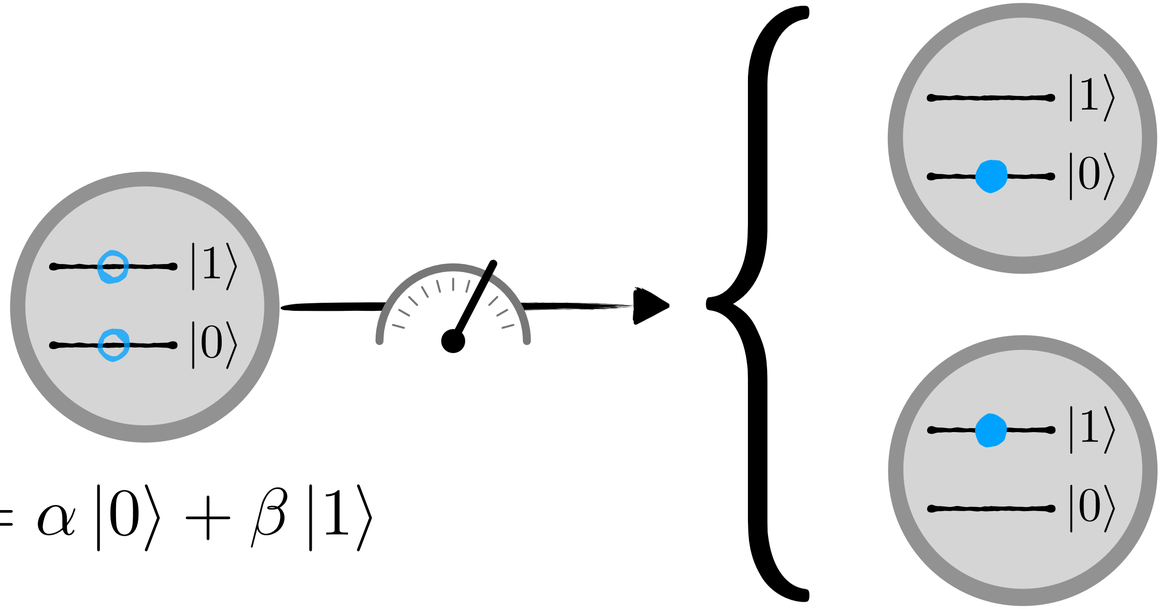
Superposition



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

Dirac Notation

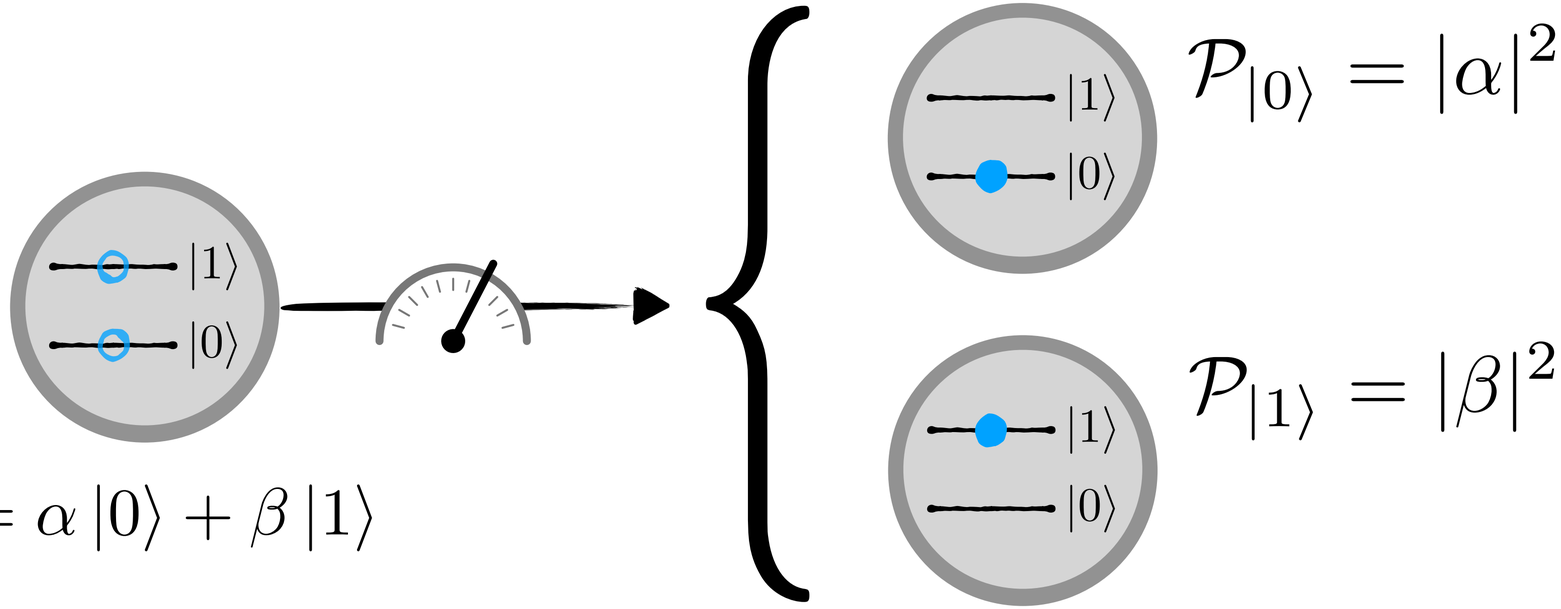
Superposition



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

Dirac Notation

Superposition



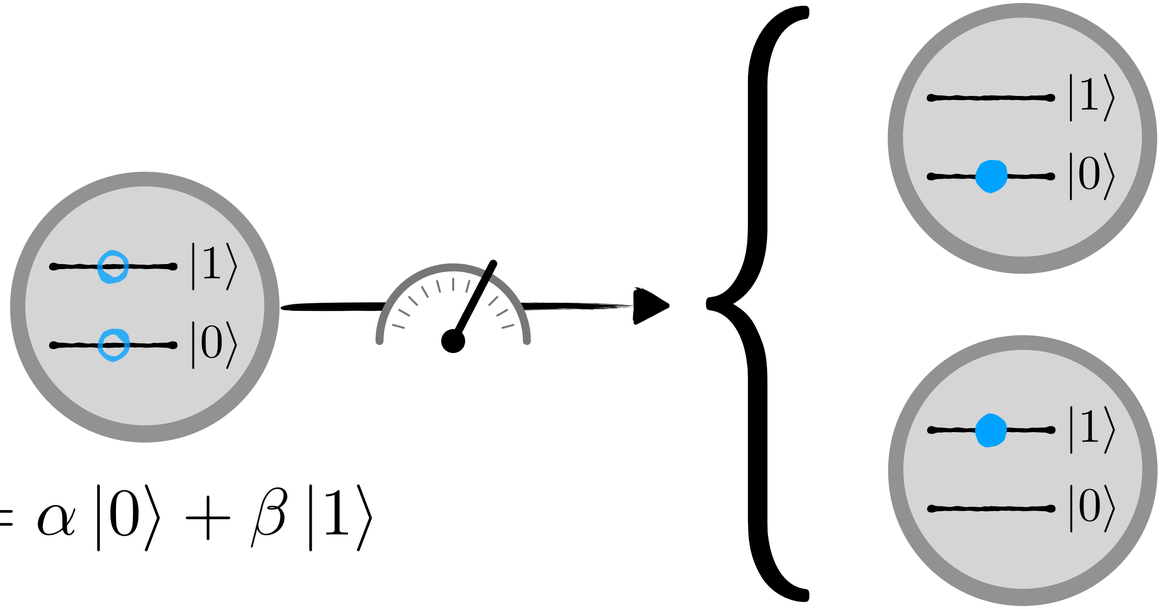
$$\mathcal{P}_{|0\rangle} = |\alpha|^2$$

$$\mathcal{P}_{|1\rangle} = |\beta|^2$$

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

Dirac Notation

Superposition



$$\mathcal{P}_{|0\rangle} = |\alpha|^2$$

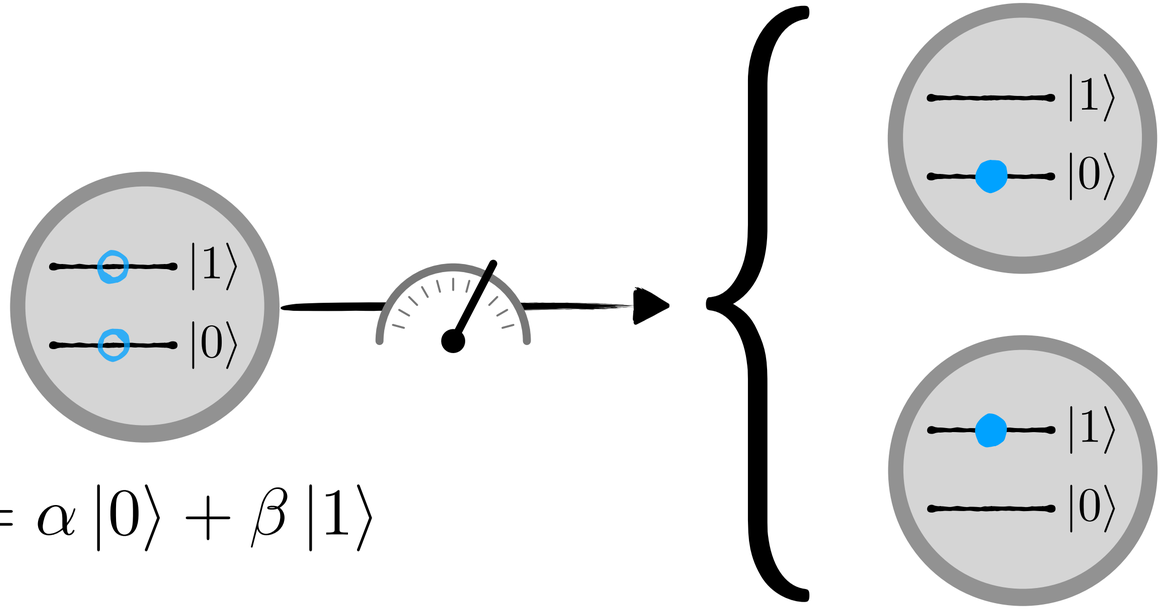
$$\mathcal{P}_{|1\rangle} = |\beta|^2$$

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

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

Dirac Notation

Superposition



$$\mathcal{P}_{|0\rangle} = |\alpha|^2$$

$$\mathcal{P}_{|1\rangle} = |\beta|^2$$

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

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

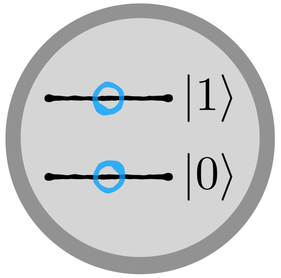
Examples :

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

Physical Representation

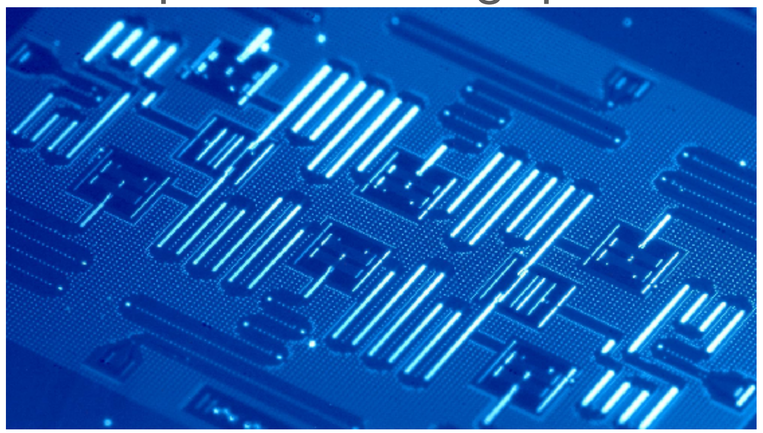
Quantum Information

Qubit

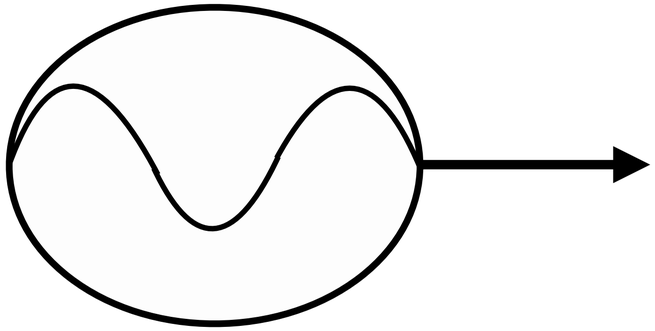


$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Supraconducting qubits



IBM



Plan

- ✓ Presentation
- ✓ Cryptography
- The qubit
- The photon: messenger of quantum information
- Entanglement and CHSH inequality
- Protocol E91
- Hands-on session

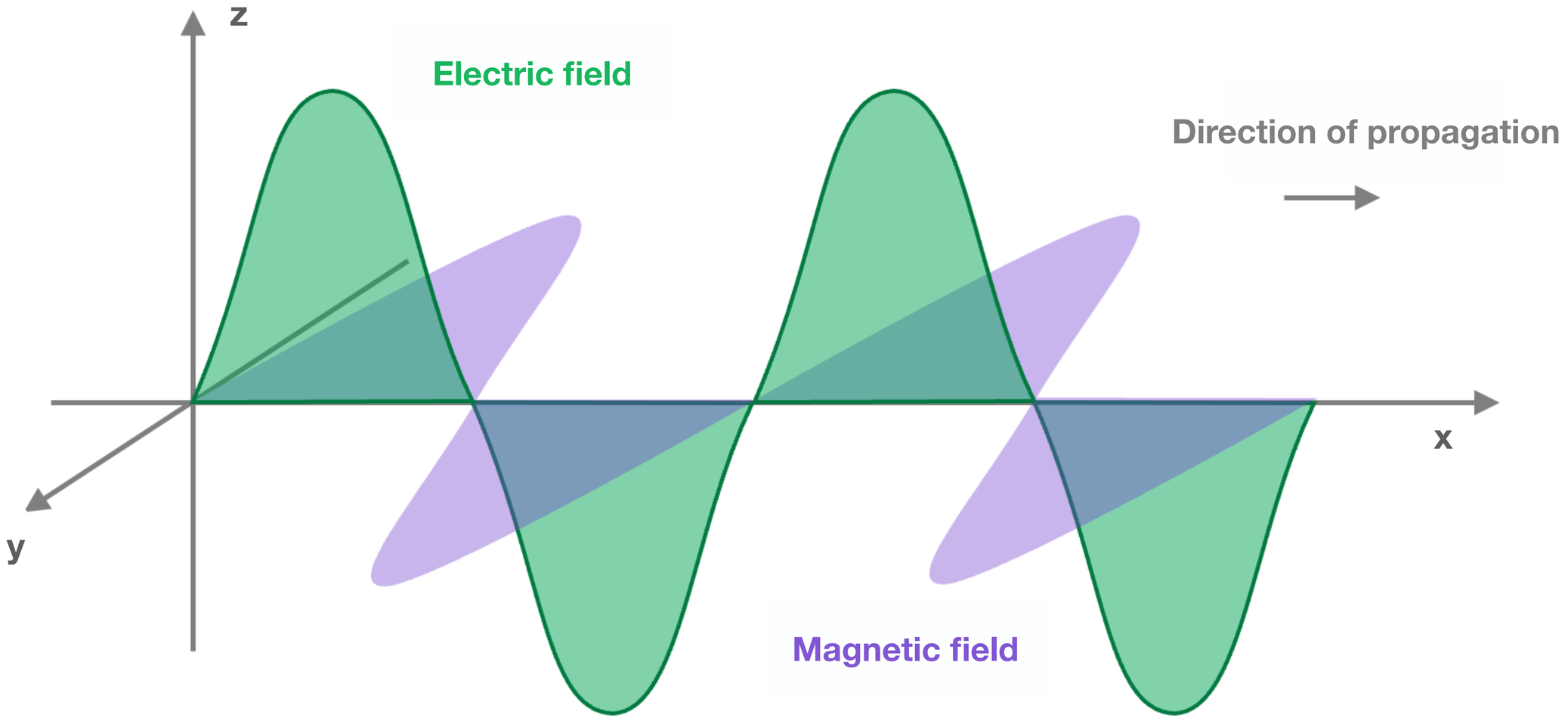
Plan

- ✓ Presentation
- ✓ Cryptography
- ✓ The qubit
- The photon: messenger of quantum information
- Entanglement and CHSH inequality
- Protocol E91
- Hands-on session

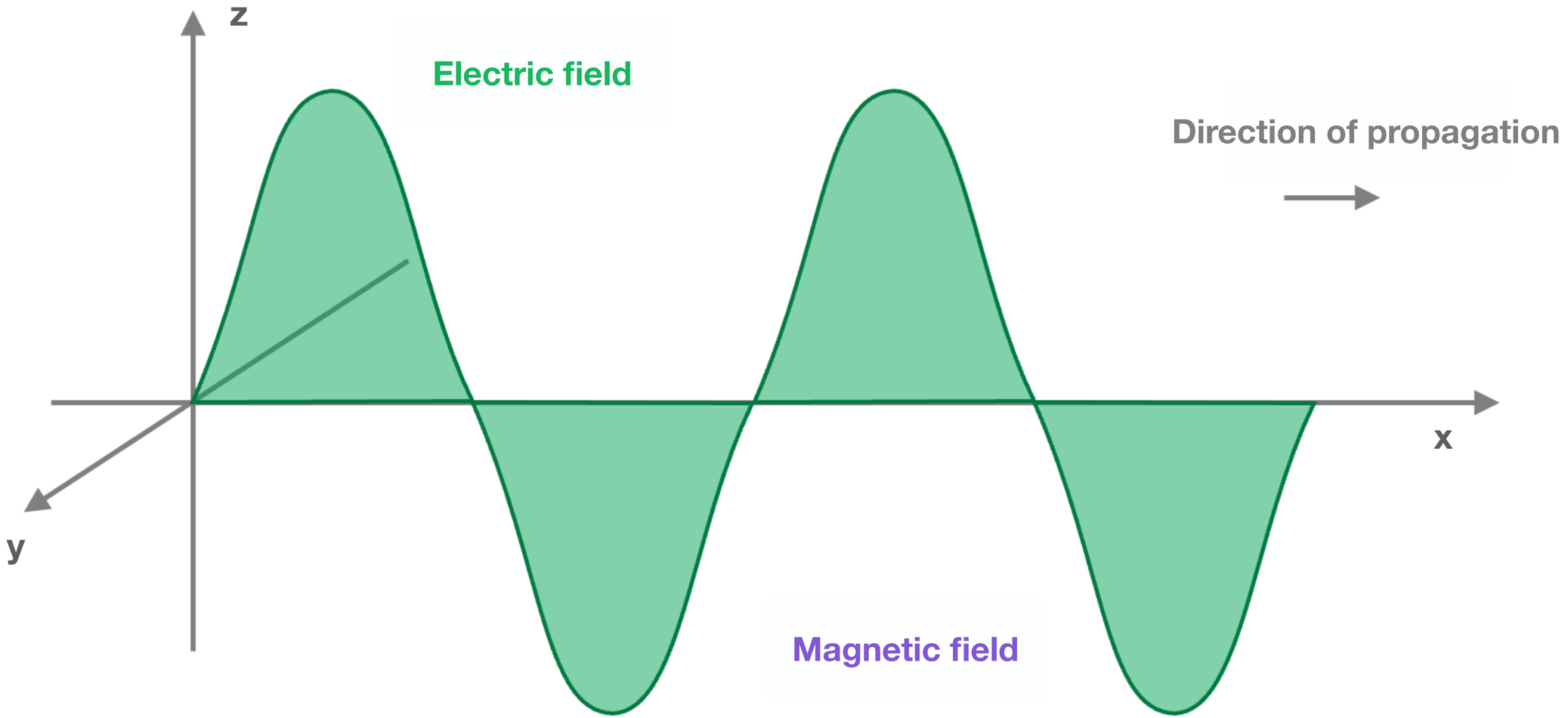
Plan

- ✓ Presentation
- ✓ Cryptography
- ✓ The qubit
- The photon: messenger of quantum information
- Entanglement and CHSH inequality
- Protocol E91
- Hands-on session

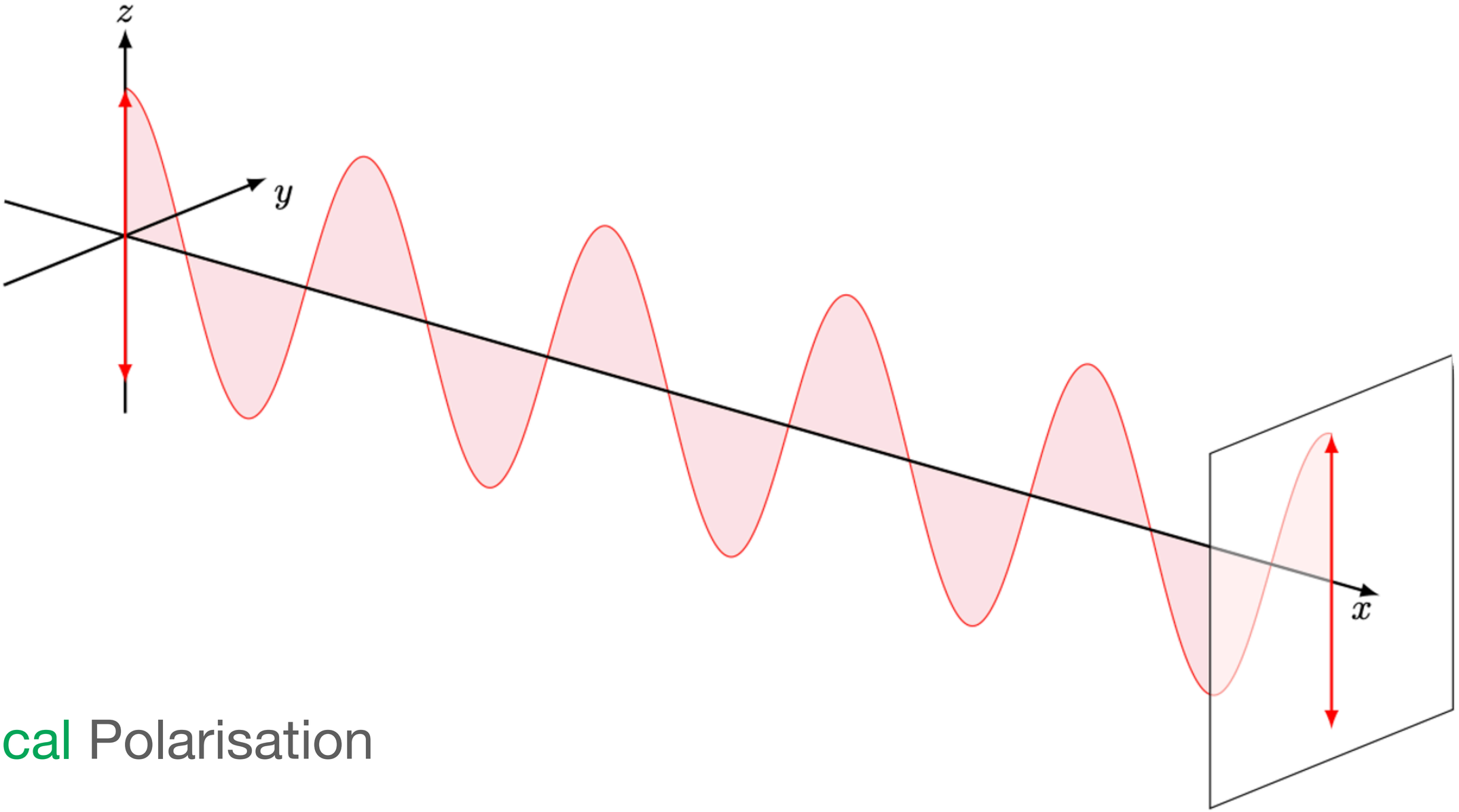
Light


z
Electric field
Direction of propagation
x
y
Magnetic field

Polarisation: a Quantum Property

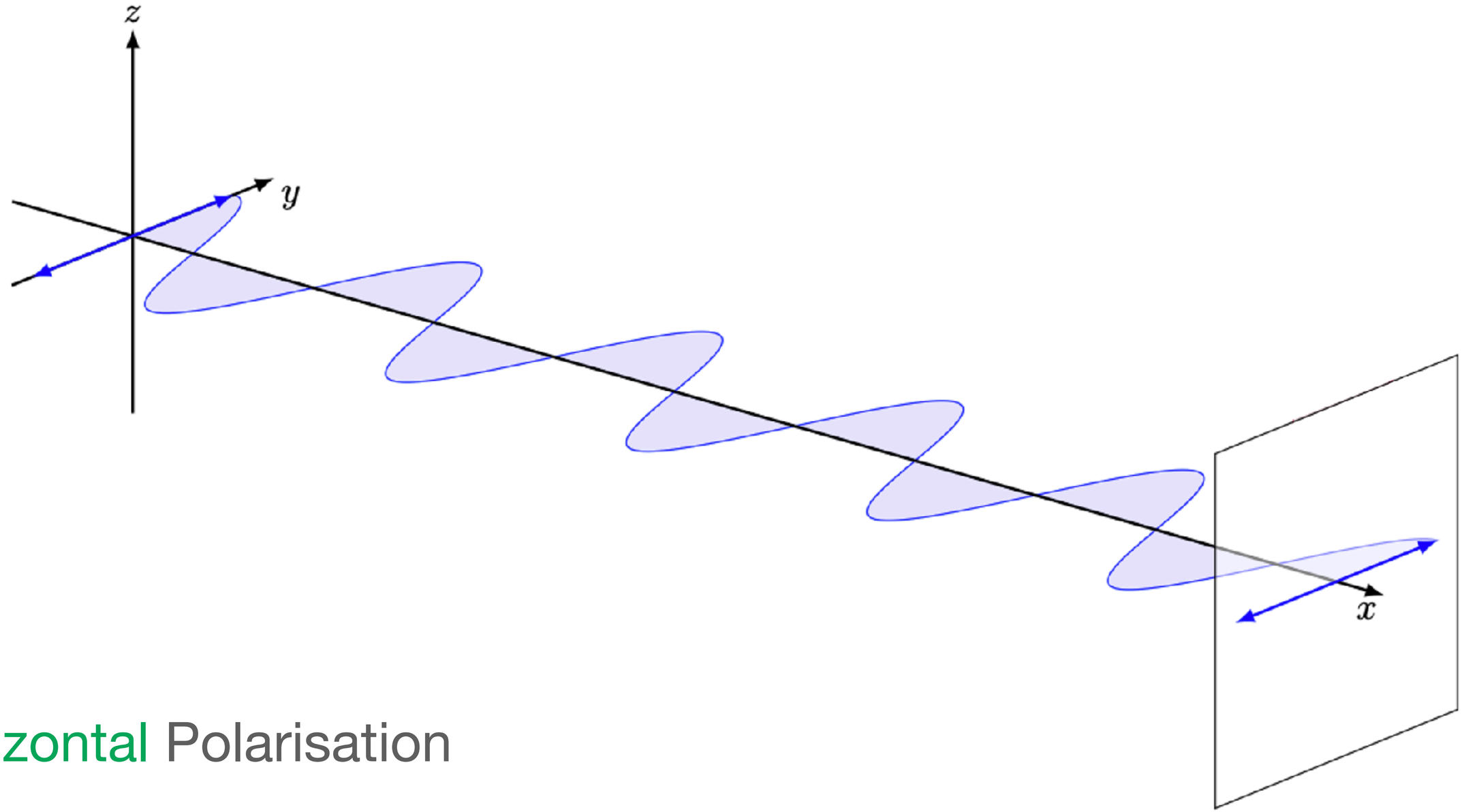


Polarisation: a Quantum Property



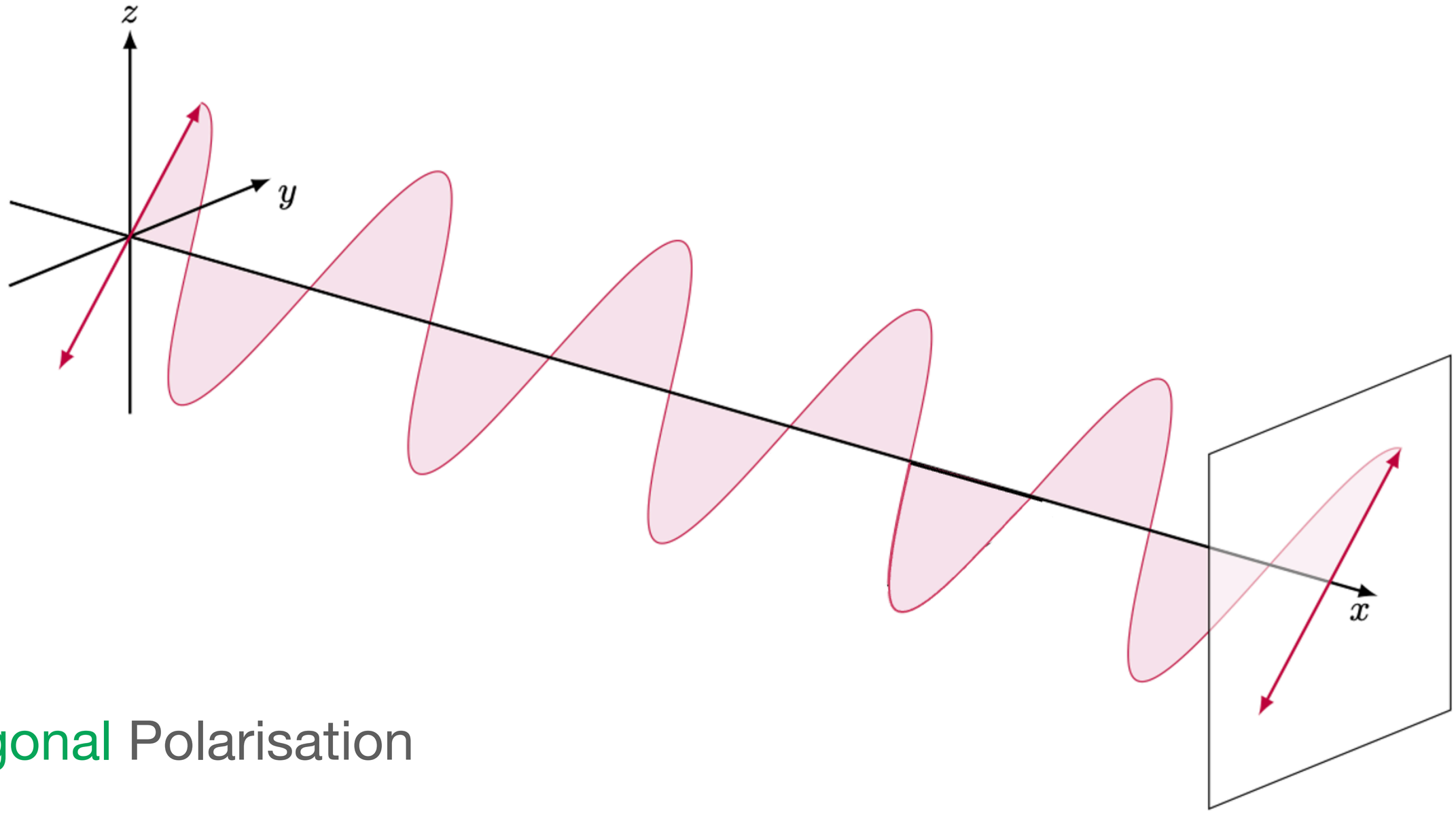
Vertical Polarisation

Polarisation: a Quantum Property



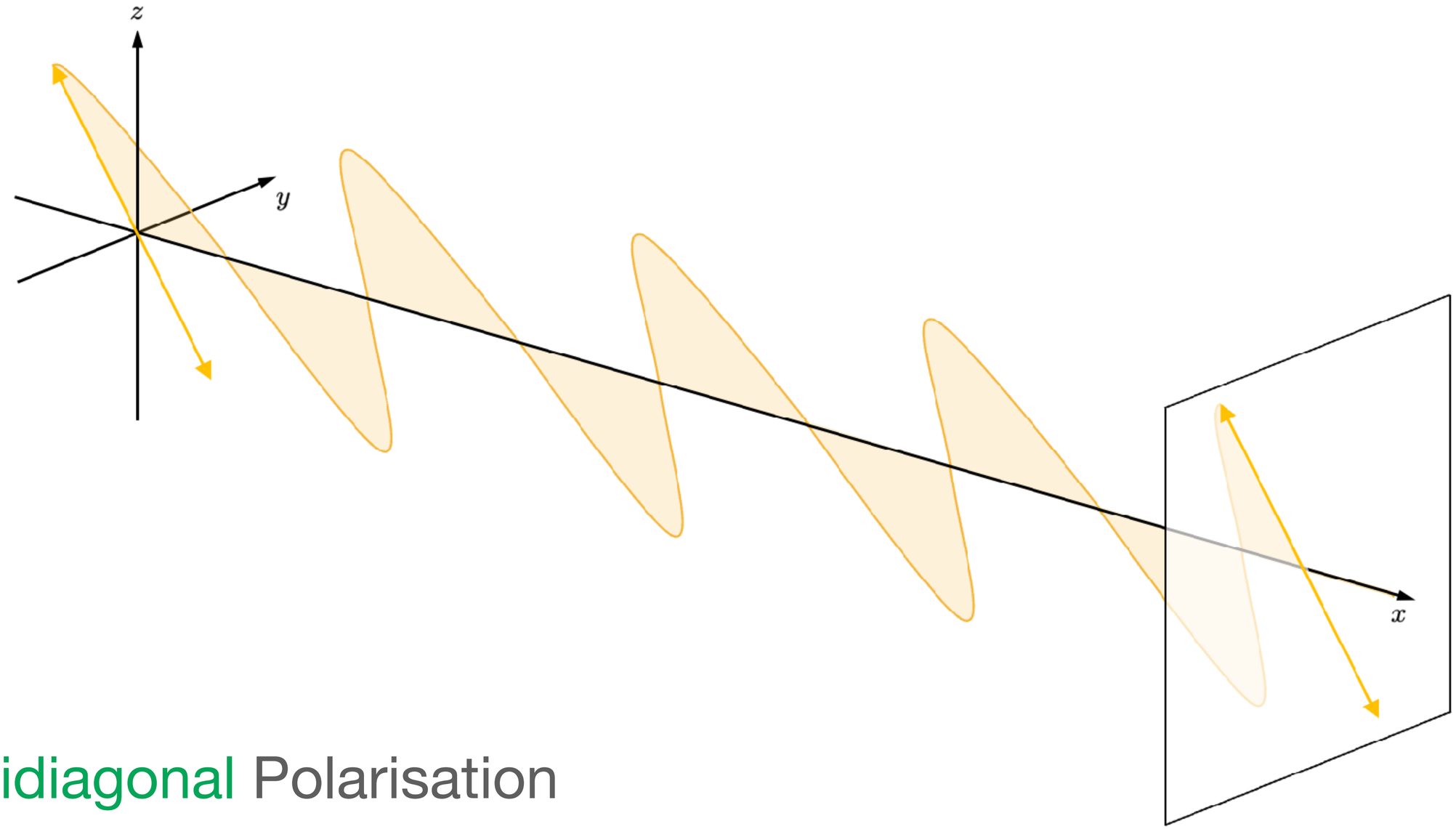
Horizontal Polarisation

Polarisation: a Quantum Property



Diagonal Polarisation

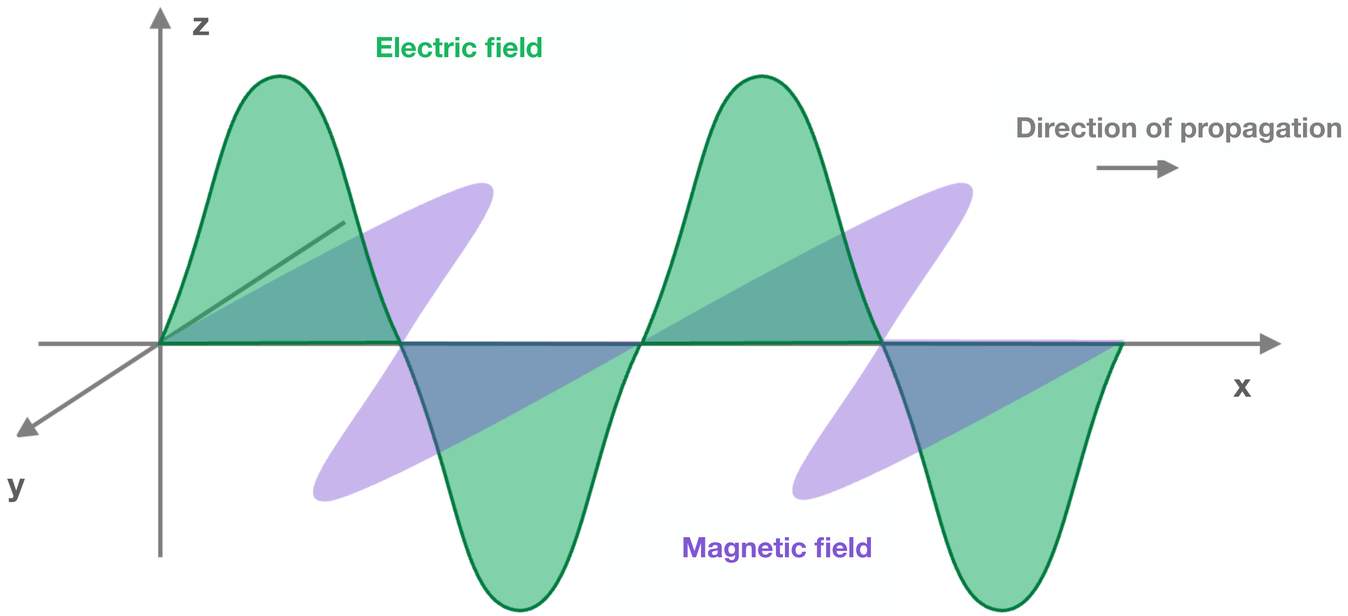
Polarisation: a Quantum Property



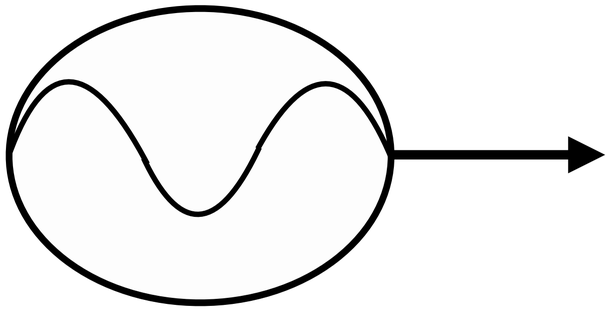
Antidiagonal Polarisation

Wave-Particle Duality of Light

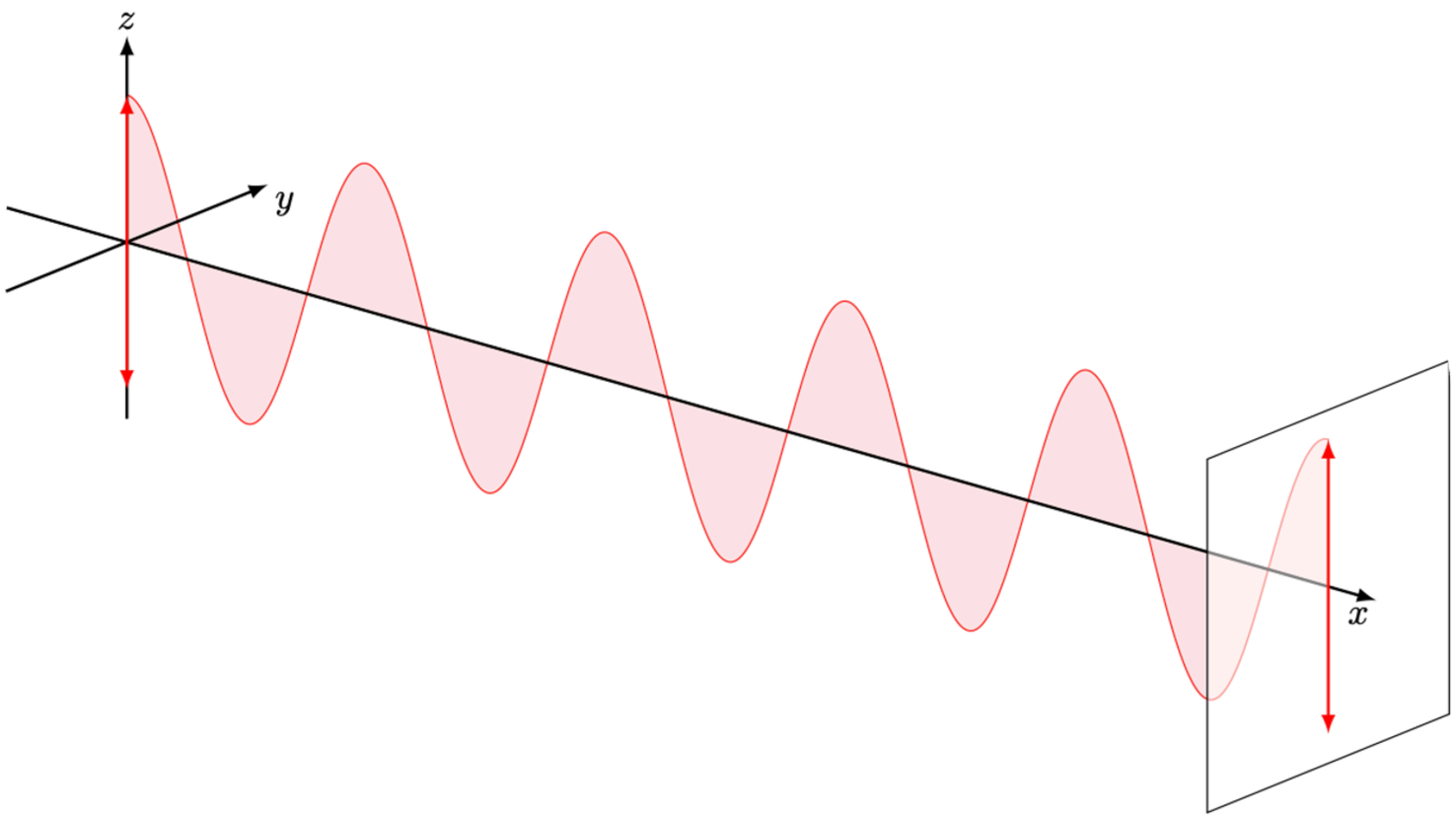
Electromagnetic wave

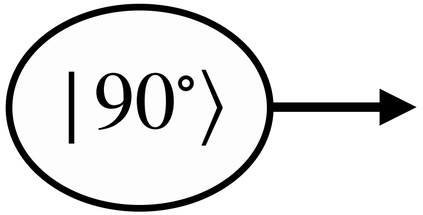


Photon

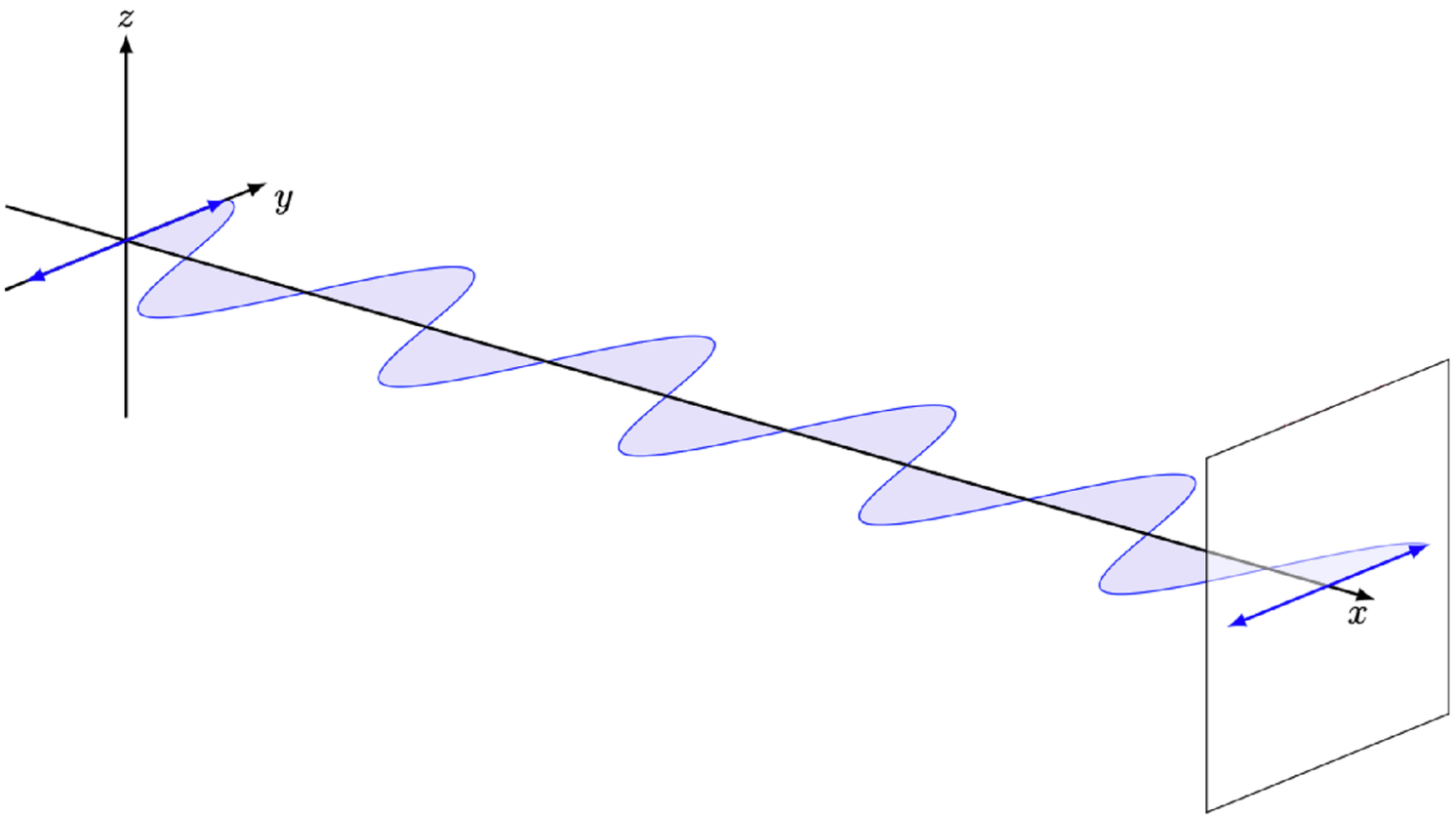


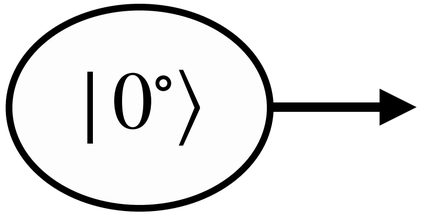
Vertical Polarisation



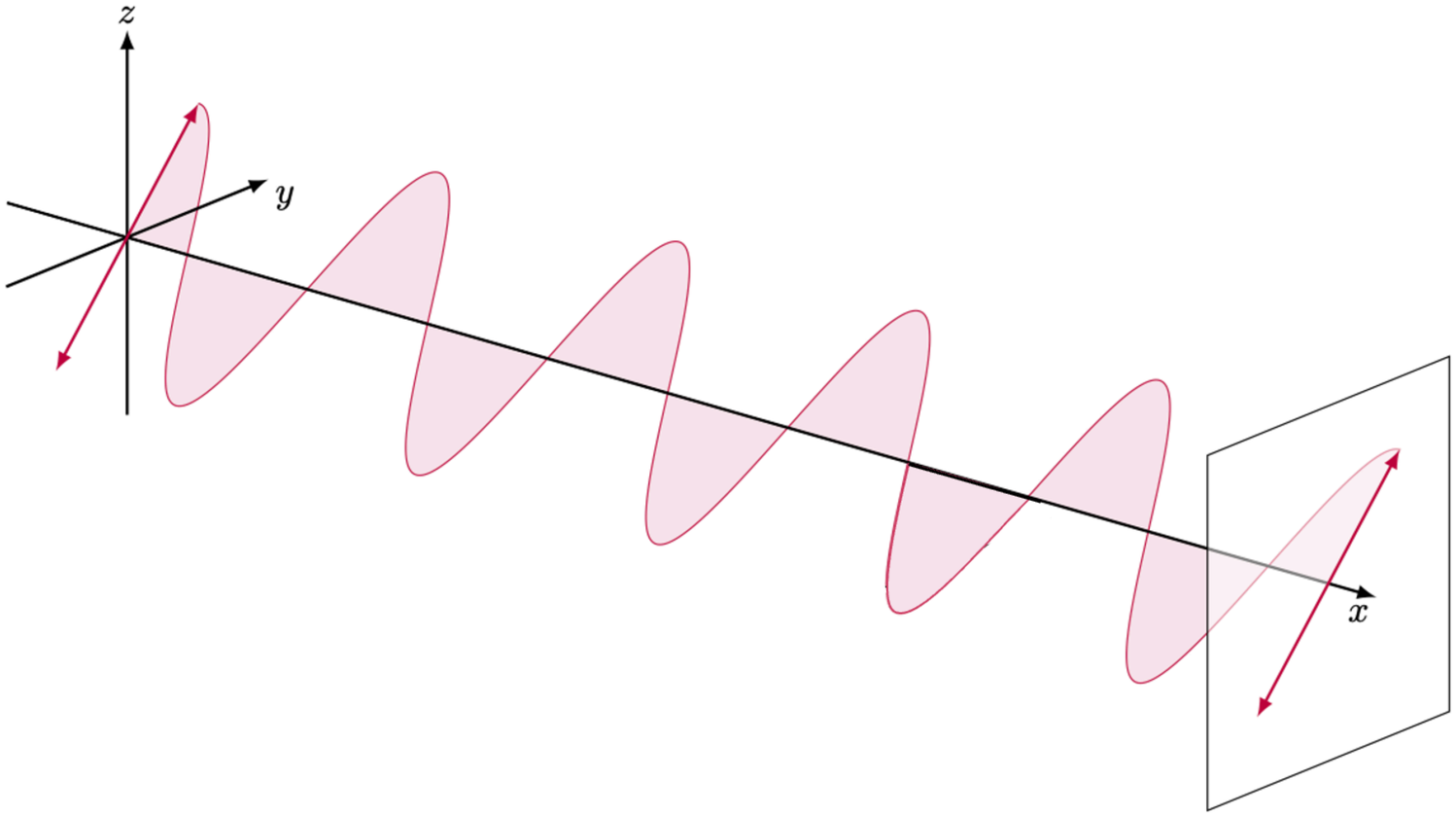


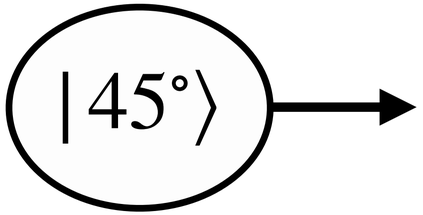
Horizontal Polarisation



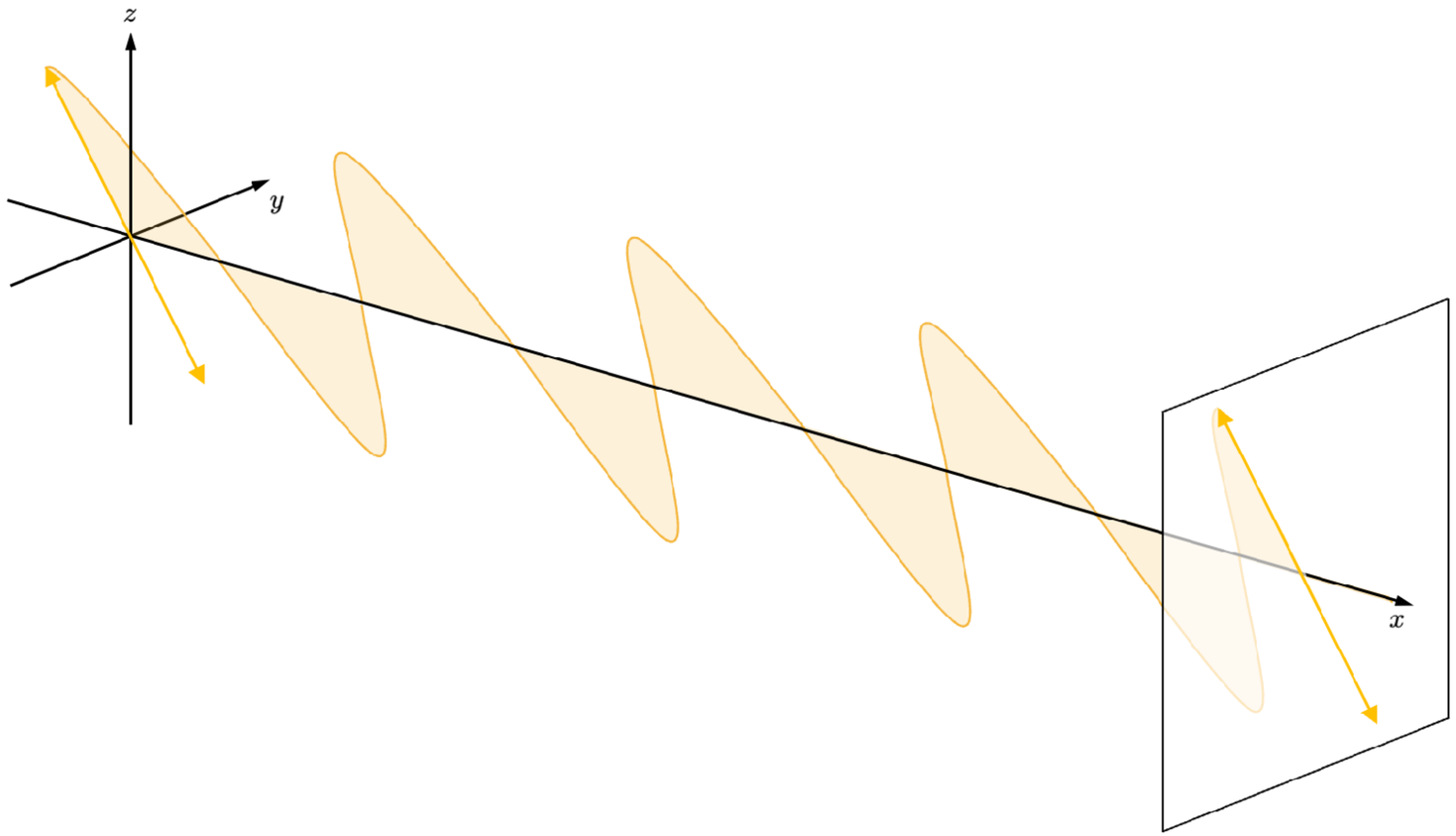


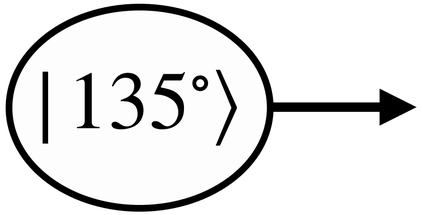
Diagonal Polarisation





Antidiagonal Polarisation

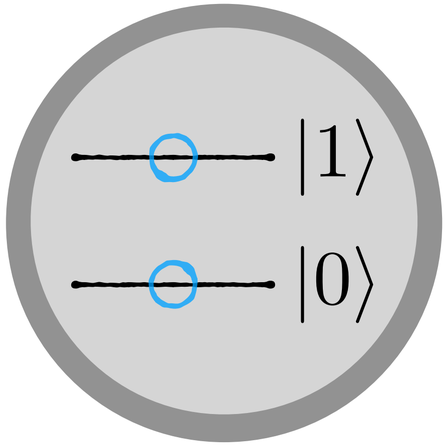




Basis States

Basis states

$|0\rangle$ et $|1\rangle$



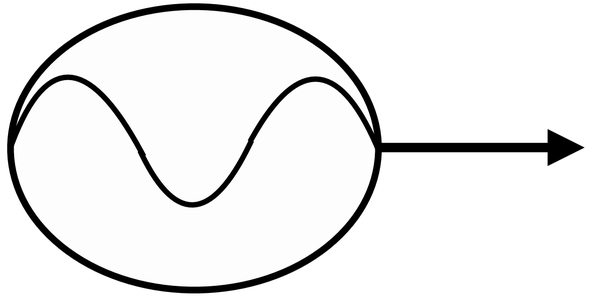
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

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

Basis States

Basis states

$|0\rangle$ et $|1\rangle$



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

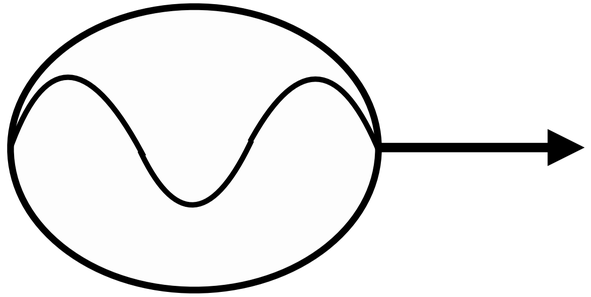
$$|\alpha|^2 + |\beta|^2 = 1$$

Basis States

Basis states

$|0\rangle$ et $|1\rangle$

$|90°\rangle$ et $|0°\rangle$



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

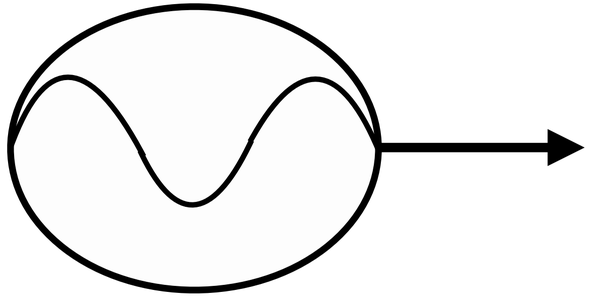
$$|\alpha|^2 + |\beta|^2 = 1$$

Basis States

Basis states

$|0\rangle$ et $|1\rangle$

$|90^\circ\rangle$ et $|0^\circ\rangle$



$$|\psi\rangle = \alpha|90^\circ\rangle + \beta|0^\circ\rangle$$

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

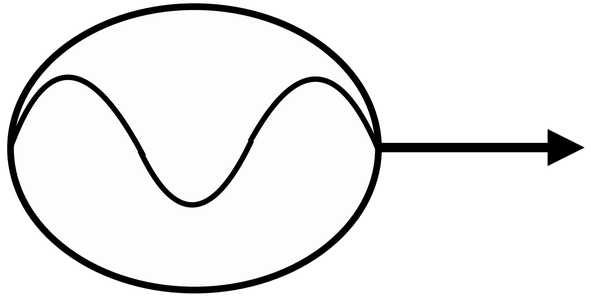
Basis States

Basis states

$|0\rangle$ et $|1\rangle$

$|90^\circ\rangle$ et $|0^\circ\rangle$

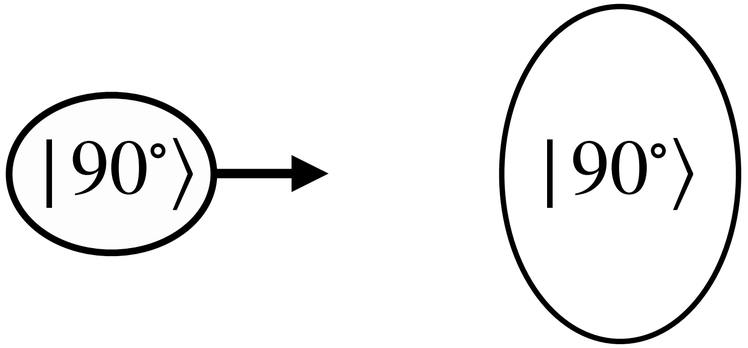
$|45^\circ\rangle$ et $|135^\circ\rangle$

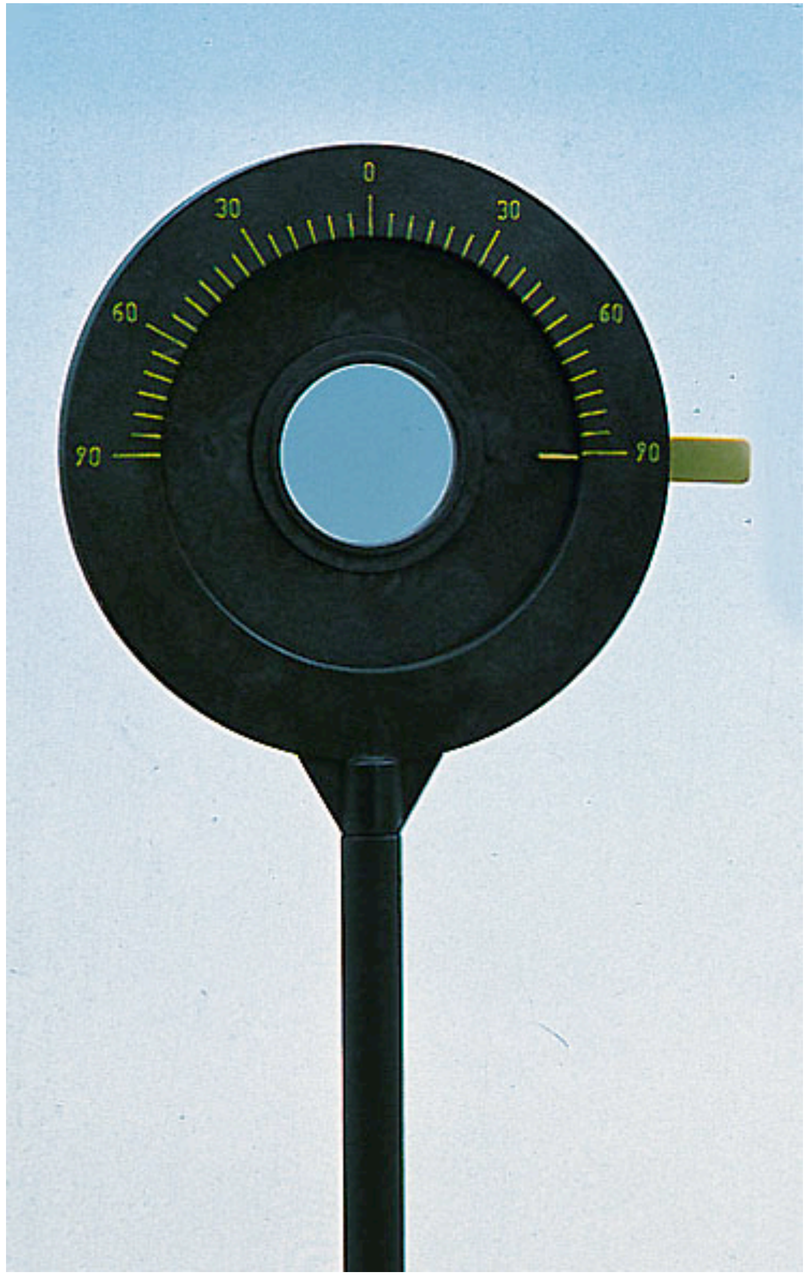


$$|\psi\rangle = \alpha|45^\circ\rangle + \beta|135^\circ\rangle$$

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

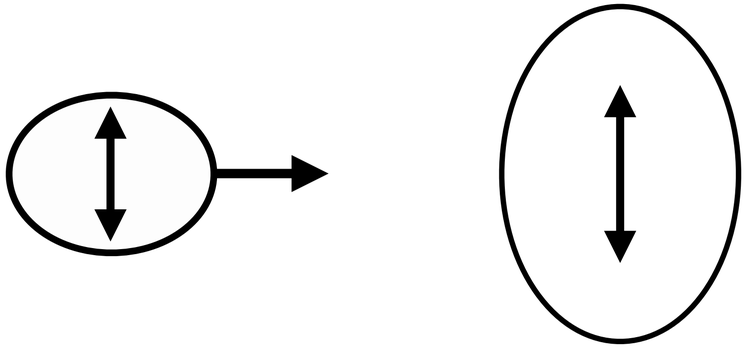
The Polarizer

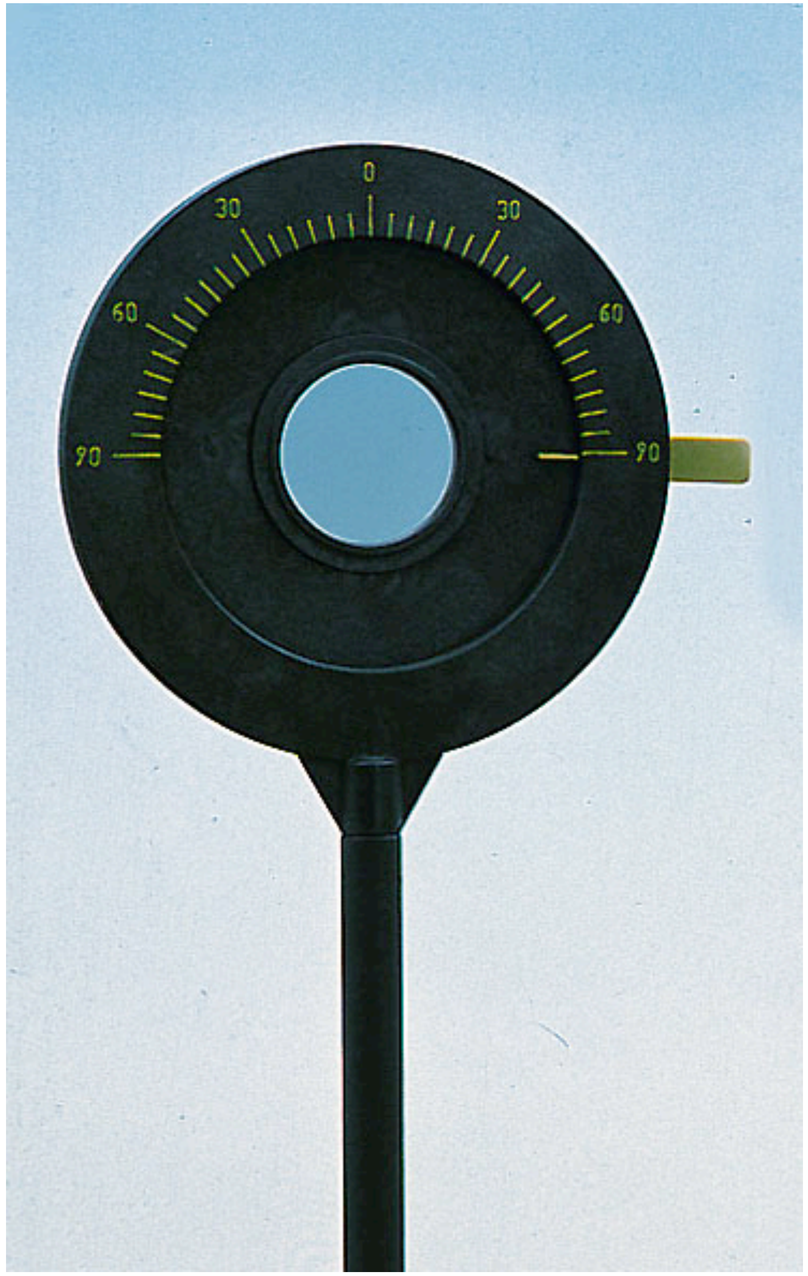




https://www.leybold-shop.fr/

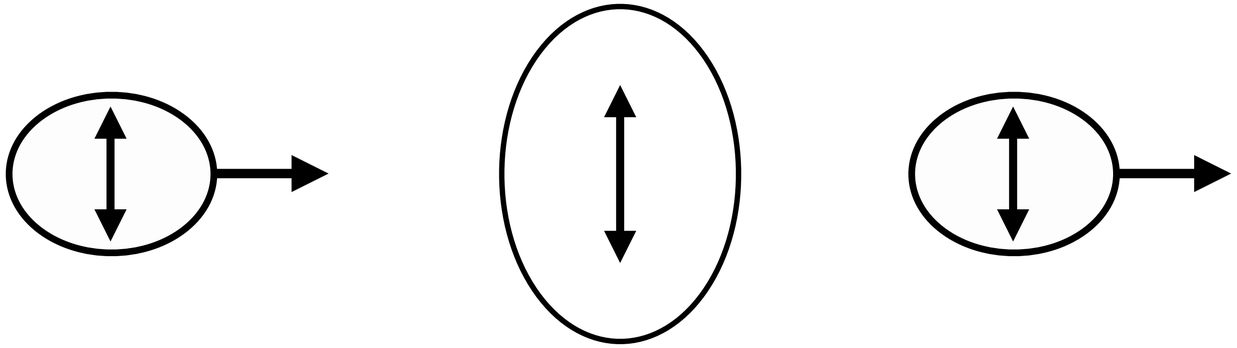
The Polarizer

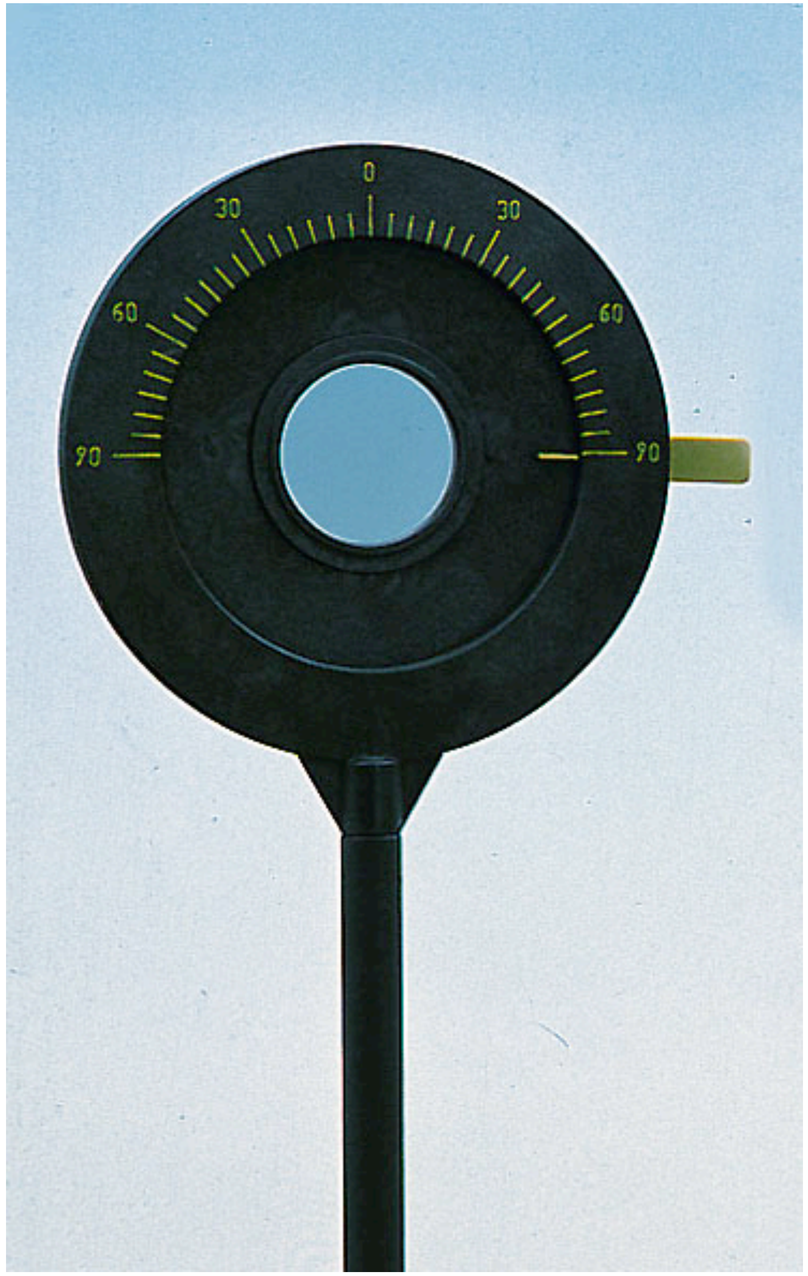




https://www.leybold-shop.fr/

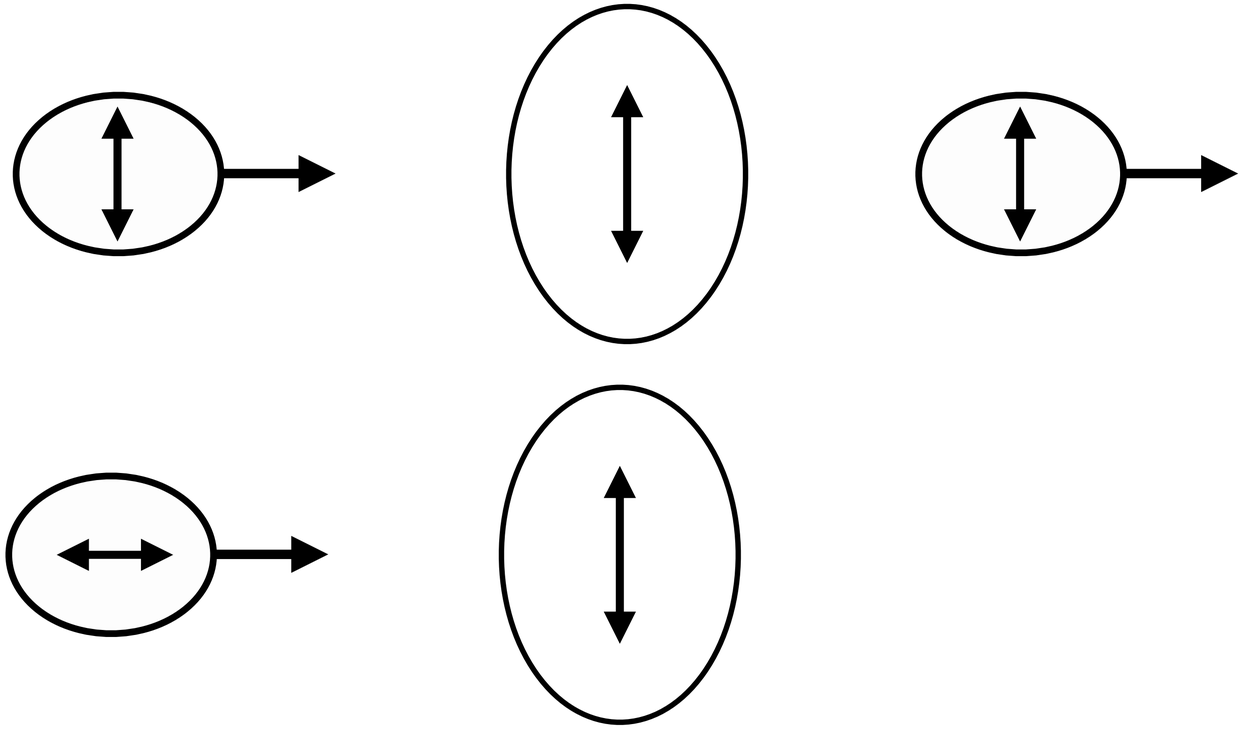
The Polarizer

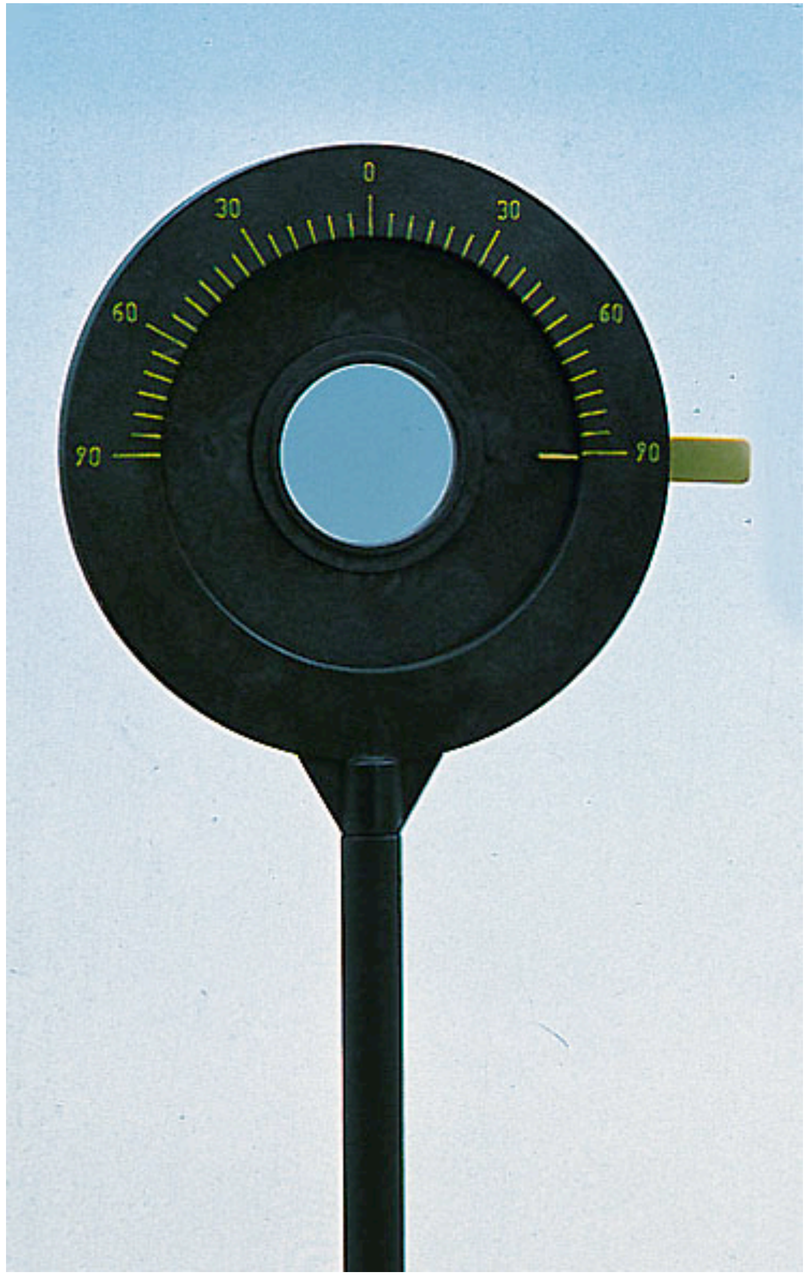




https://www.leybold-shop.fr/

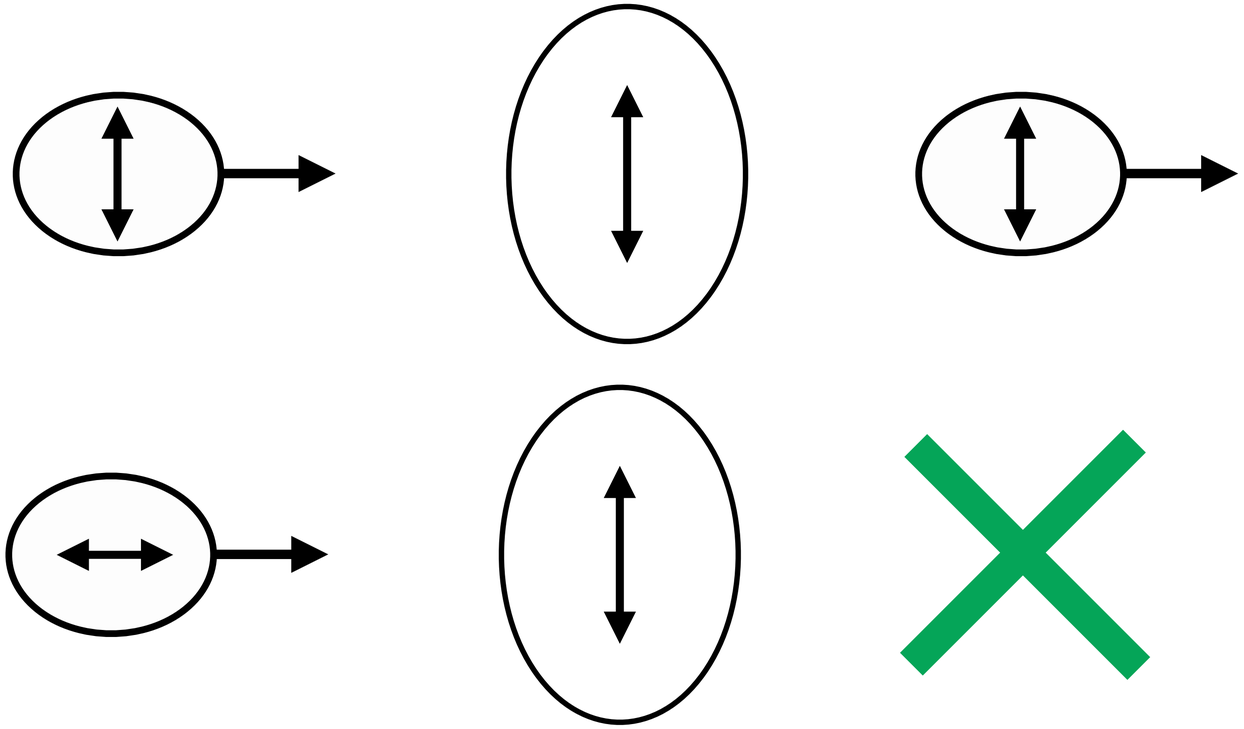
The Polarizer

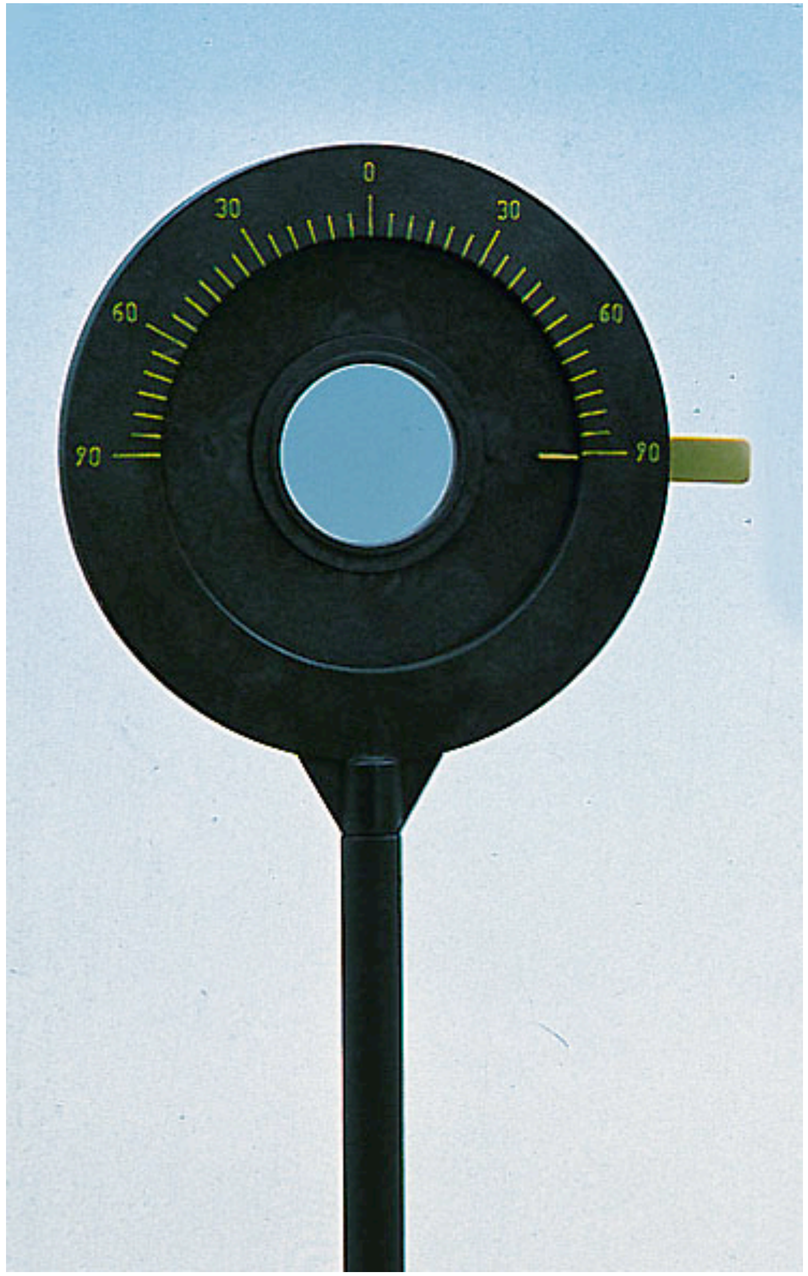




https://www.leybold-shop.fr/

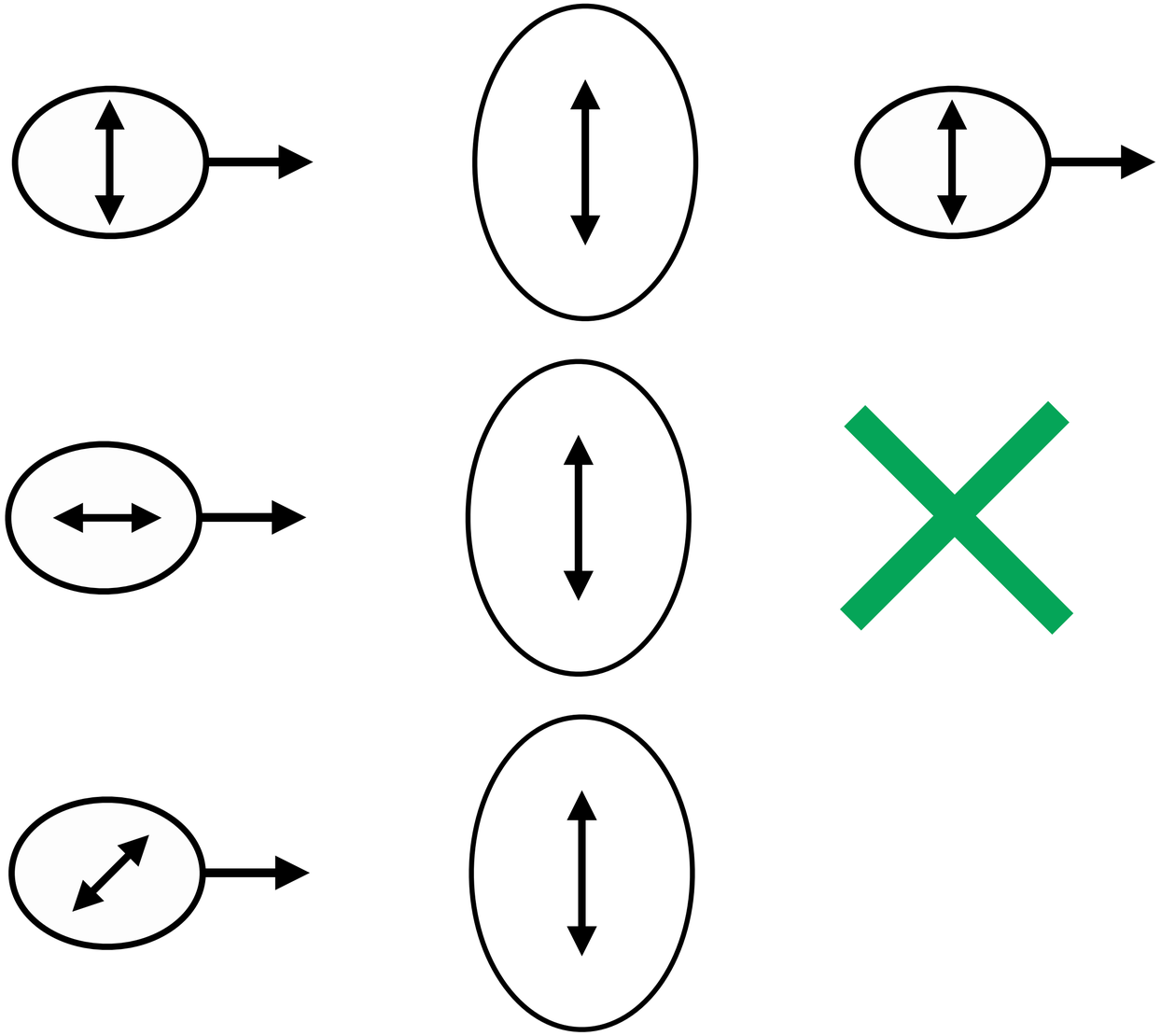
The Polarizer

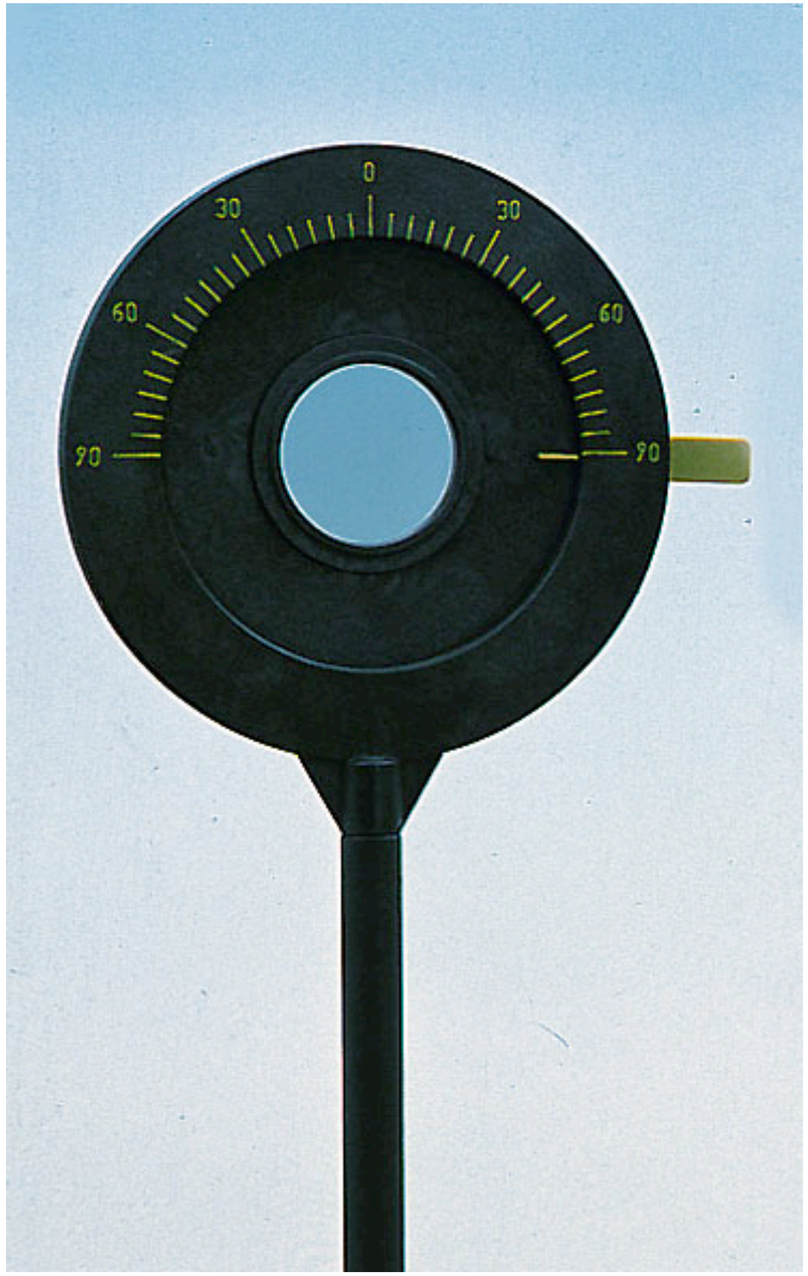




https://www.leybold-shop.fr/

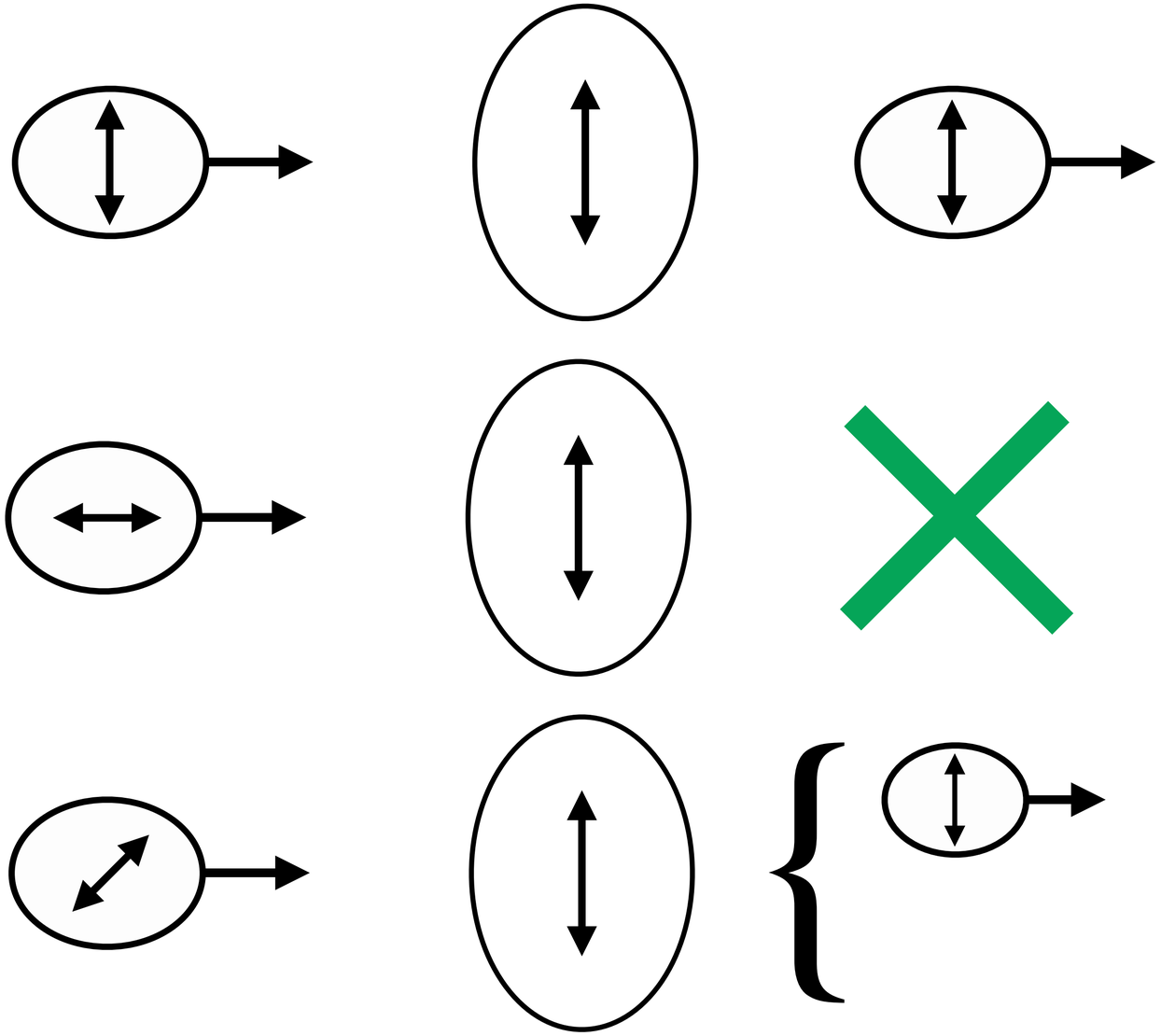
The Polarizer

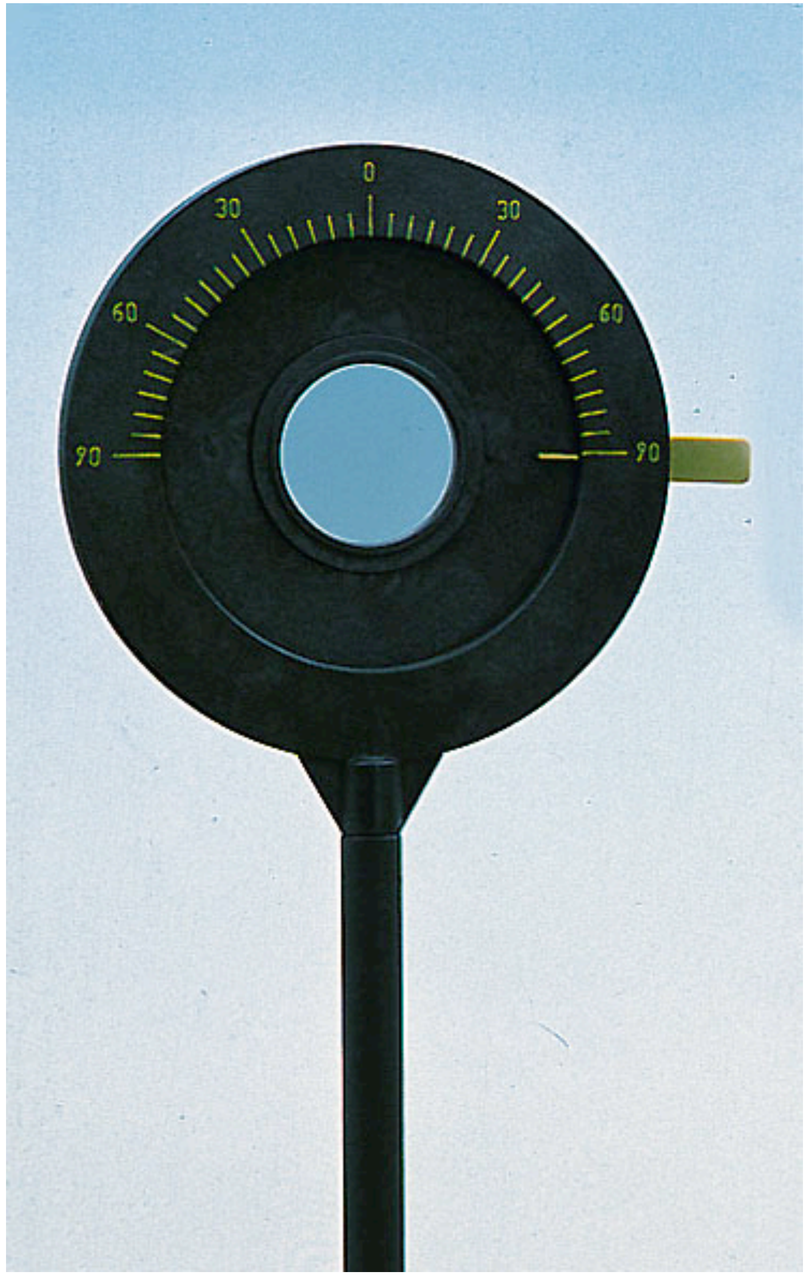




https://www.leybold-shop.fr/

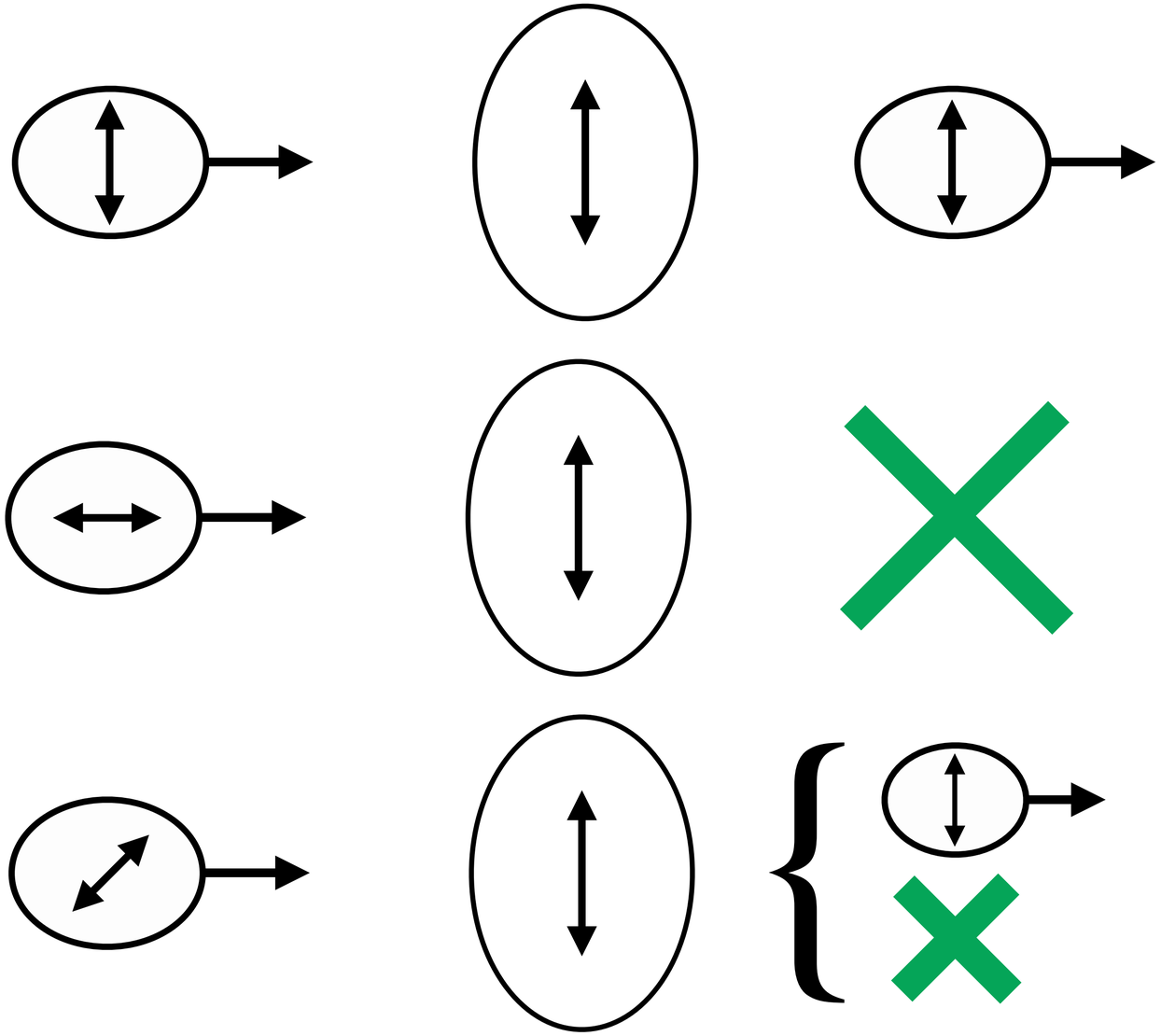
The Polarizer

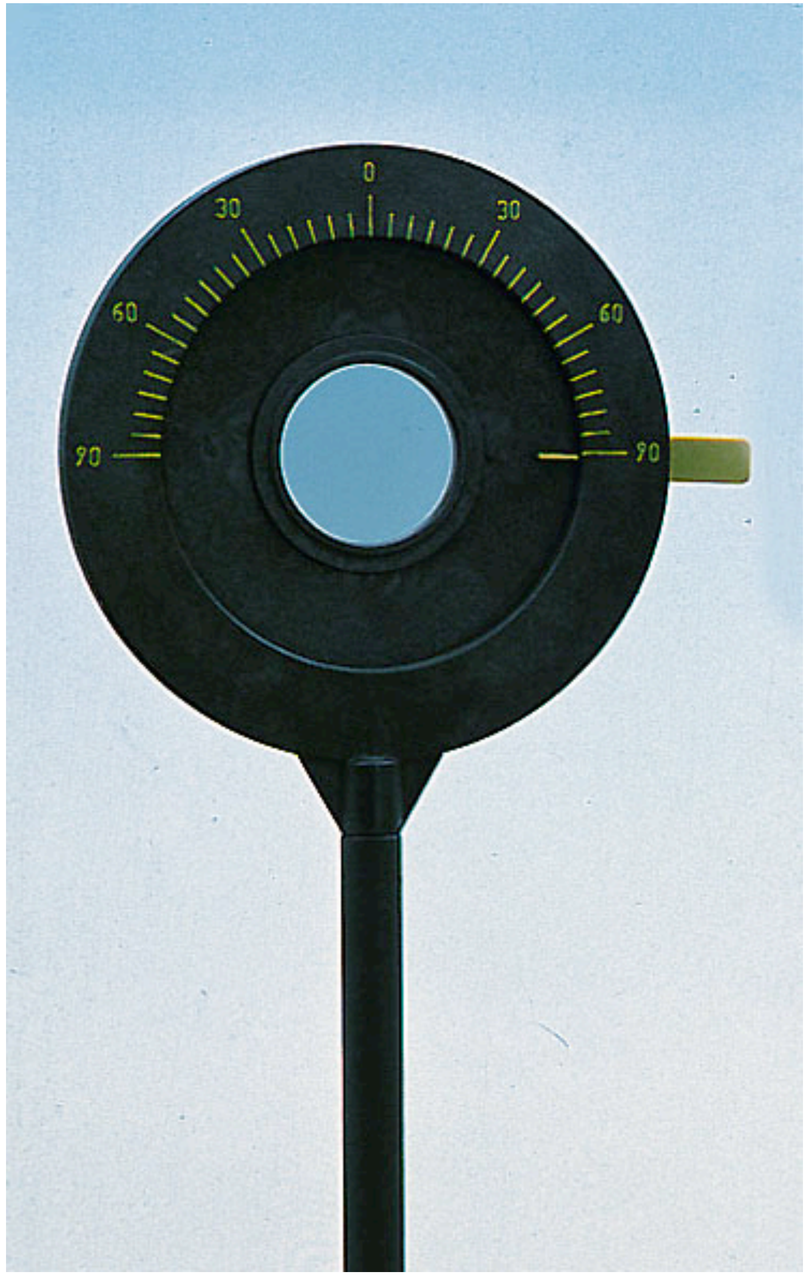




https://www.leybold-shop.fr/

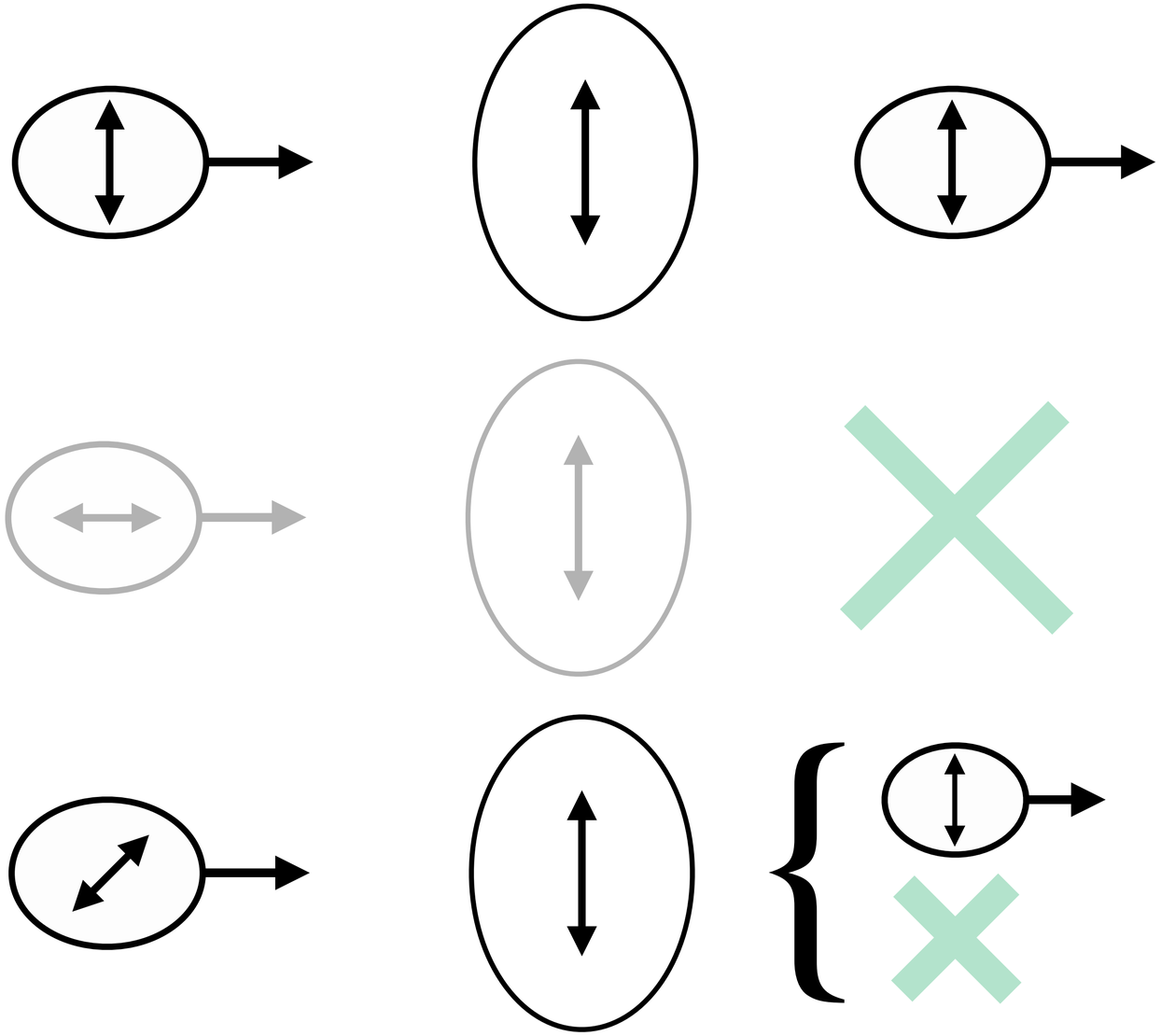
The Polarizer

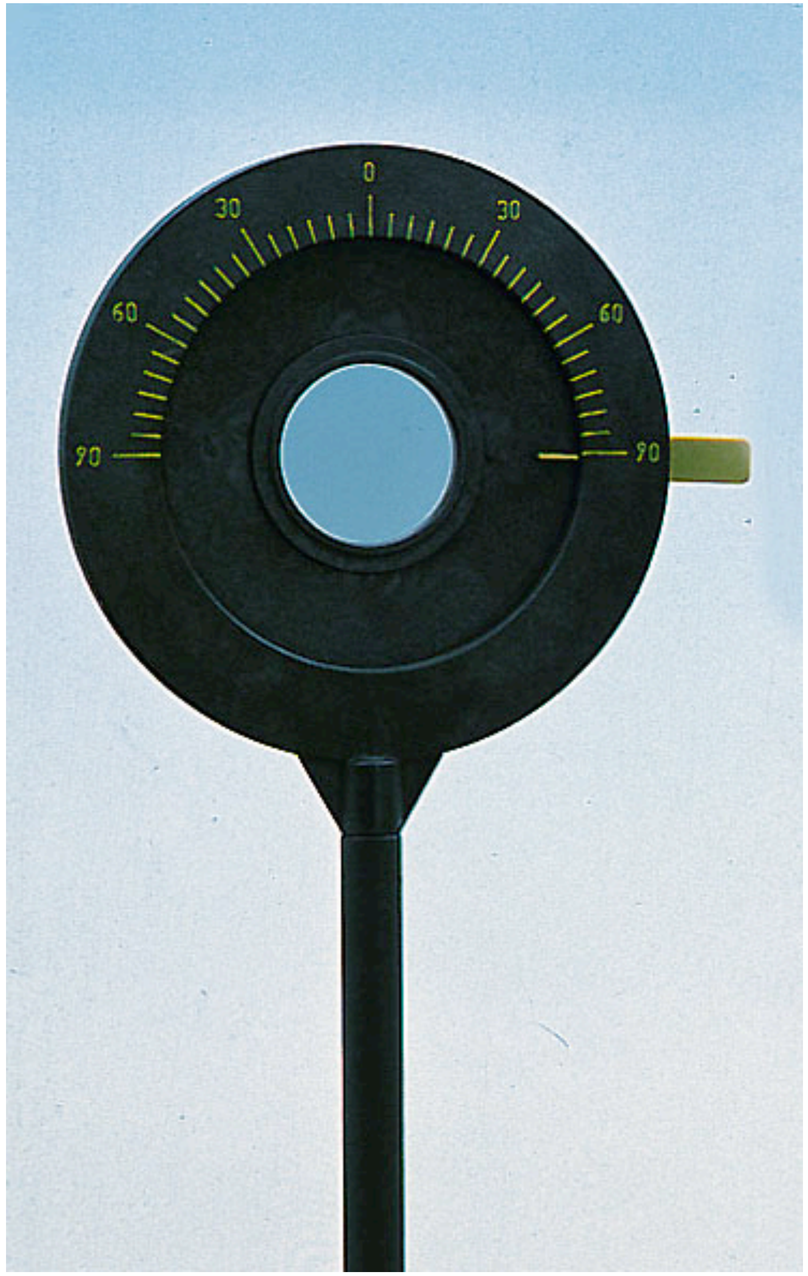




https://www.leybold-shop.fr/

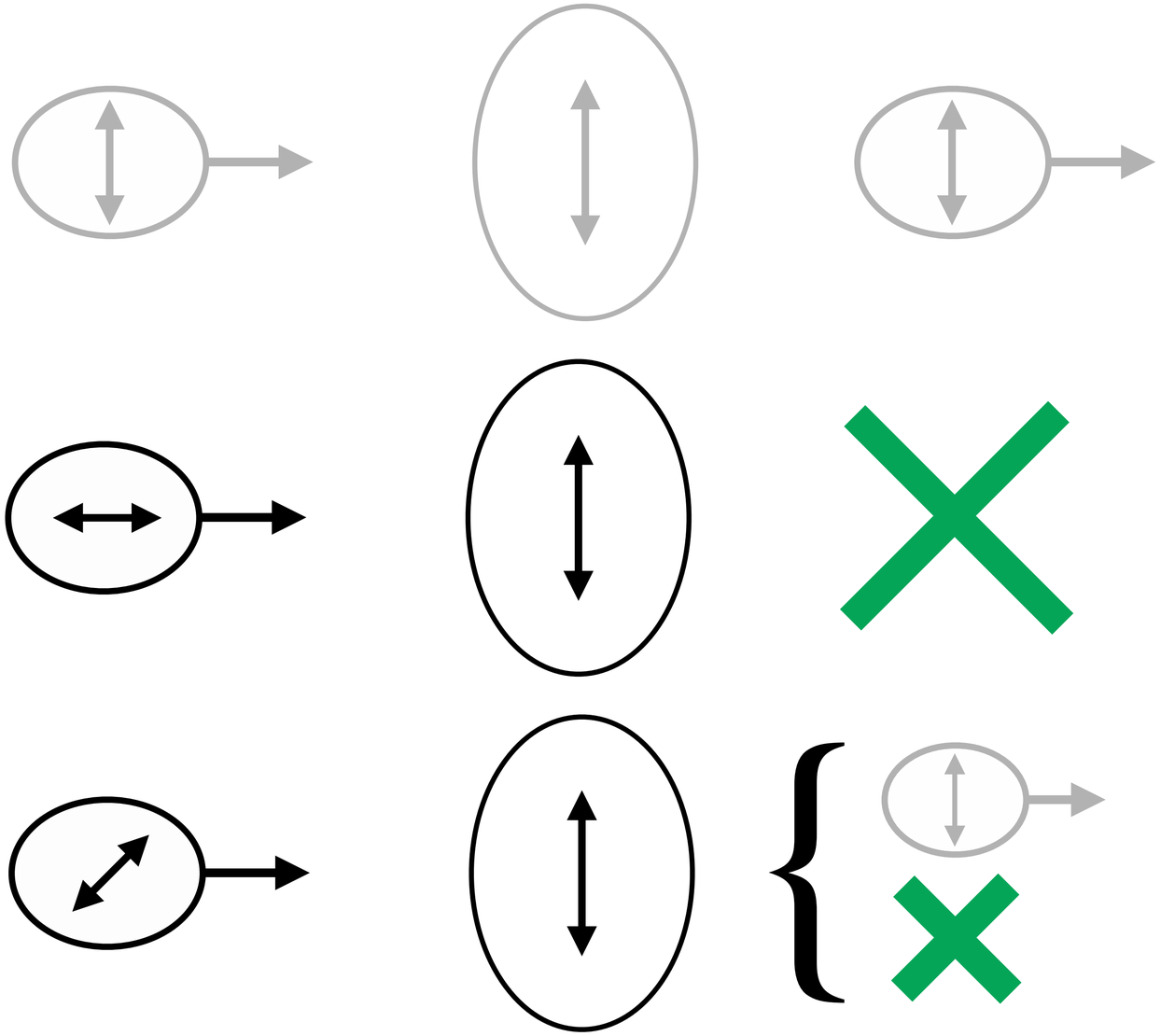
The Polarizer

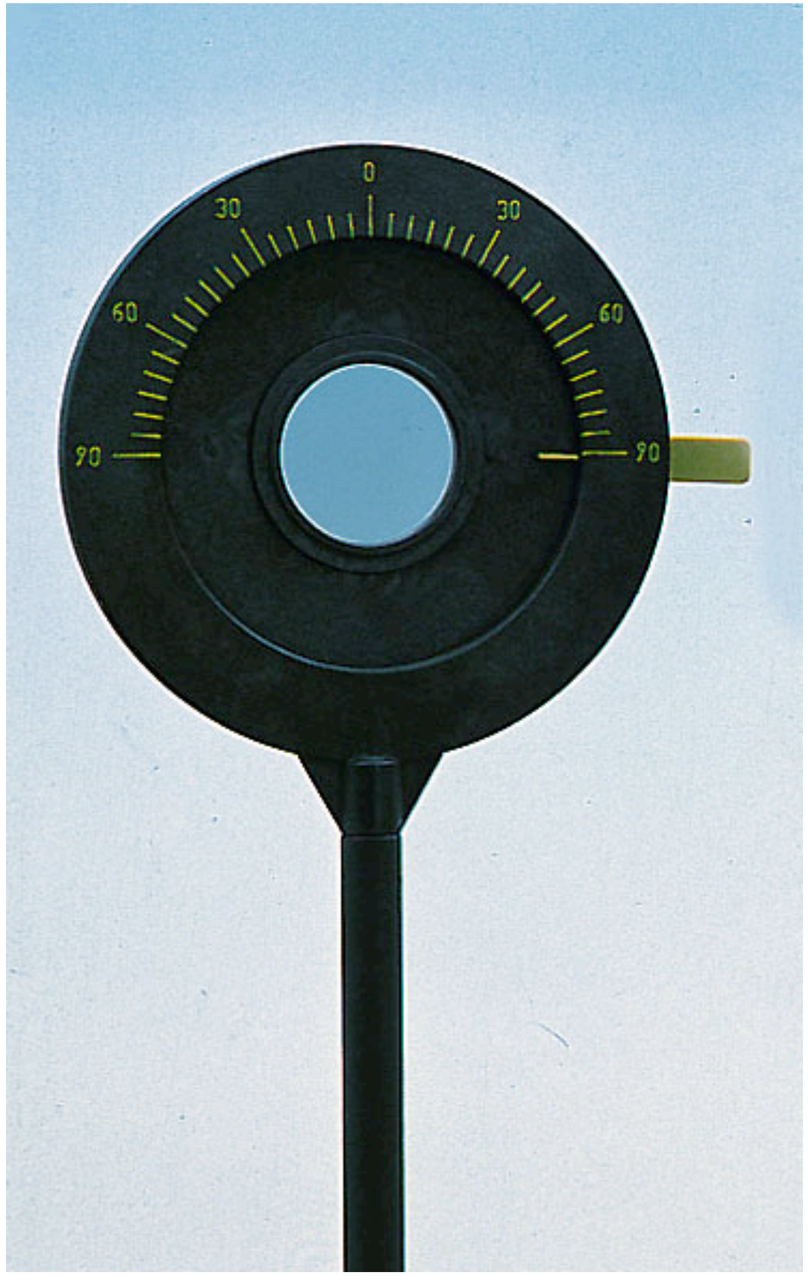




https://www.leybold-shop.fr/

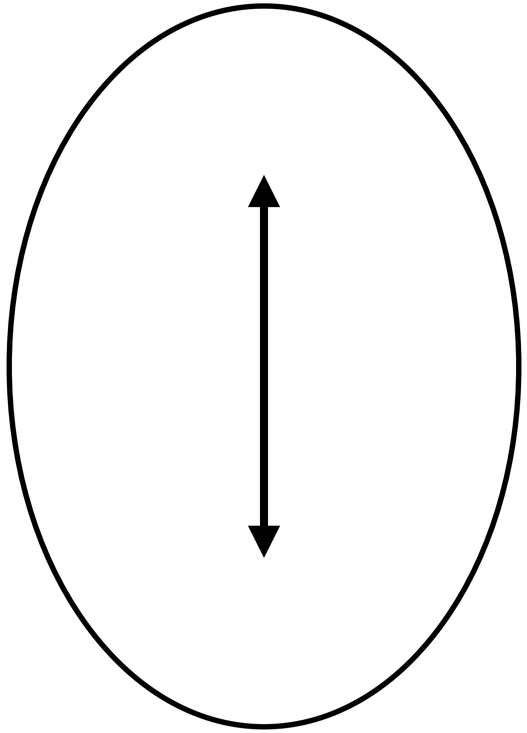
The Polarizer



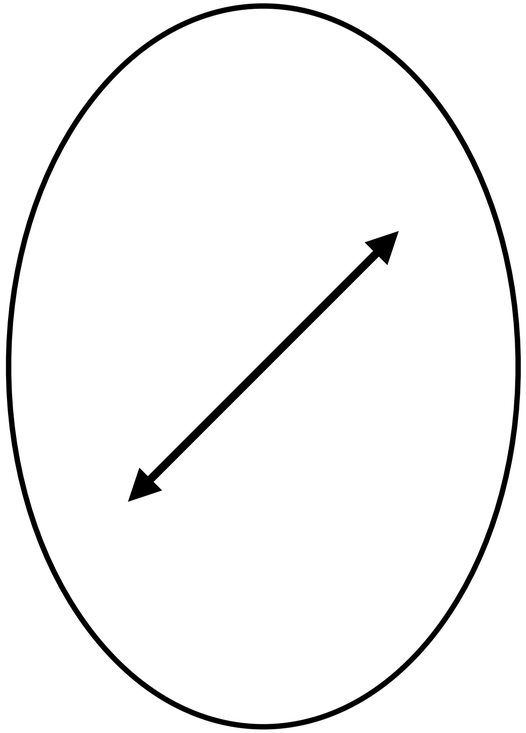


https://www.leybold-shop.fr/

Measurement Basis

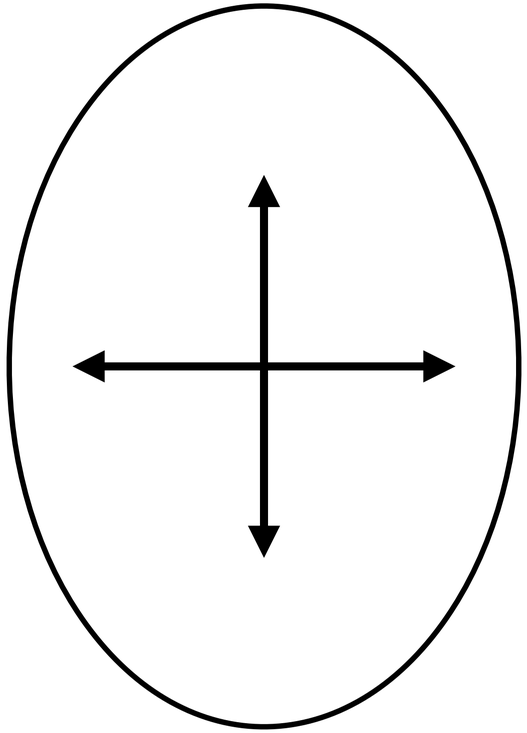


Vertical Basis

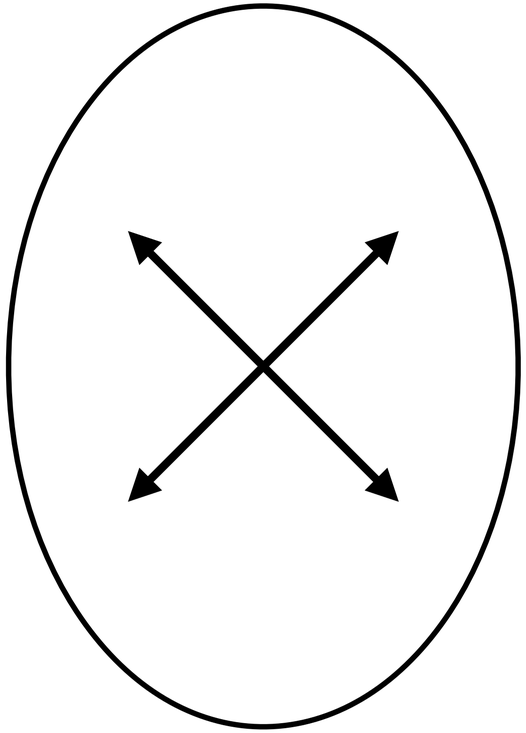


Diagonal Basis

Measurement Basis

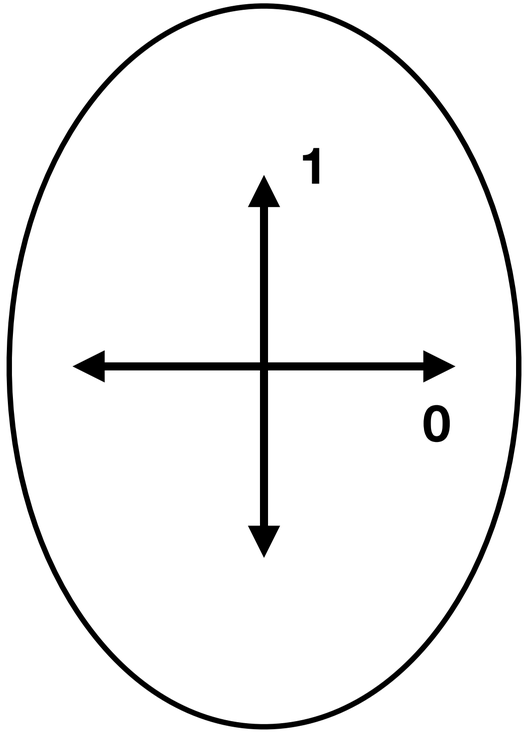


Vertical Basis

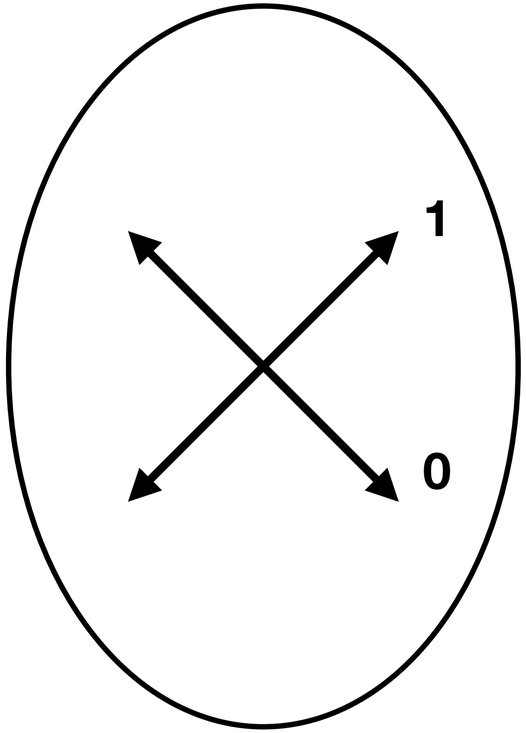


Diagonal Basis

Measurement Basis

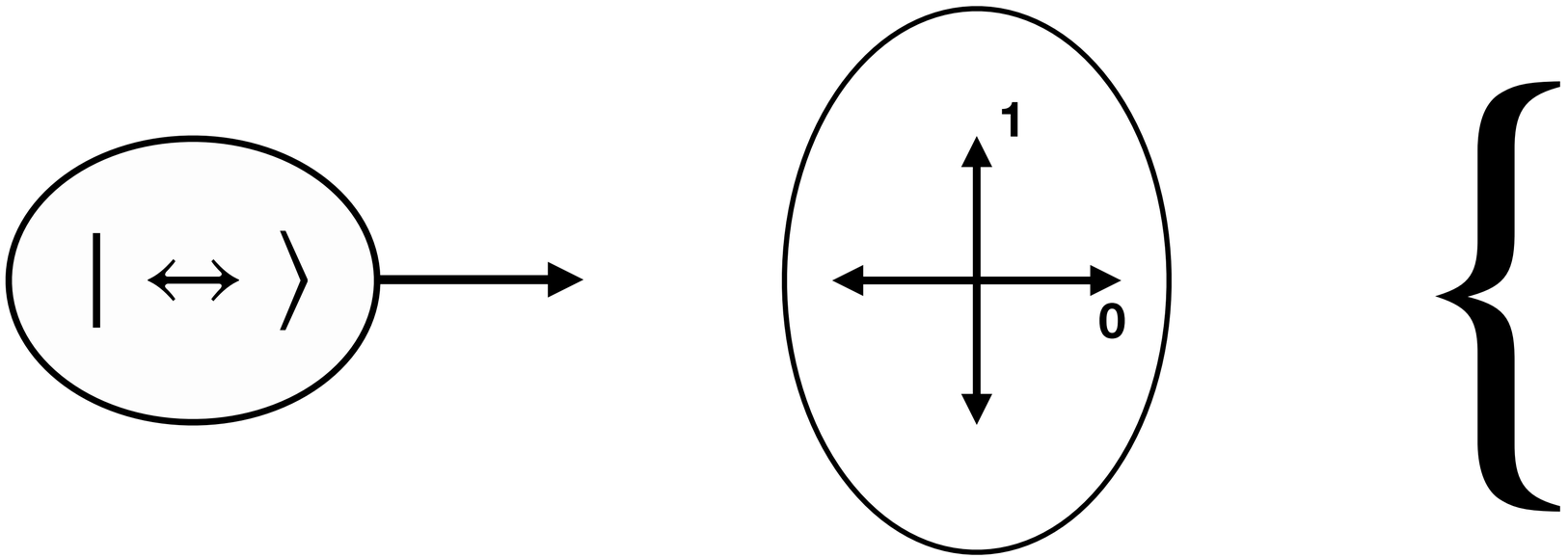


Vertical Basis



Diagonal Basis

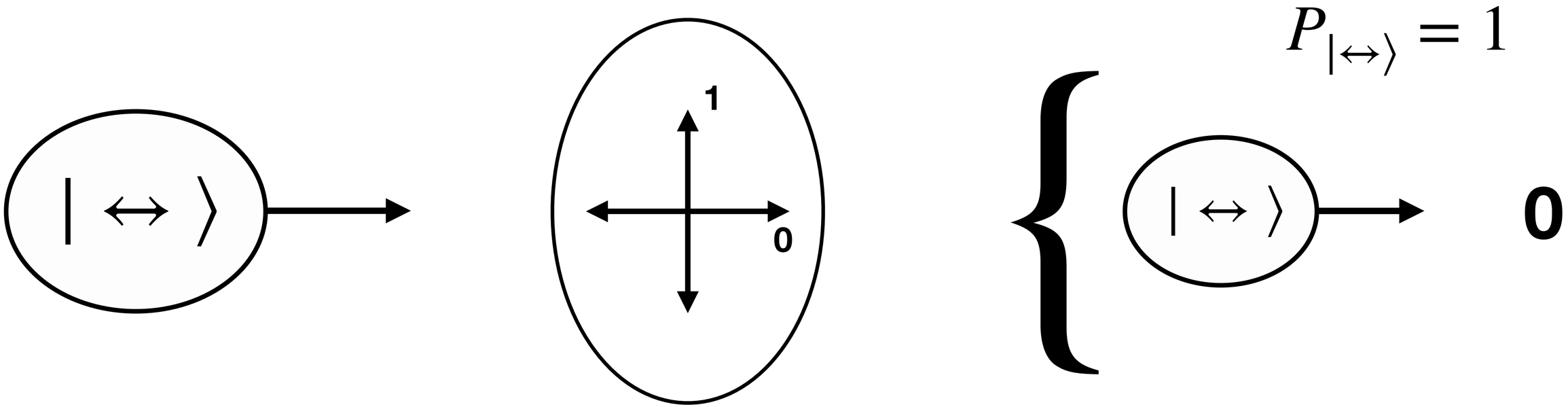
Measurement



$$\{$$

$$|90^\circ\rangle \equiv |\updownarrow\rangle$$
$$|0^\circ\rangle \equiv |\leftrightarrow\rangle$$

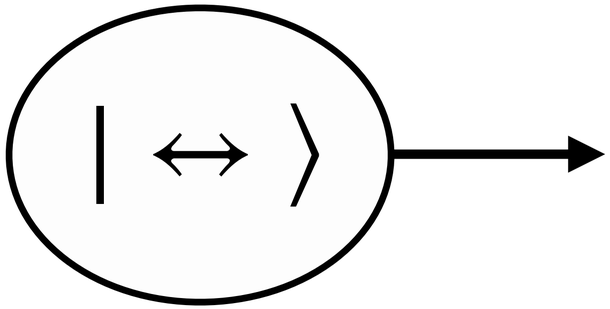
Measurement



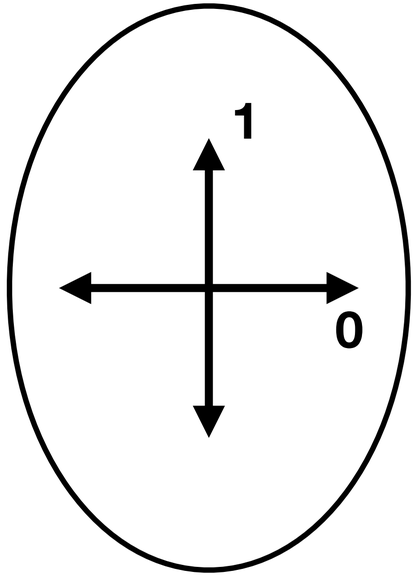
$|90°\rangle \equiv |\updownarrow\rangle$

$|0°\rangle \equiv |\leftrightarrow\rangle$

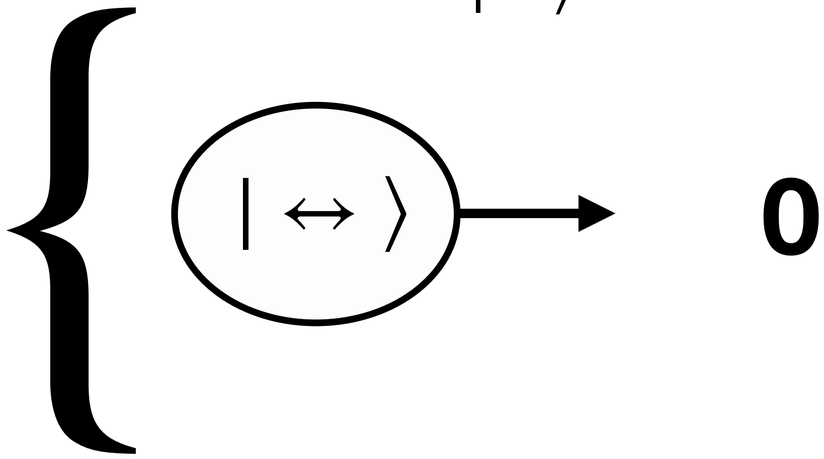
Measurement



$1|\leftrightarrow\rangle + 0|\updownarrow\rangle$



$P_{|\leftrightarrow\rangle} = 1$



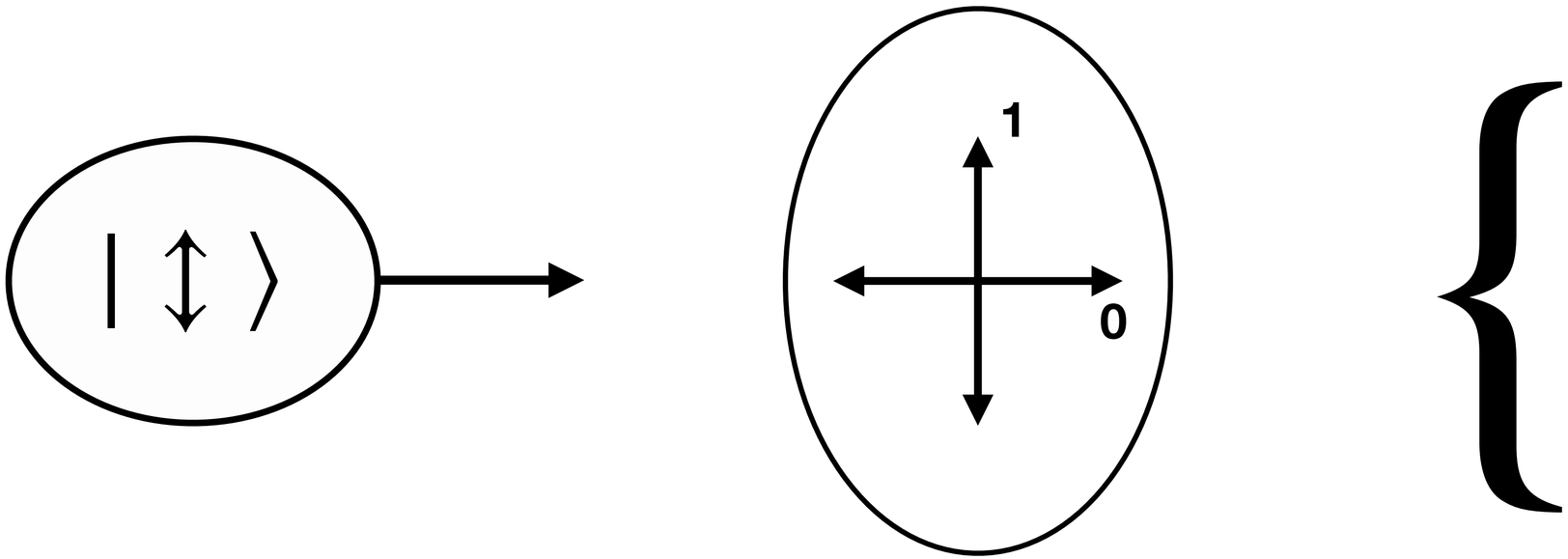
$|90°\rangle \equiv |\updownarrow\rangle$

$|0°\rangle \equiv |\leftrightarrow\rangle$

$P_{|\leftrightarrow\rangle} = |1|^2$

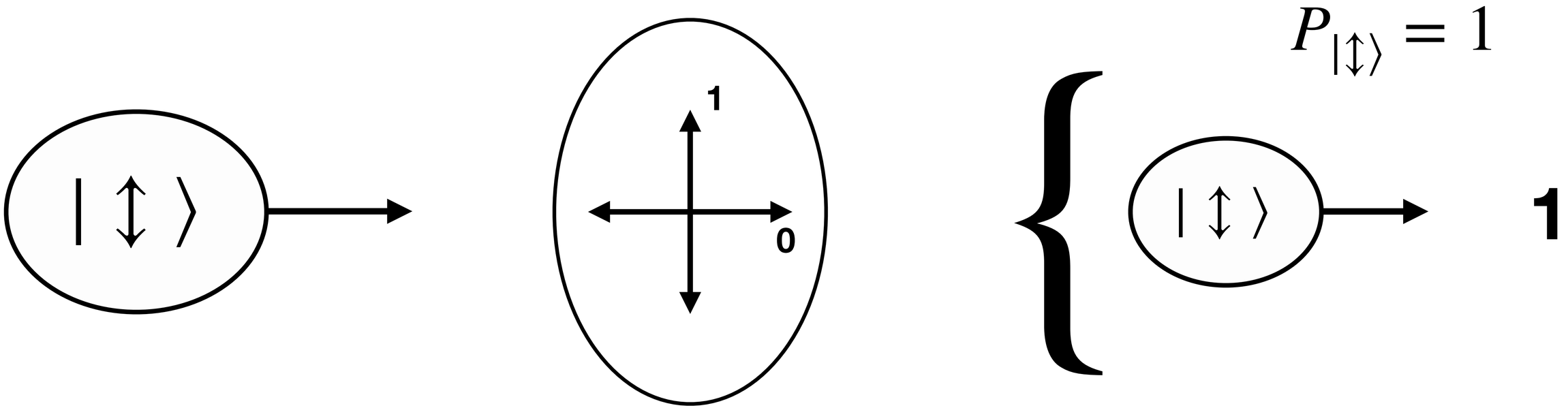
$P_{|\updownarrow\rangle} = |0|^2$

Measurement



$$|90^\circ\rangle \equiv |\updownarrow\rangle$$
$$|0^\circ\rangle \equiv |\leftrightarrow\rangle$$

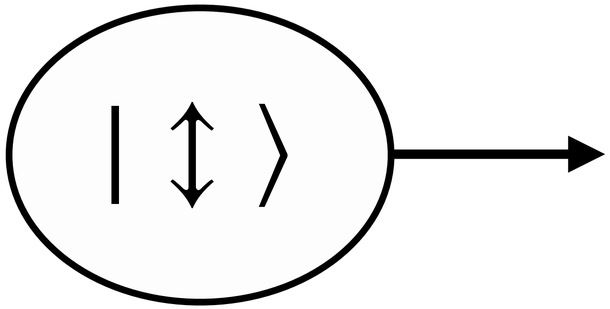
Measurement



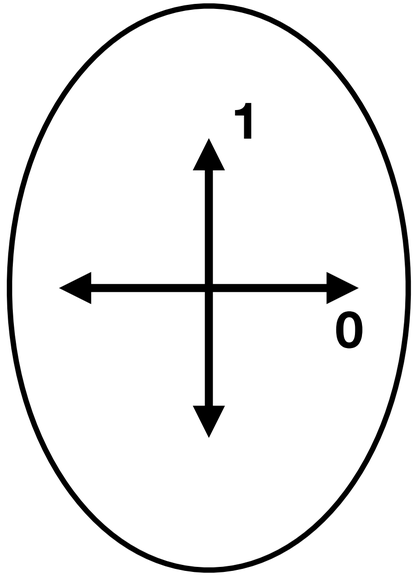
$|90°\rangle \equiv |\updownarrow\rangle$

$|0°\rangle \equiv |\leftrightarrow\rangle$

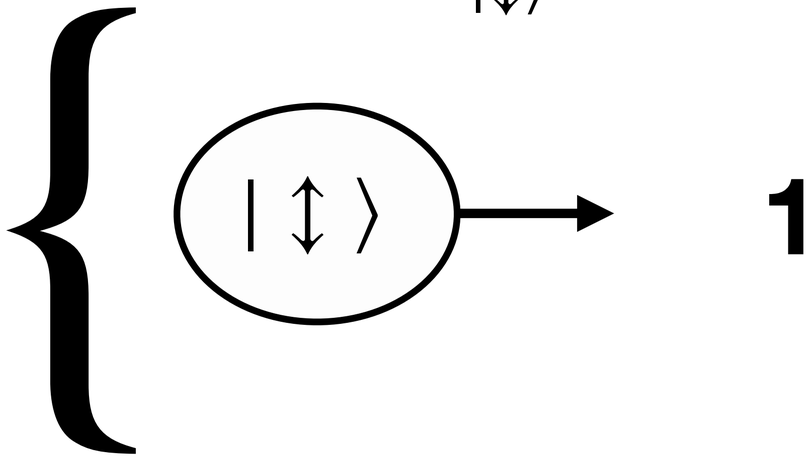
Measurement



$$0\,|\leftrightarrow\rangle + 1\,|\updownarrow\rangle$$



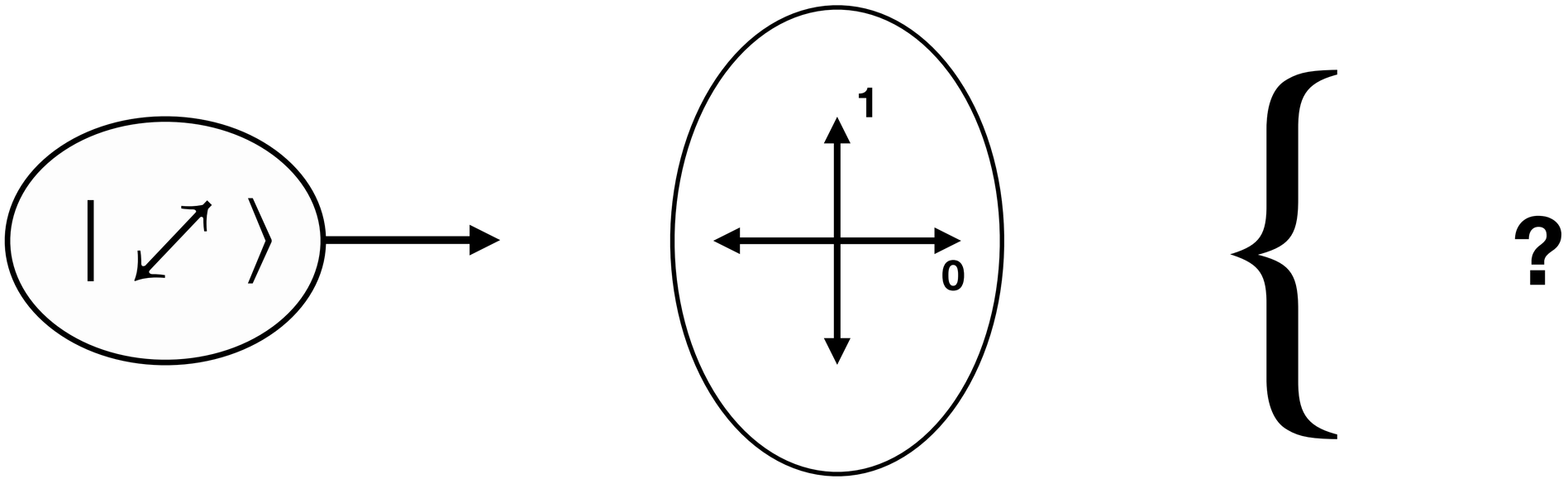
$$P_{|\updownarrow\rangle} = 1$$



$$|90^\circ\rangle \equiv |\updownarrow\rangle$$
$$|0^\circ\rangle \equiv |\leftrightarrow\rangle$$

$$P_{|\leftrightarrow\rangle} = |0|^2 \qquad P_{|\updownarrow\rangle} = |1|^2$$

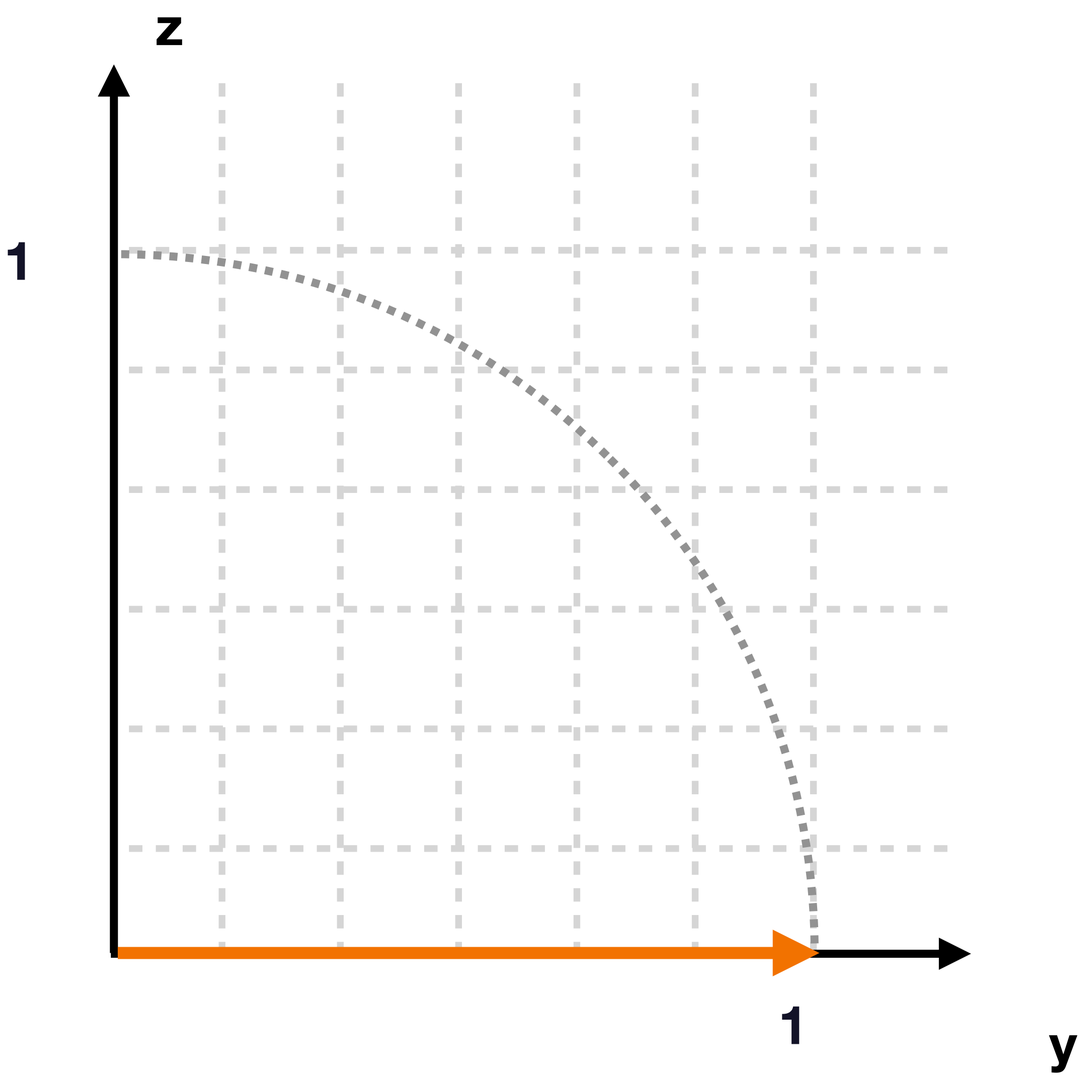
Measurement



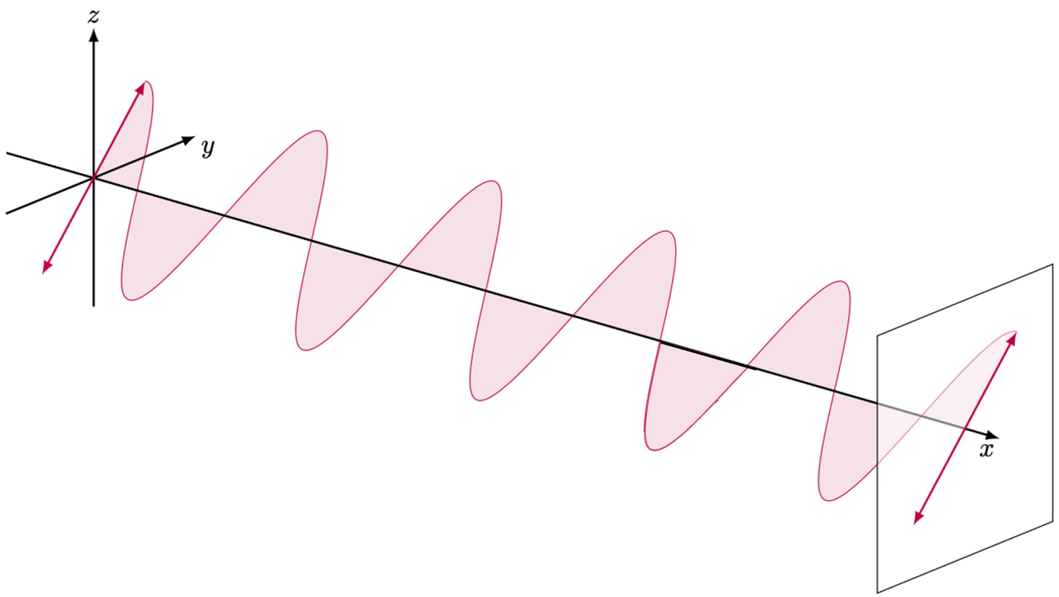
$|45°\rangle \equiv |\nearrow\swarrow\rangle$

$|135°\rangle \equiv |\nwarrow\searrow\rangle$

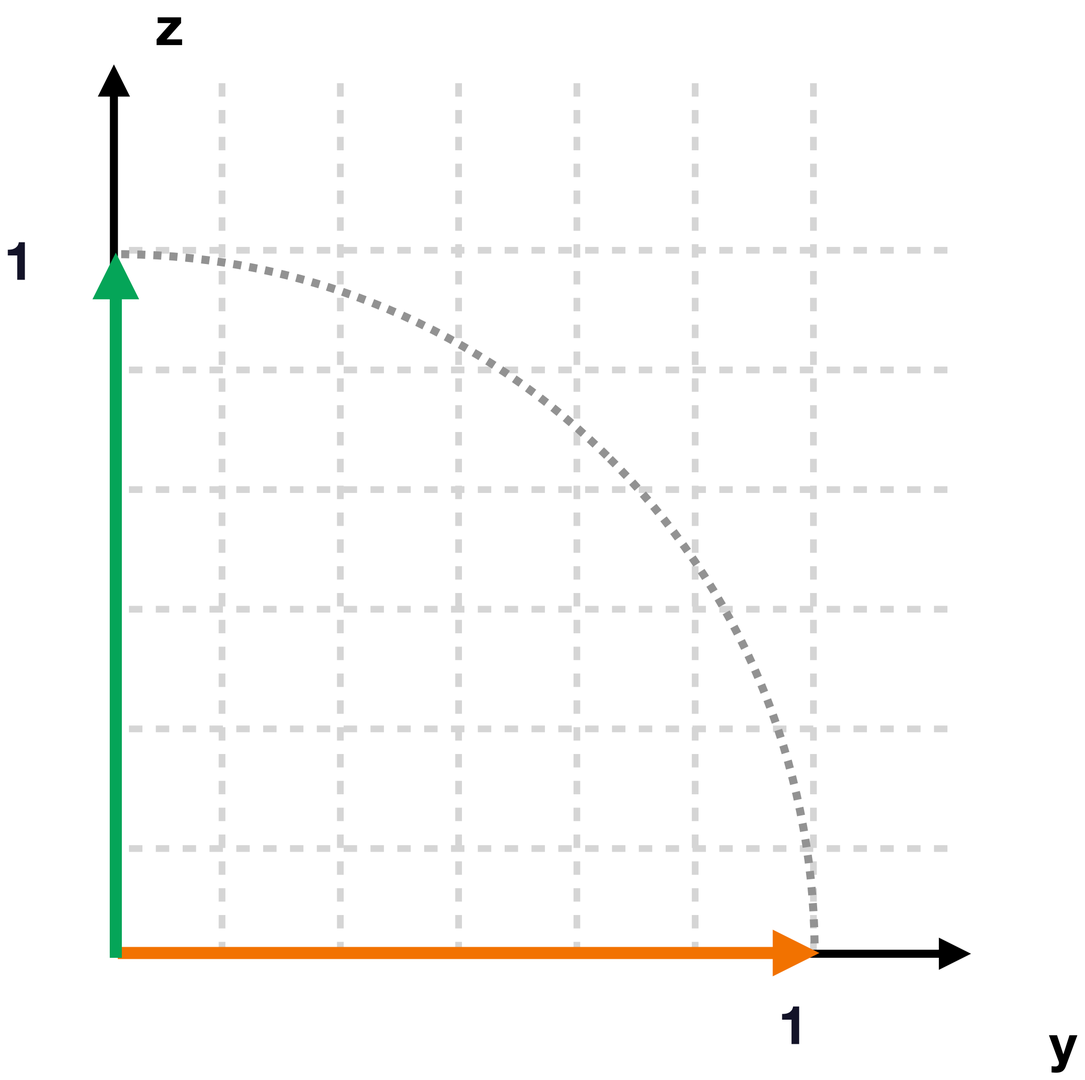
Measurement



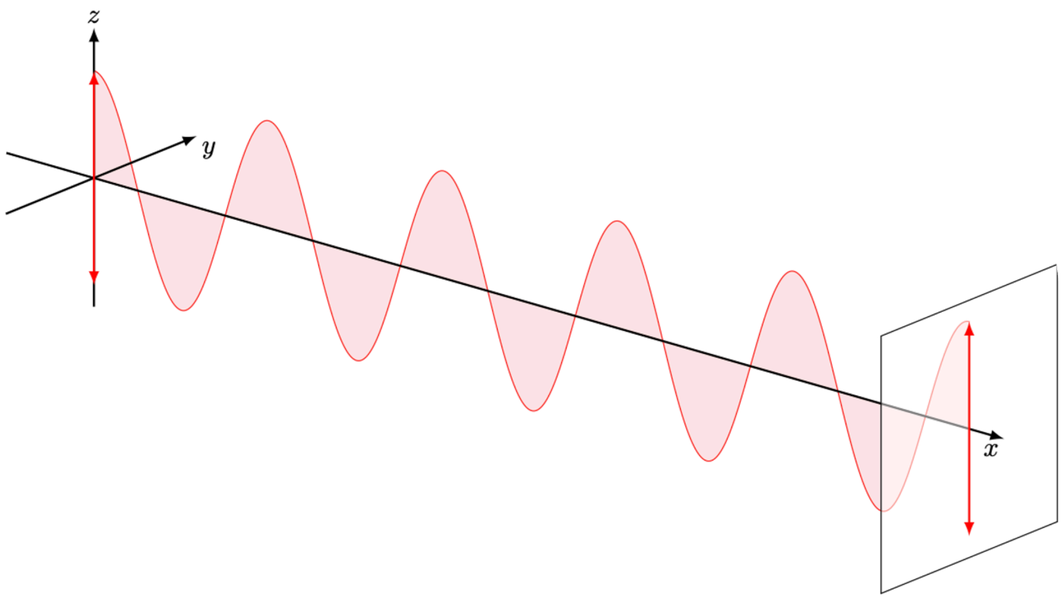
$|\leftrightarrow\rangle$



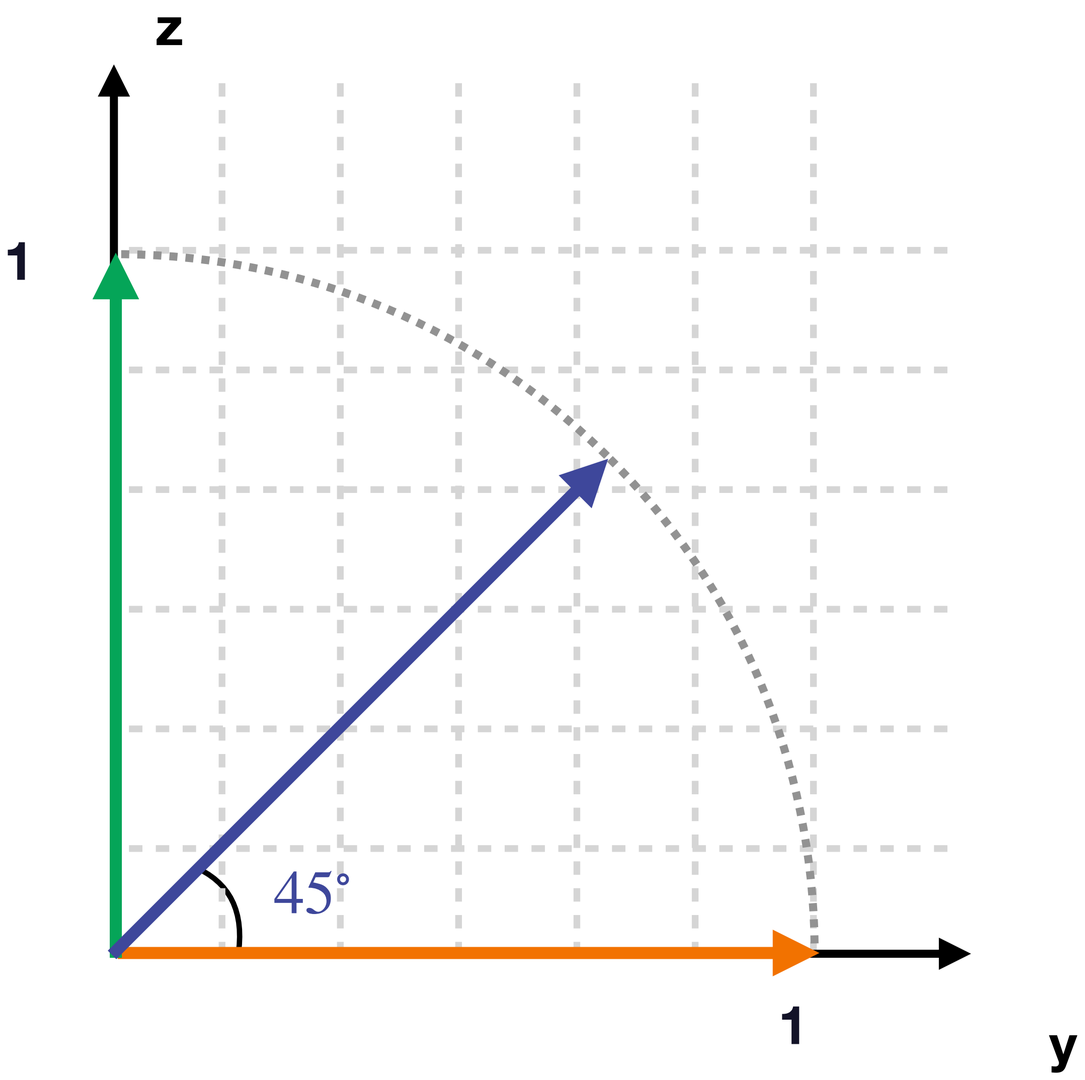
Measurement



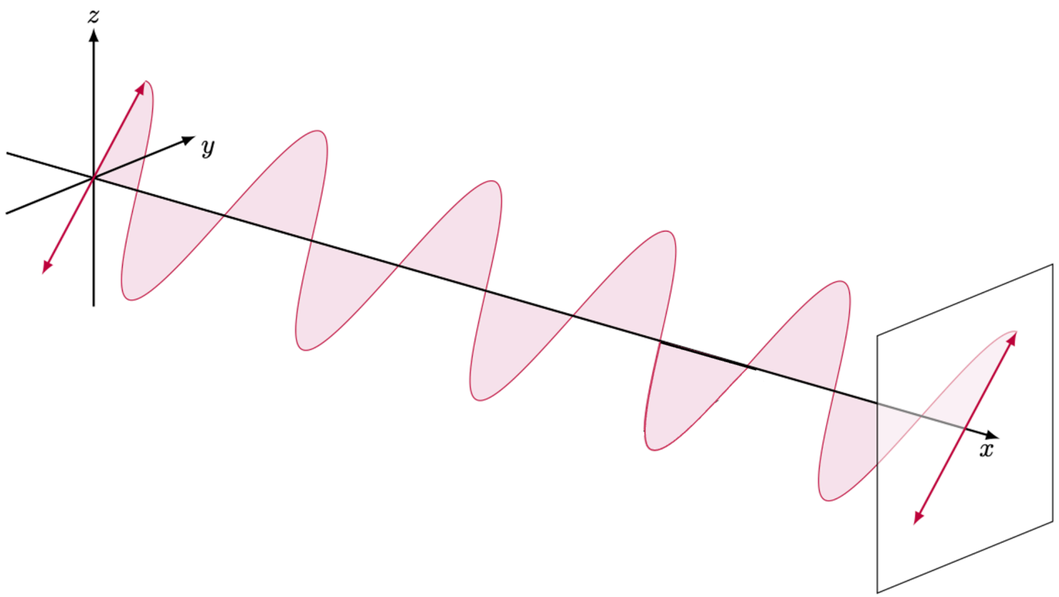
$|\leftrightarrow\rangle \quad |\updownarrow\rangle$



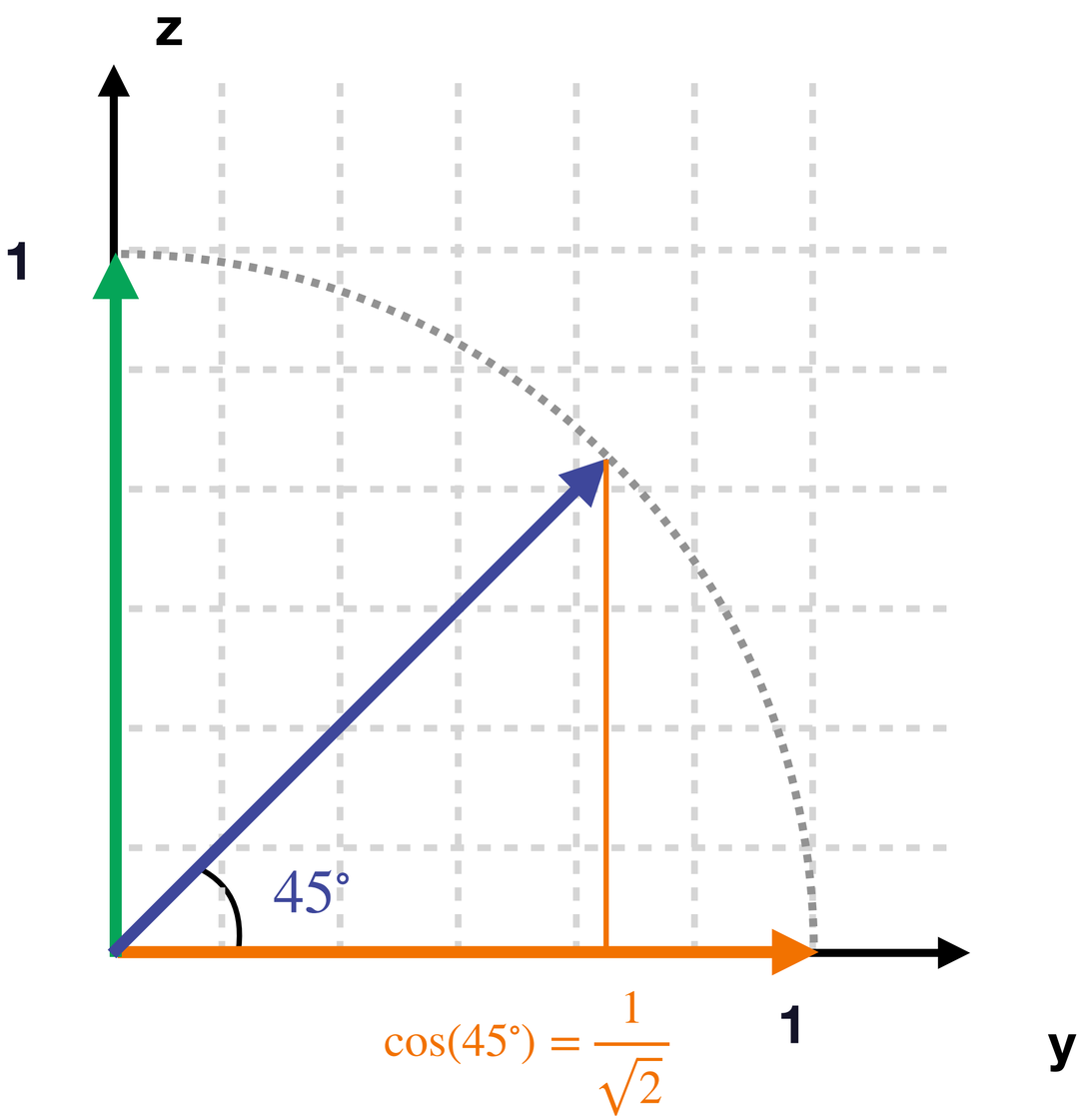
Measurement



$|\leftrightarrow\rangle \quad |\updownarrow\rangle \quad |\nearrow\!\!\!\!\swarrow\rangle$



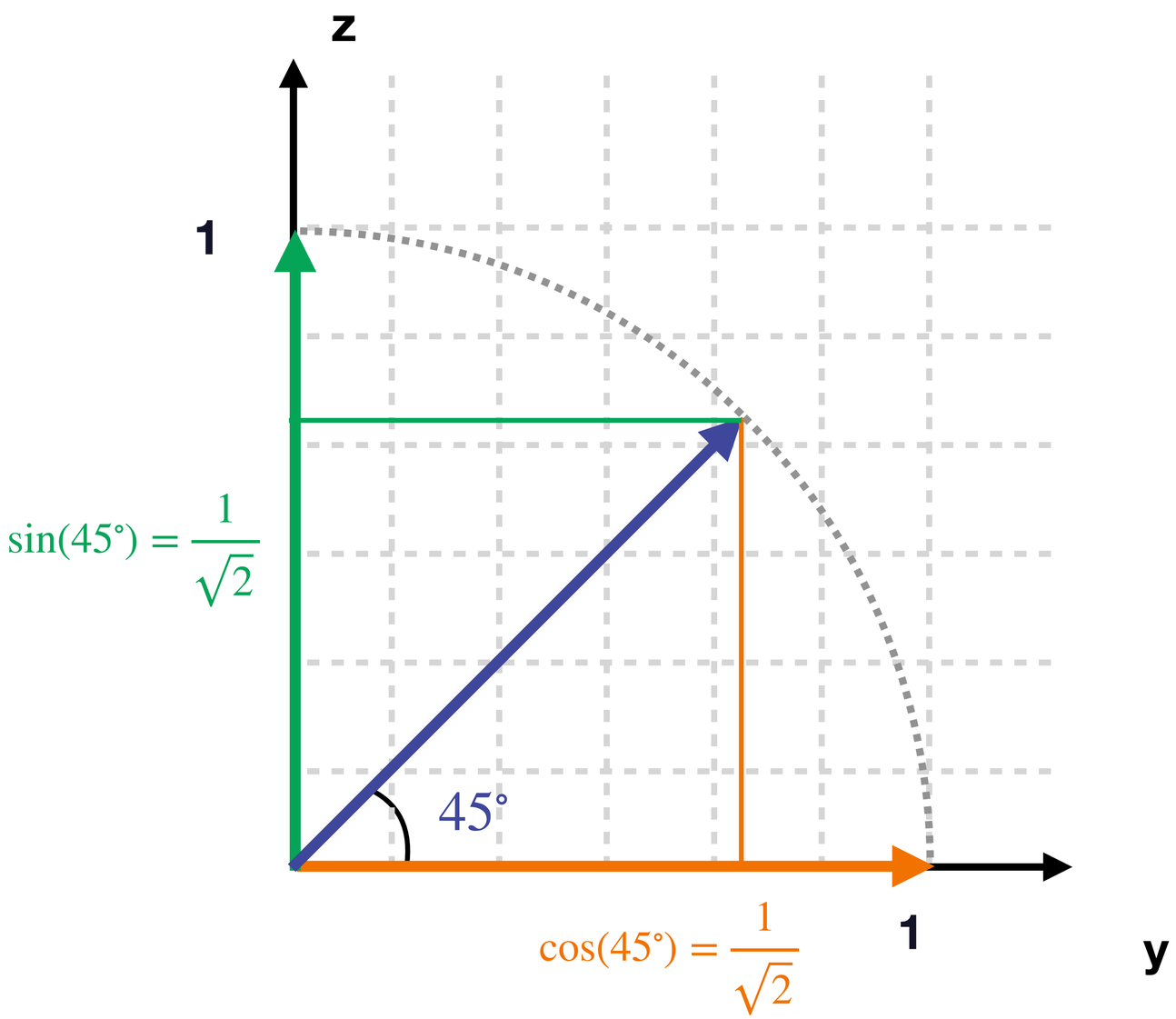
Measurement



$|\leftrightarrow\rangle \quad |\updownarrow\rangle \quad |\nearrow\!\!\!\swarrow\rangle$

$$|\nearrow\!\!\!\swarrow\rangle = \frac{1}{\sqrt{2}}|\leftrightarrow\rangle +$$

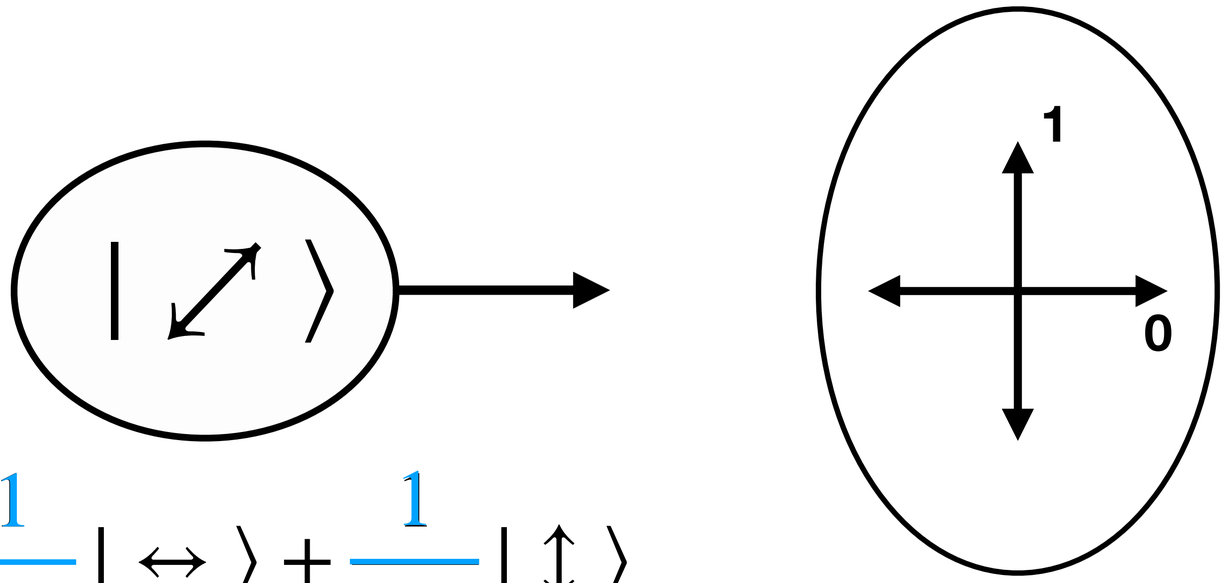
Measurement



$|\leftrightarrow\rangle \quad |\updownarrow\rangle \quad |\nearrow\!\!\!\swarrow\rangle$

$$|\nearrow\!\!\!\swarrow\rangle = \frac{1}{\sqrt{2}}|\leftrightarrow\rangle + \frac{1}{\sqrt{2}}|\updownarrow\rangle$$

Measurement



$$\frac{1}{\sqrt{2}}|\leftrightarrow\rangle + \frac{1}{\sqrt{2}}|\updownarrow\rangle$$

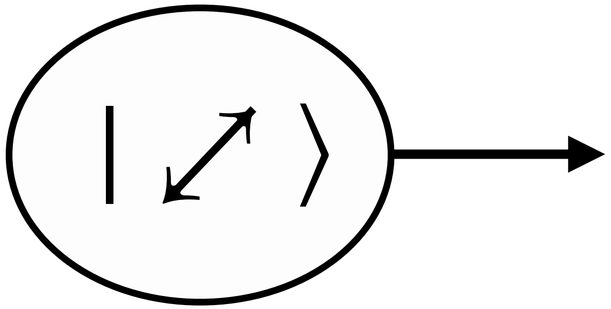
$$|45^\circ\rangle \equiv |\nearrow\swarrow\rangle$$

$$|135^\circ\rangle \equiv |\nwarrow\searrow\rangle$$

?

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

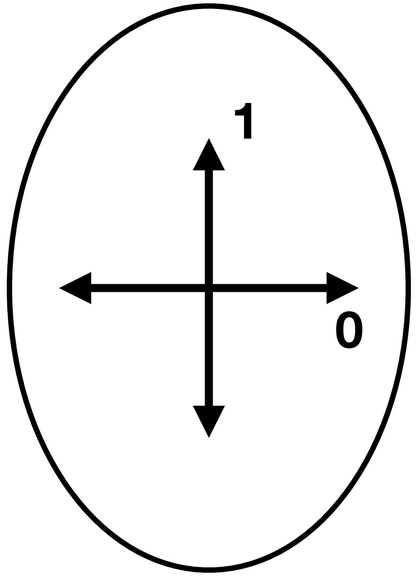
Measurement



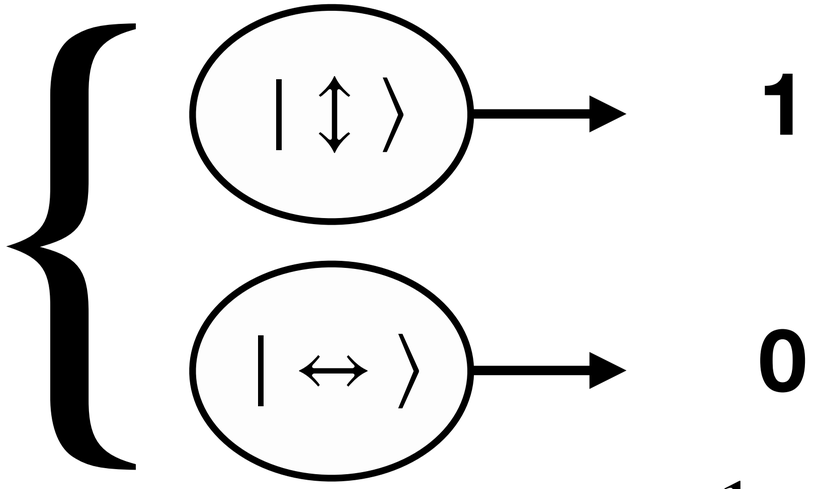
$$\frac{1}{\sqrt{2}}|\leftrightarrow\rangle + \frac{1}{\sqrt{2}}|\updownarrow\rangle$$

$$|45^\circ\rangle \equiv |\nearrow\swarrow\rangle$$

$$|135^\circ\rangle \equiv |\nwarrow\searrow\rangle$$



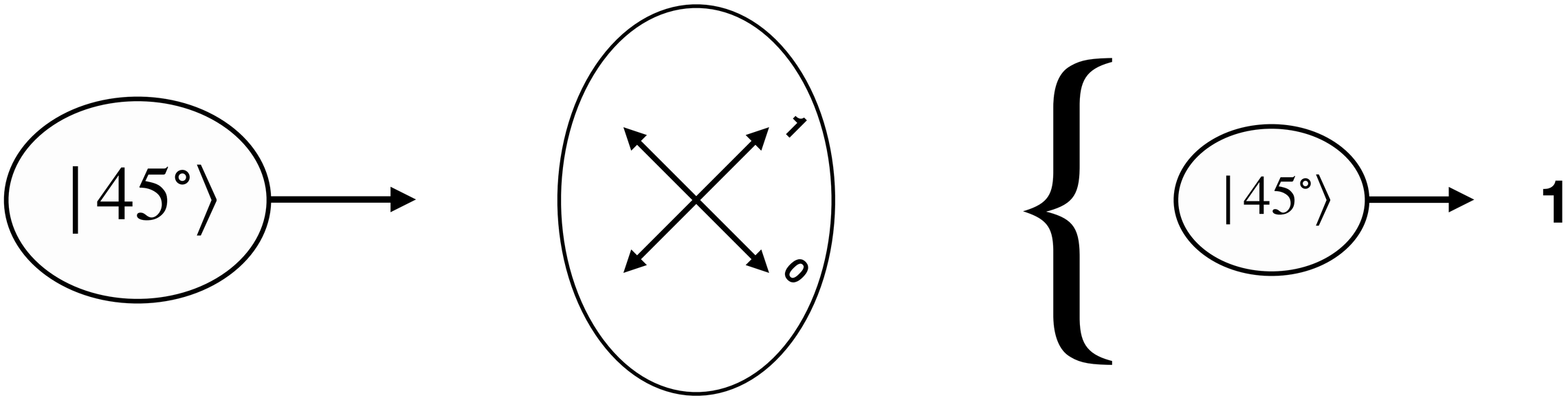
$$P_{|\updownarrow\rangle} = \frac{1}{2}$$



$$P_{|\leftrightarrow\rangle} = \frac{1}{2}$$

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

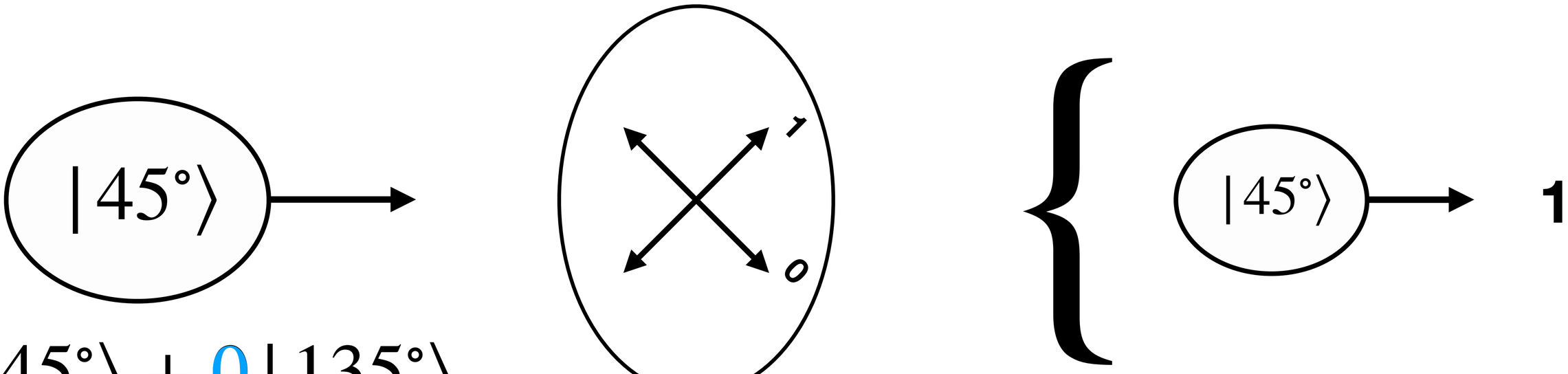
Mesure



$|45°\rangle \equiv |\nearrow\swarrow\rangle$

$|135°\rangle \equiv |\nwarrow\searrow\rangle$

Mesure



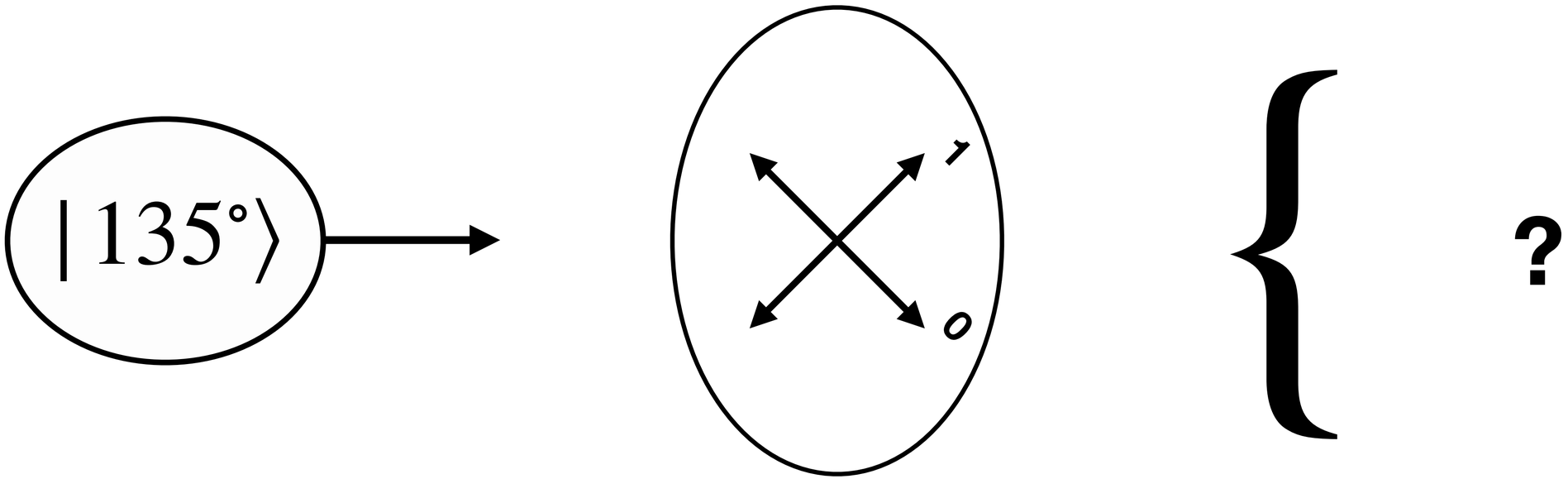
$$1|45^\circ\rangle + 0|135^\circ\rangle$$

$$|45^\circ\rangle \equiv |\nearrow\swarrow\rangle$$

$$|135^\circ\rangle \equiv |\nwarrow\searrow\rangle$$

$$P_{|45^\circ\rangle} = |1|^2 \qquad P_{|135^\circ\rangle} = |0|^2$$

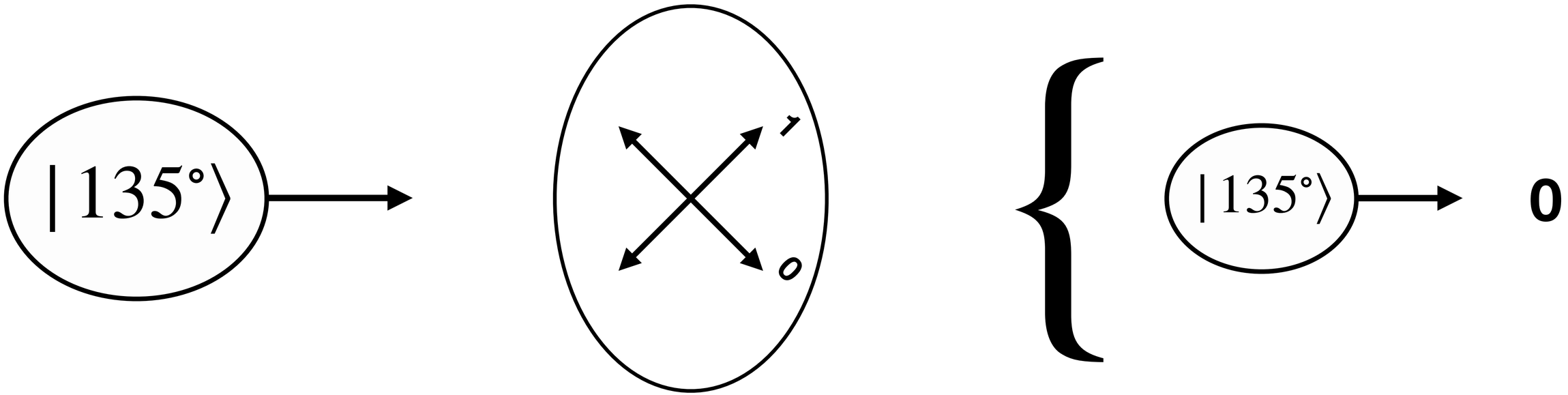
Mesure



$|45°\rangle \equiv |\nearrow\swarrow\rangle$

$|135°\rangle \equiv |\nwarrow\searrow\rangle$

Mesure



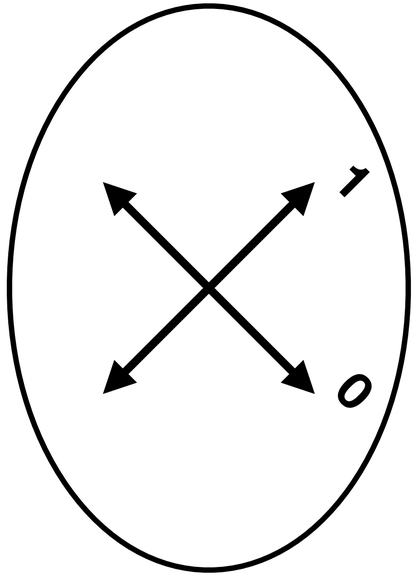
$|45°\rangle \equiv |\ \nearrow\!\!\!\!\swarrow\ \rangle$

$|135°\rangle \equiv |\ \nwarrow\!\!\!\!\searrow\ \rangle$

Mesure

$|135°\rangle$

$1|0°\rangle + 0|90°\rangle$



$|135°\rangle$ → **0**

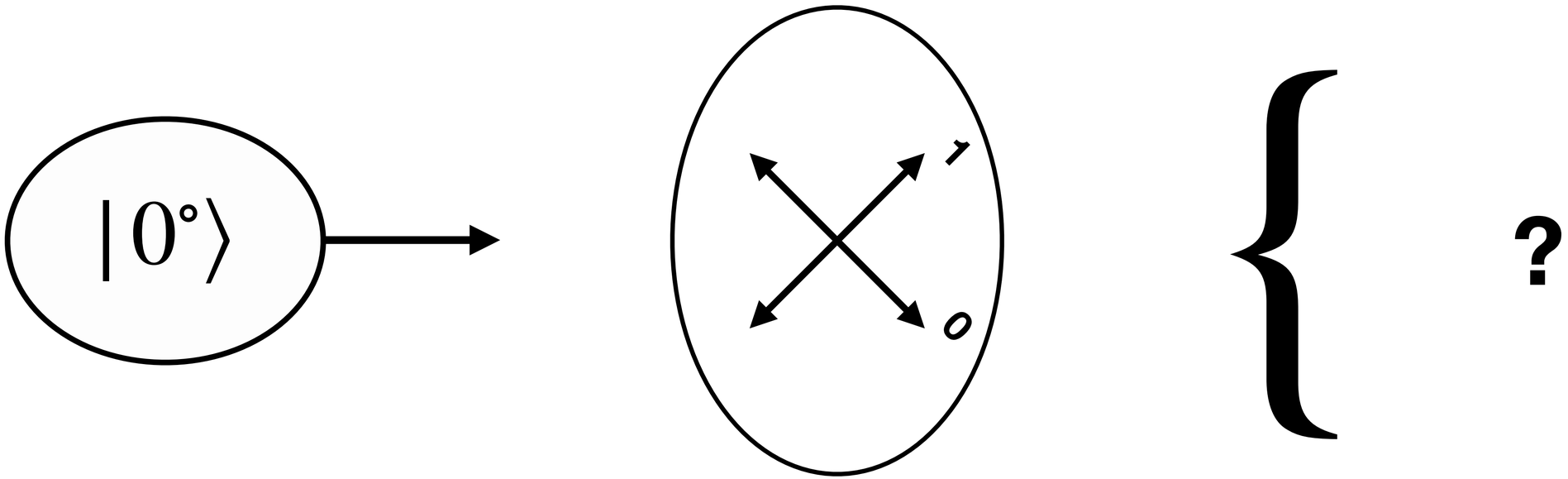
$|45°\rangle \equiv |\nearrow\swarrow\rangle$

$|135°\rangle \equiv |\nwarrow\searrow\rangle$

$P_{|0°\rangle} = |1|^2$

$P_{|90°\rangle} = |0|^2$

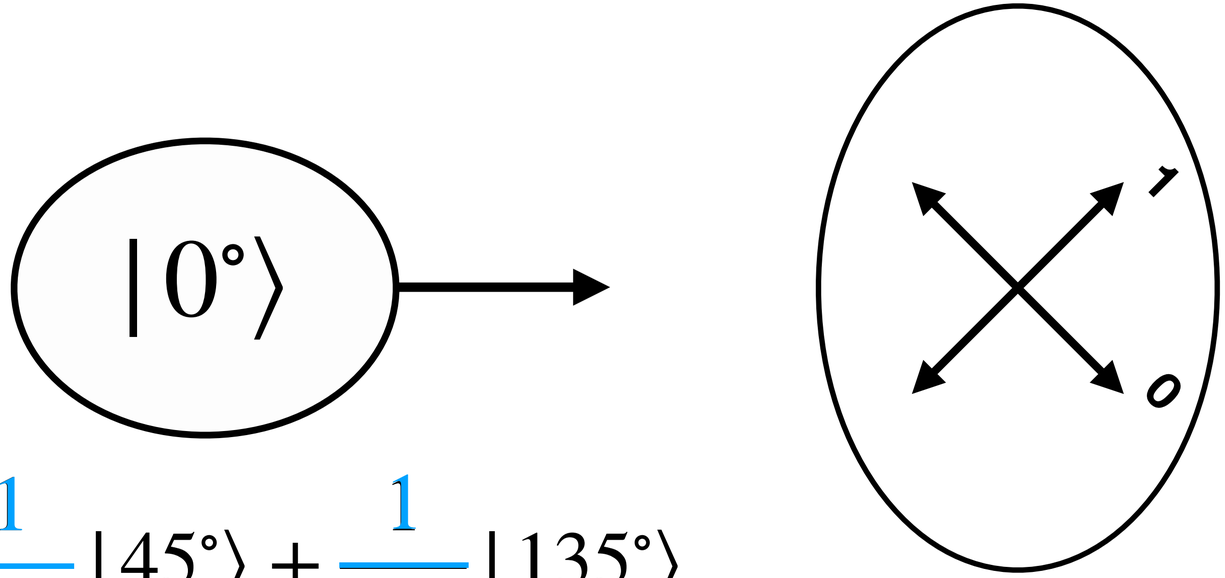
Mesure



$|45°\rangle \equiv |\nearrow\swarrow\rangle$

$|135°\rangle \equiv |\nwarrow\searrow\rangle$

Mesure



$$\frac{1}{\sqrt{2}}|45°\rangle + \frac{1}{\sqrt{2}}|135°\rangle$$

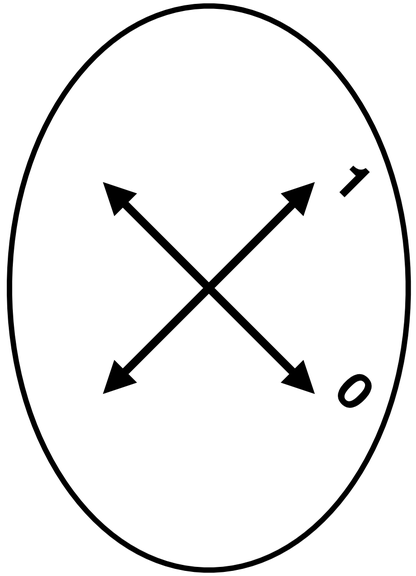
$|45°\rangle \equiv |\nearrow\swarrow\rangle$

$|135°\rangle \equiv |\nwarrow\searrow\rangle$

{ ?

Mesure

$$|0°\rangle \longrightarrow$$



$$\frac{1}{\sqrt{2}}|45°\rangle + \frac{1}{\sqrt{2}}|135°\rangle$$

$$|45°\rangle \equiv |\nearrow\swarrow\rangle$$

$$|135°\rangle \equiv |\nwarrow\searrow\rangle$$

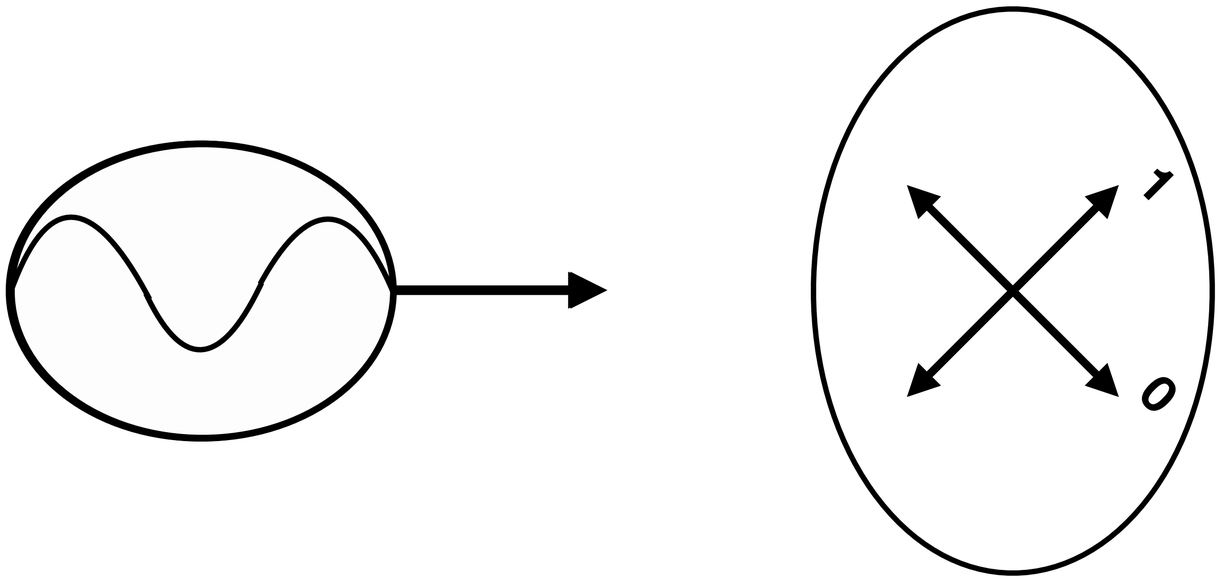
$$P_{|45°\rangle} = \frac{1}{2}$$

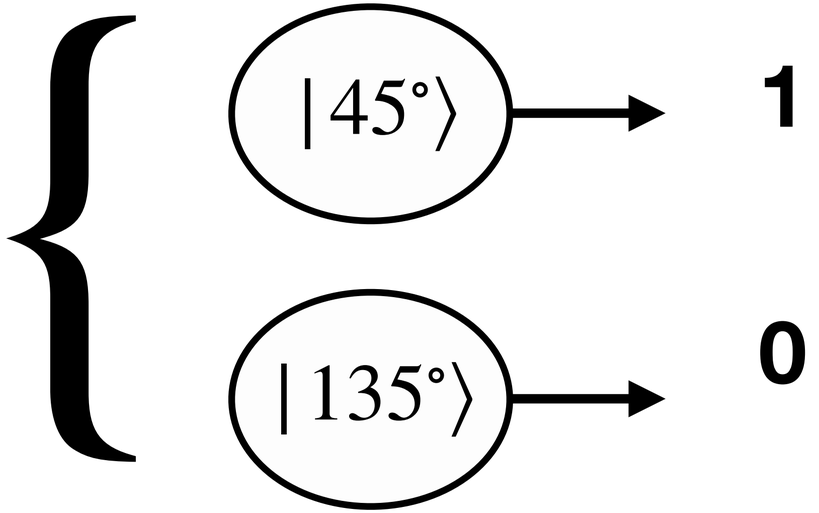
$$\left\{ \begin{array}{ll} |45°\rangle \longrightarrow & \mathbf{1} \\ |135°\rangle \longrightarrow & \mathbf{0} \end{array} \right.$$

$$P_{|135°\rangle} = \frac{1}{2}$$

Mesure

$$P_{|45^\circ\rangle} = |\alpha|^2$$





$$P_{|135^\circ\rangle} = |\beta|^2$$

$|45^\circ\rangle \equiv |\nearrow\swarrow\rangle$

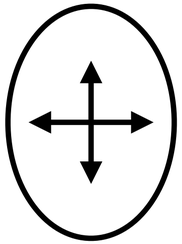
$|135^\circ\rangle \equiv |\nwarrow\searrow\rangle$

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

Superposition & Quantum Measurement

Key points

- Quantum measurement collapses the polarization into one of the basis states of the measurement basis.

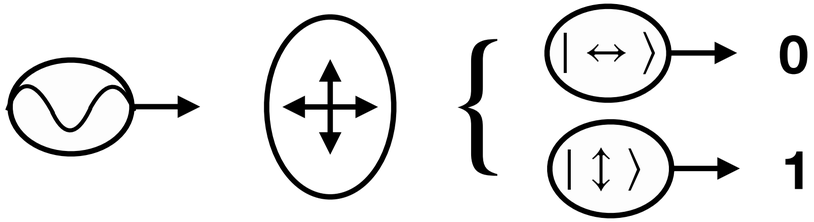


$|\updownarrow\rangle$ ou $|\leftrightarrow\rangle$

Superposition & Quantum Measurement

Key points

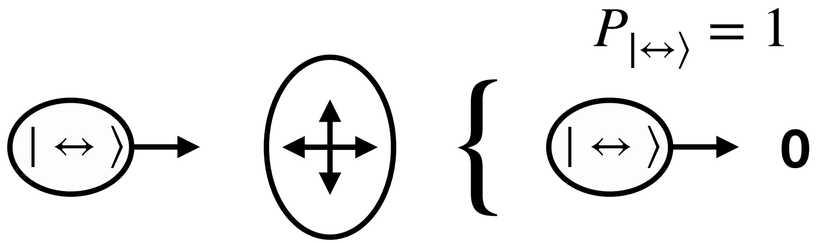
- Quantum measurement collapses the polarization into one of the basis states of the measurement basis.
- If the incident photon is in a superposition state, the measurement result is random.



Superposition & Quantum Measurement

Key points

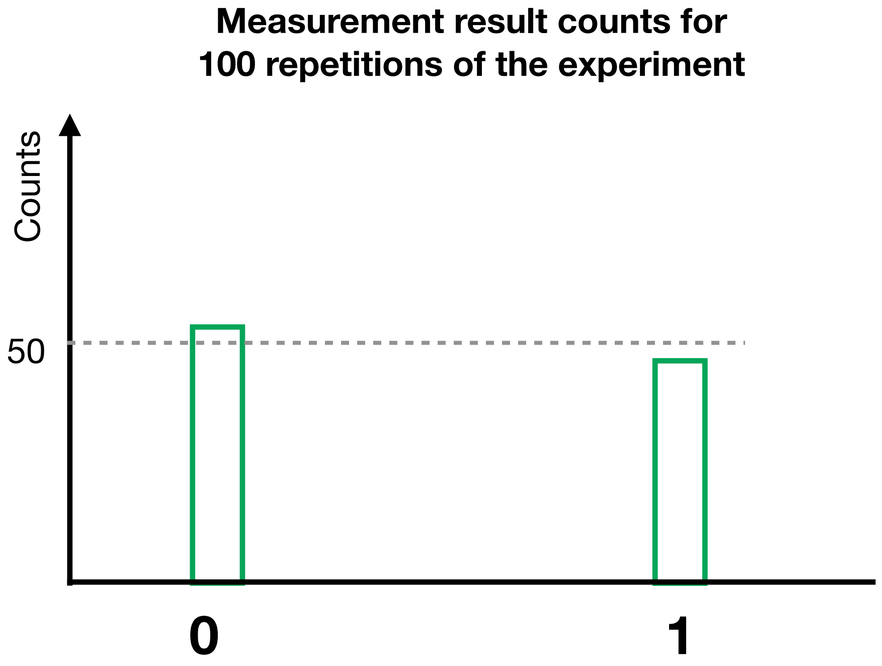
- Quantum measurement collapses the polarization into one of the basis states of the measurement basis.
- If the incident photon is in a superposition state, the measurement result is random.
- If the incident photon is in a basis state of the measurement basis, the result will always be the same.



Superposition & Quantum Measurement

Key points

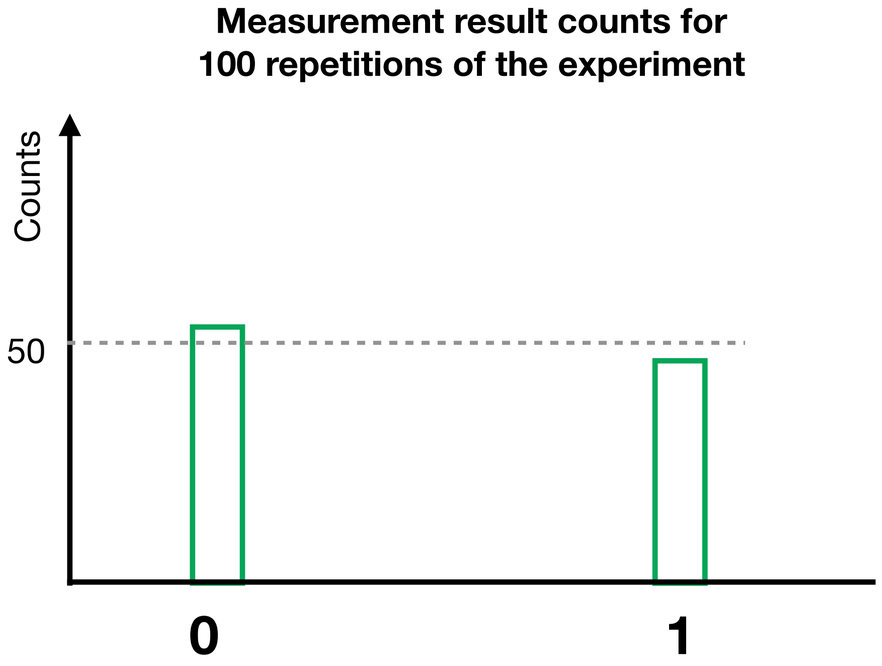
- Quantum measurement collapses the polarization into one of the basis states of the measurement basis.
- If the incident photon is in a superposition state, the measurement result is random.
- If the incident photon is in a basis state of the measurement basis, the result will always be the same.
- To describe the quantum state of an incident photon, the measurement experiment must be repeated multiple times and the results compiled to build statistics.



Superposition & Quantum Measurement

Key points

- Quantum measurement collapses the polarization into one of the basis states of the measurement basis.
- If the incident photon is in a superposition state, the measurement result is random.
- If the incident photon is in a basis state of the measurement basis, the result will always be the same.
- To describe the quantum state of an incident photon, the measurement experiment must be repeated multiple times and the results compiled to build statistics.
- Otherwise, we cannot say anything.



Encoding Information

Bit to transmit

0

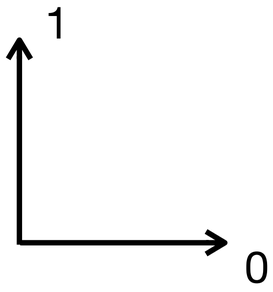
1

Encoding Information

Bit to transmit

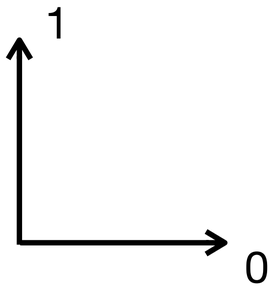
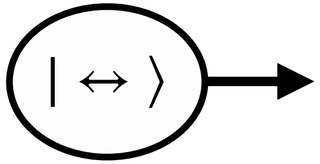
Measurement basis

0

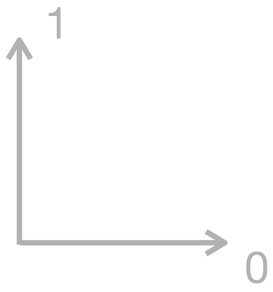
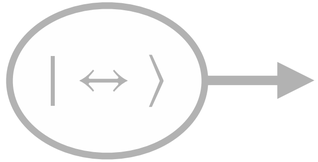
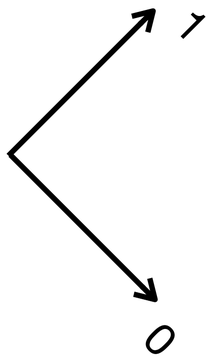


1

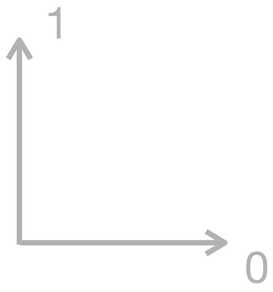
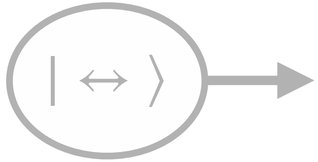
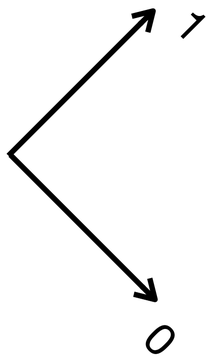
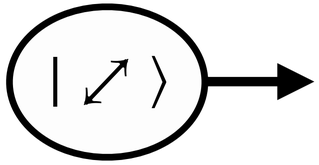
Encoding Information

Bit to transmit	Measurement basis		Encoded photon
0		$\Rightarrow$	
1			

Encoding Information

Bit to transmit	Measurement basis		Encoded photon
0		$\Rightarrow$	
1			

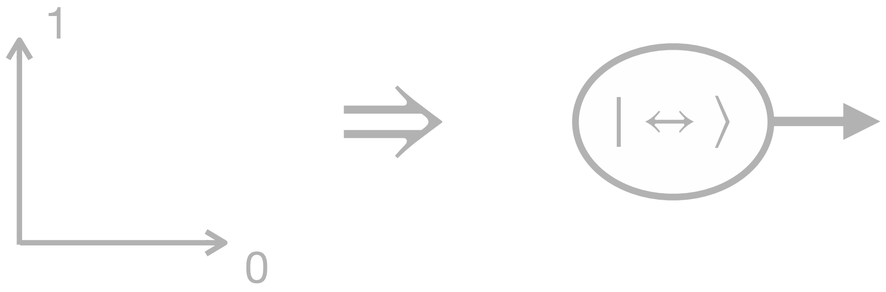
Encoding Information

Bit to transmit	Measurement basis		Encoded photon
0		⇒	
1		⇒	

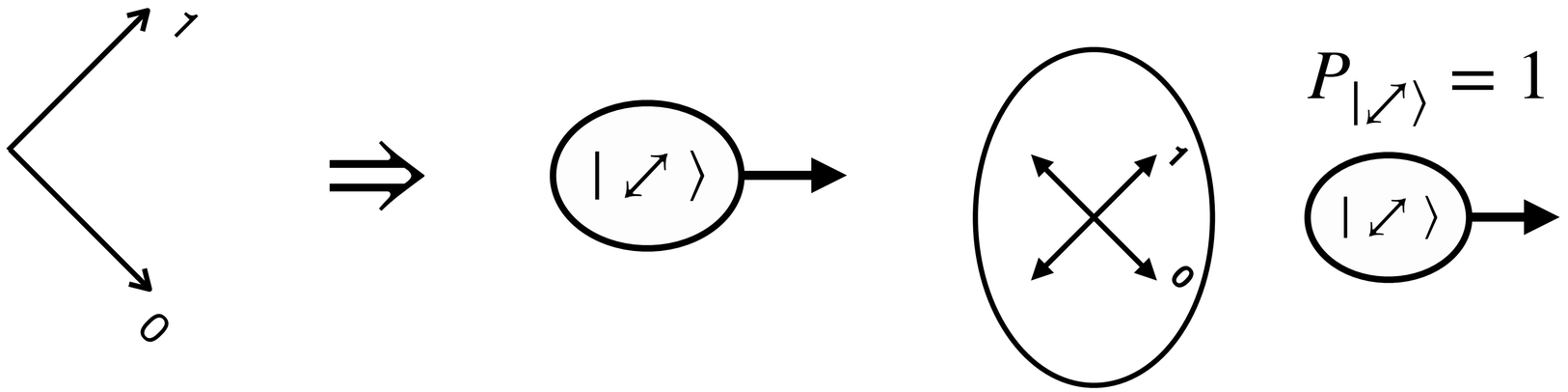
Encoding Information

Bit to transmit | **Measurement basis** | **Encoded photon** | **Transmitted bit**

0

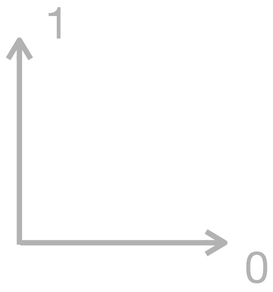
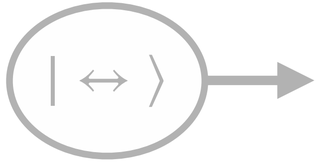
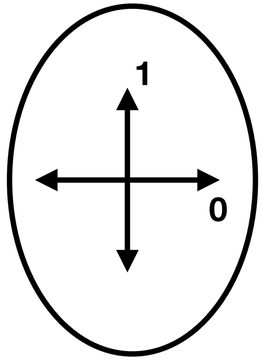
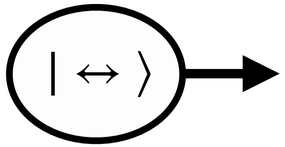
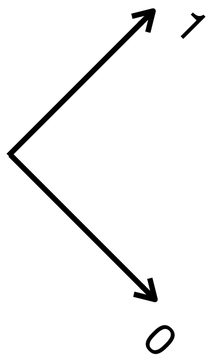
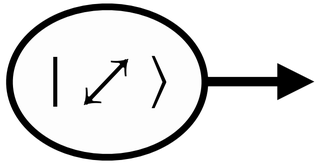
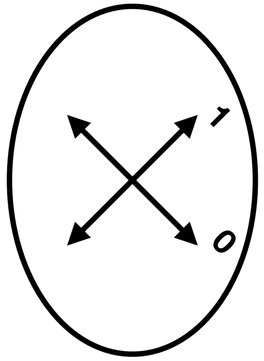
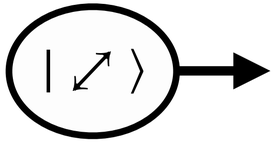


1



1

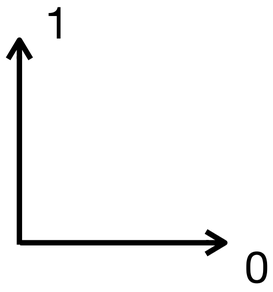
Encoding Information

Bit to transmit	Measurement basis		Encoded photon			Transmitted bit
0		$\Rightarrow$			$P_{\lvert\leftrightarrow\rangle} = 1$ 	0
1		$\Rightarrow$			$P_{\lvert\nearrow\rangle} = 1$ 	1

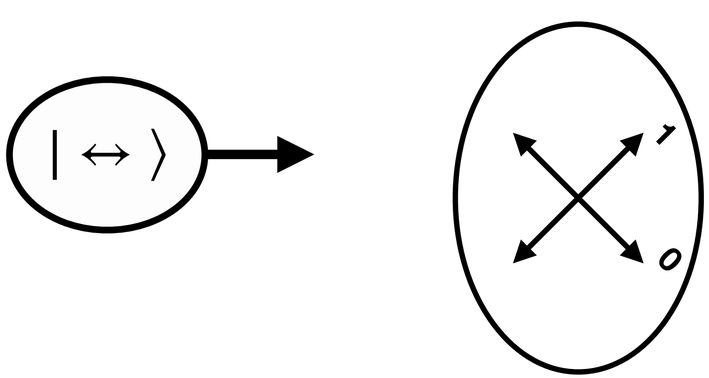
Encoding Information

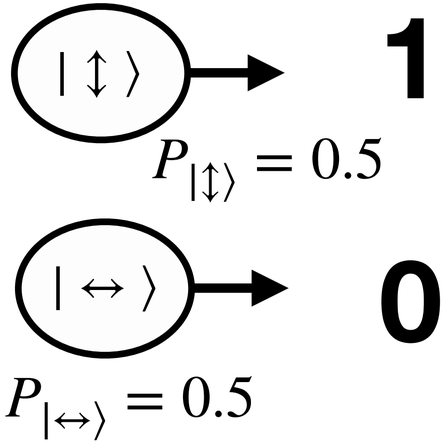
Bit to transmit | **Measurement basis** | **Encoded photon** | **Transmitted bit**

0

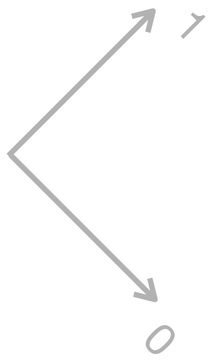


$\Rightarrow$

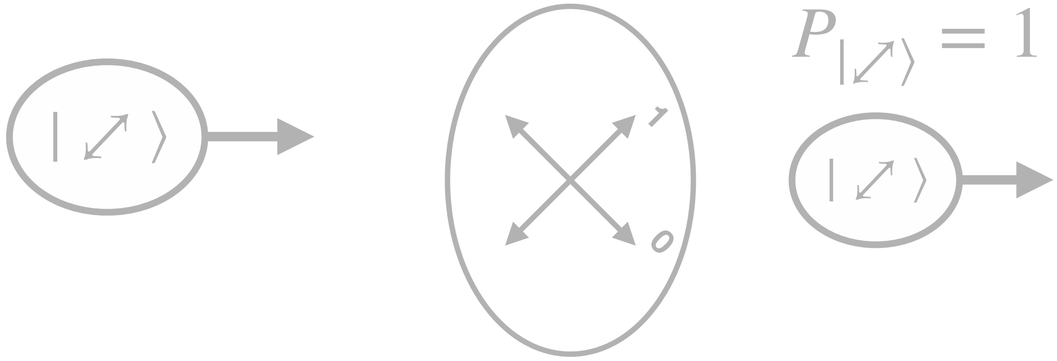




1

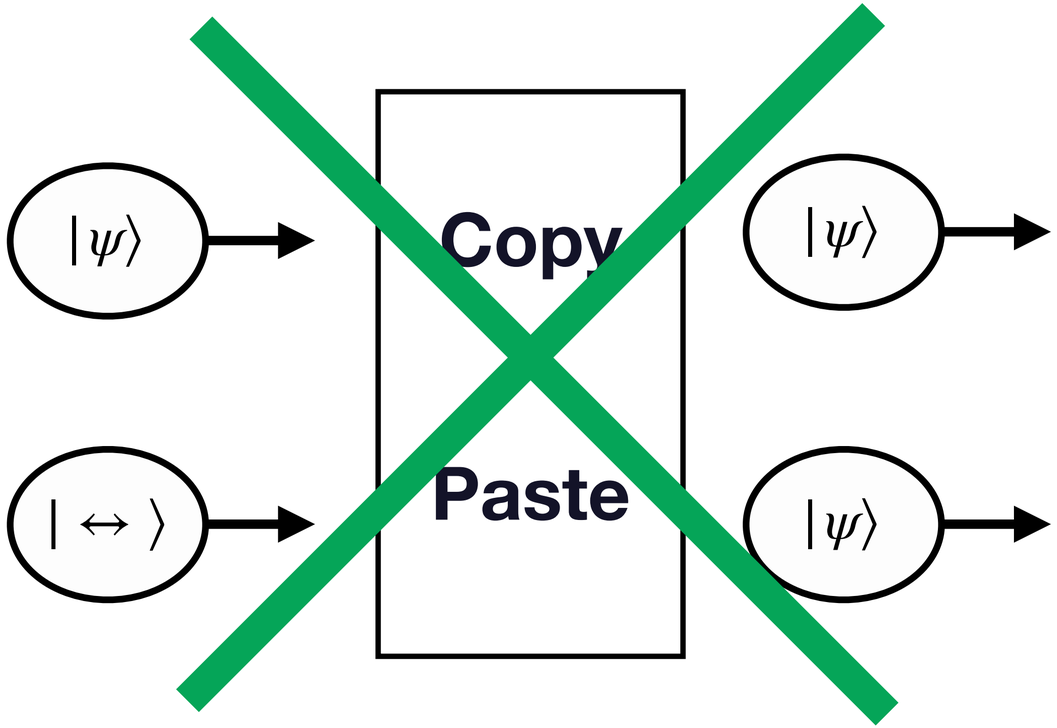


$\Rightarrow$



No-Cloning Theorem

"It is impossible to copy the quantum state of one photon into the quantum state of a second one."



Plan

- ✓ Presentation
- ✓ Cryptography
- ✓ The qubit
- The photon: messenger of quantum information
- Entanglement and CHSH inequality
- Protocol E91
- Hands-on session

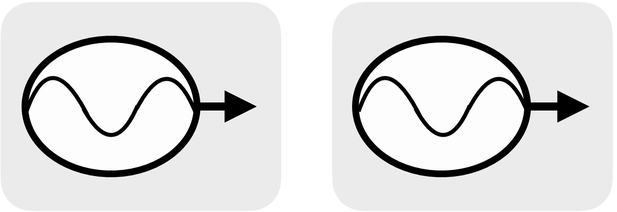
Plan

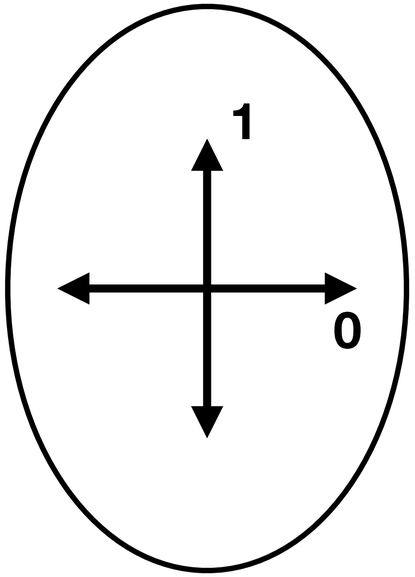
- ✓ Presentation
- ✓ Cryptography
- ✓ The qubit
- ✓ The photon: messenger of quantum information
- ○ Entanglement and CHSH inequality
- ○ Protocol E91
- ○ Hands-on session

Plan

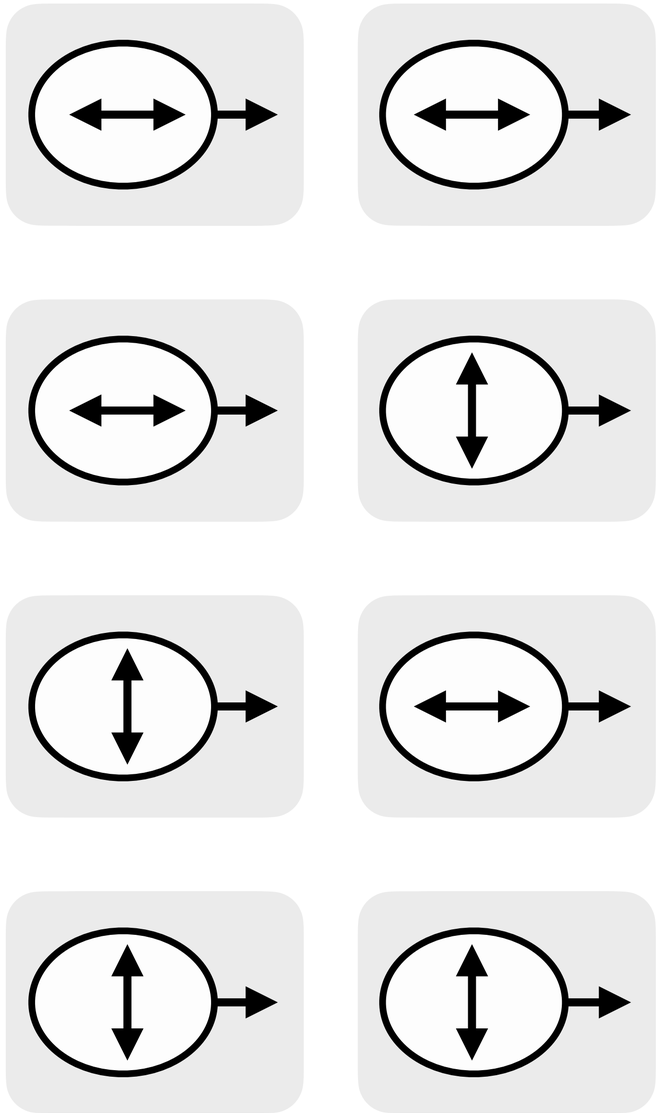
- ✓ Presentation
- ✓ Cryptography
- ✓ The qubit
- ✓ The photon: messenger of quantum information
- Entanglement and CHSH inequality
- Protocol E91
- Hands-on session

Entanglement





$$\alpha|\leftrightarrow\leftrightarrow\rangle + \beta|\leftrightarrow\updownarrow\rangle$$
$$+\delta|\updownarrow\leftrightarrow\rangle + \gamma|\updownarrow\updownarrow\rangle$$



$$P_{|\leftrightarrow\leftrightarrow\rangle} = |\alpha|^2$$

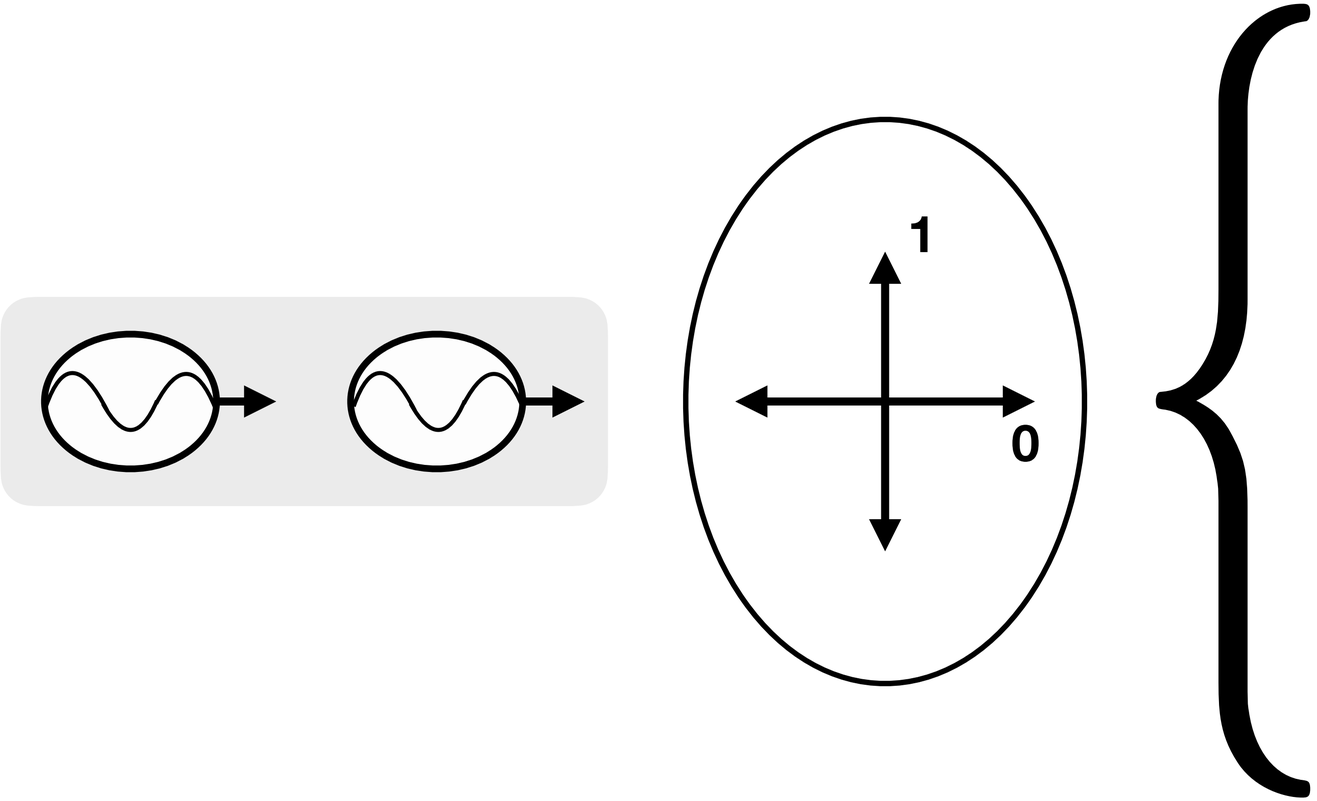
$$P_{|\leftrightarrow\updownarrow\rangle} = |\beta|^2$$

$$P_{|\updownarrow\leftrightarrow\rangle} = |\delta|^2$$

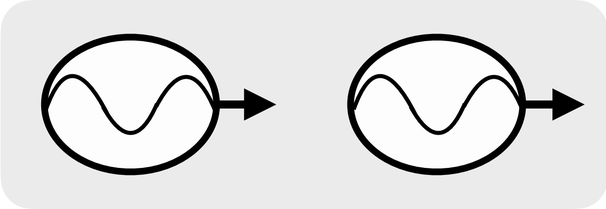
$$P_{|\updownarrow\updownarrow\rangle} = |\gamma|^2$$

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

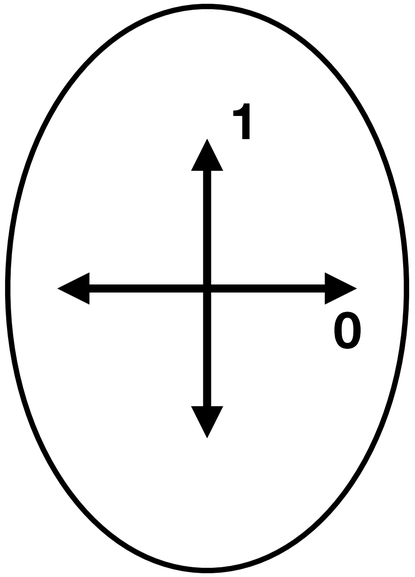
Entanglement



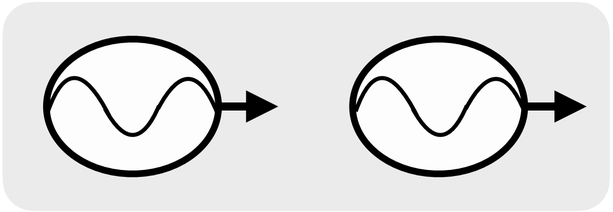
Entanglement



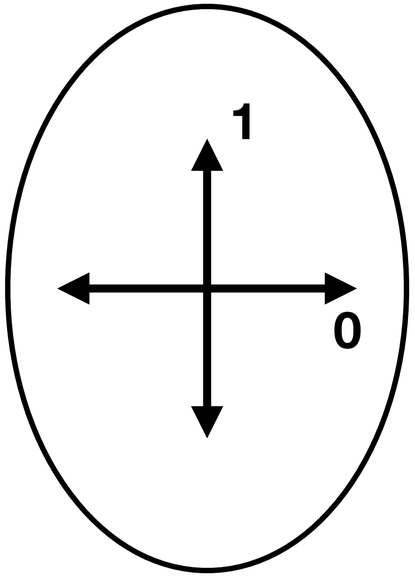
$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle+\frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$

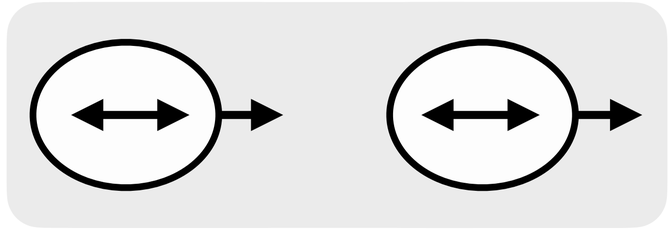


Entanglement

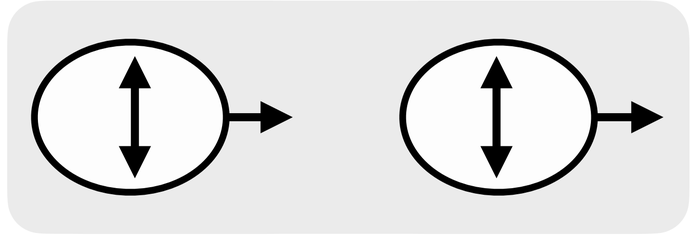


$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle + \frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$



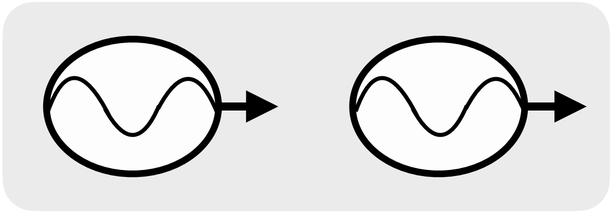


$$P_{|\leftrightarrow\leftrightarrow\rangle} = \frac{1}{2}$$

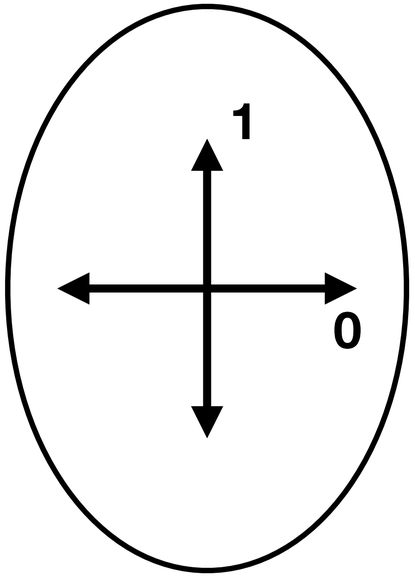


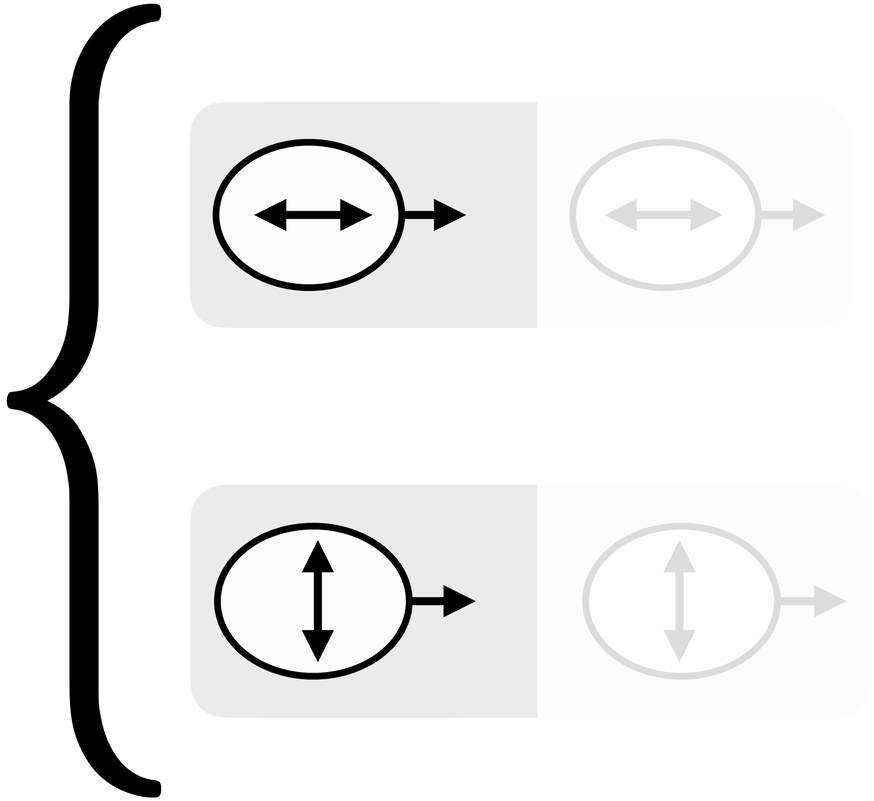
$$P_{|\updownarrow\updownarrow\rangle} = \frac{1}{2}$$

Entanglement



$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle + \frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$





$$P_{|\leftrightarrow\leftrightarrow\rangle} = \frac{1}{2}$$

$$P_{|\updownarrow\updownarrow\rangle} = \frac{1}{2}$$

Bell Pairs

$$\Phi^+$$

$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle + \frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$

$$\Phi^-$$

$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle - \frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$

$$\Psi^+$$

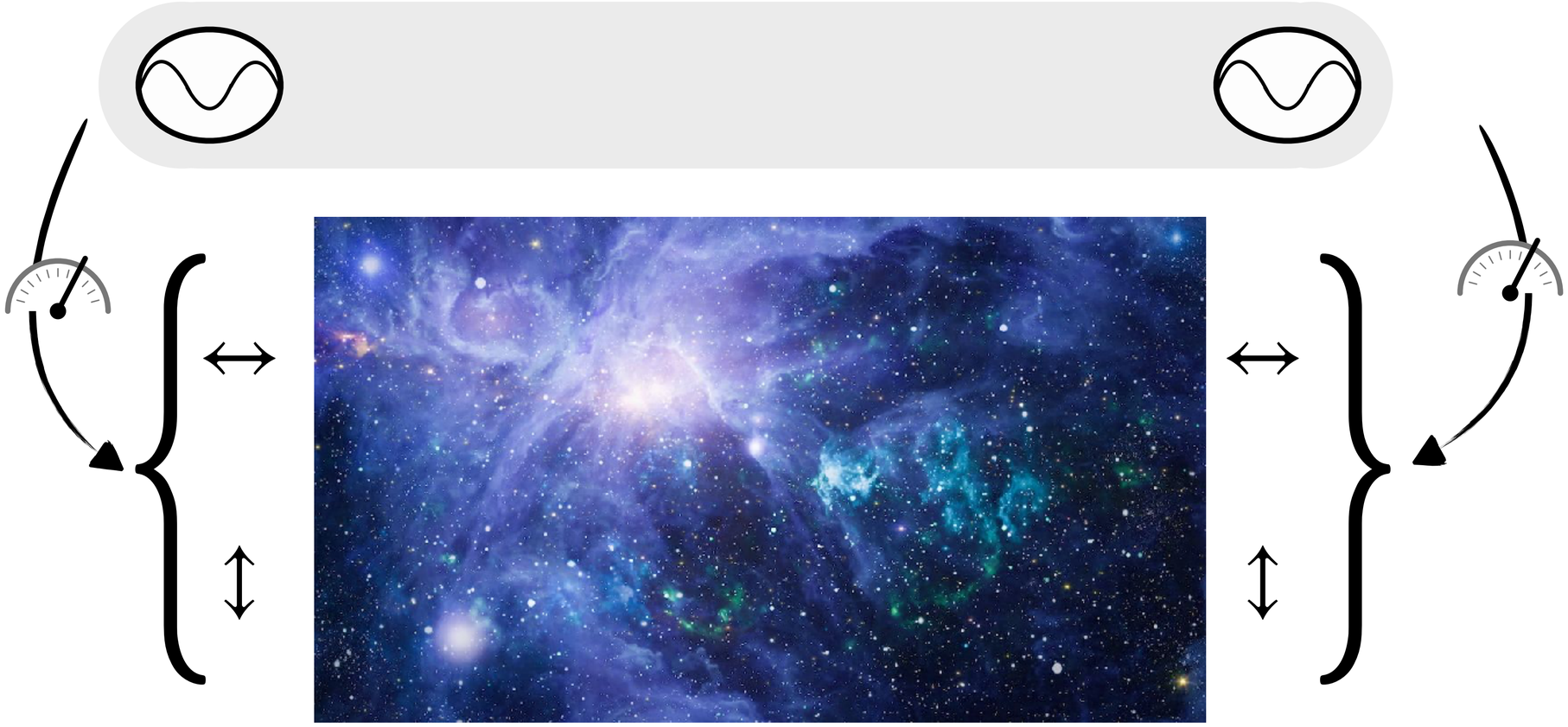
$$\frac{1}{\sqrt{2}}|\leftrightarrow\updownarrow\rangle + \frac{1}{\sqrt{2}}|\updownarrow\leftrightarrow\rangle$$

$$\Psi^-$$

$$\frac{1}{\sqrt{2}}|\leftrightarrow\updownarrow\rangle - \frac{1}{\sqrt{2}}|\updownarrow\leftrightarrow\rangle$$

Distance-independent correlations

$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle+\frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$

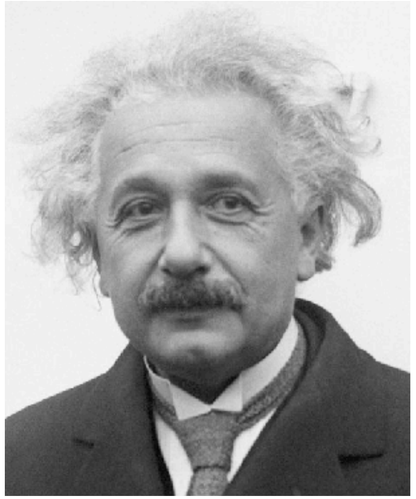


© Shutterstock

Interpreting Entanglement

AB Lagrelius & Westphal

The measurement of the first entangled photon instantly determines the state of the second, regardless of the distance!

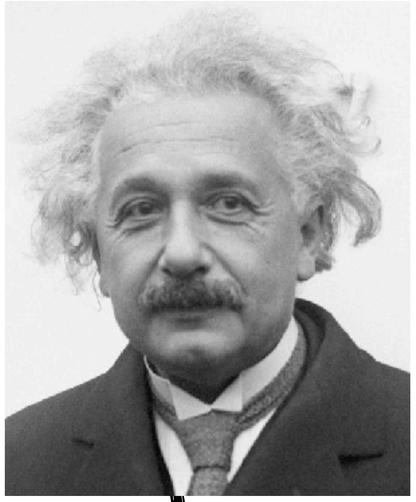


(Image credit: Bettmann / Contributor via Getty Images)

Interpreting Entanglement

AB Lagrelius & Westphal

The measurement of the first entangled photon instantly determines the state of the second, regardless of the distance!



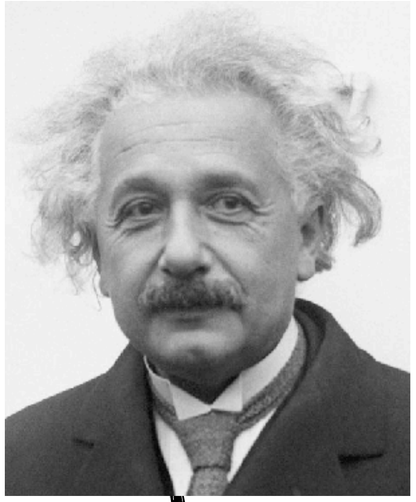
(Image credit: Bettmann / Contributor via Getty Images)

Impossible! The choice of the state must be determined before the measurement! There must be hidden variables!

Interpreting Entanglement

AB Lagrelius & Westphal

non-locality!



(Image credit: Bettmann / Contributor via Getty Images)

Impossible!
The choice of the state must be determined before the measurement!
There must be hidden variables!

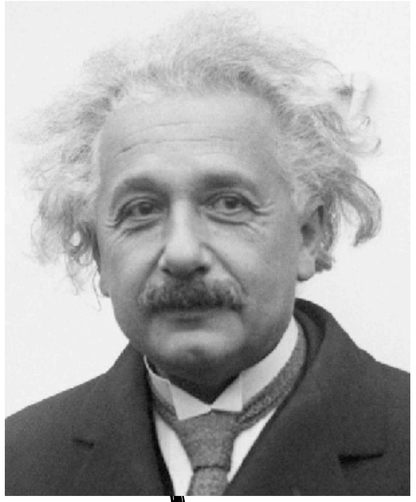
Interpreting Entanglement

AB Lagrelius & Westphal

non-locality!

Actually, I have a way to experimentally verify whether there are hidden variables or not!

1974, CERN



(Image credit: Bettmann / Contributor via Getty Images)

Impossible!
The choice of the state must be determined before the measurement!
There must be hidden variables!

Interpreting Entanglement

1974, CERN

Bell's Inequality

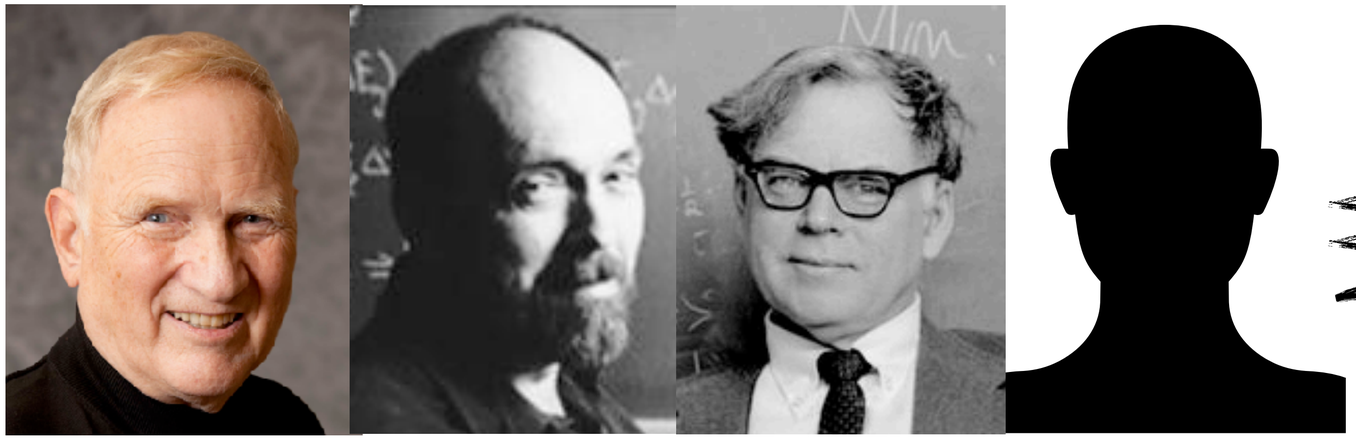
Interpreting Entanglement

1974, CERN

1964

Bell's Inequality

1969



John Clauser | Michael Horne | Abner Shimony | Richard Holt

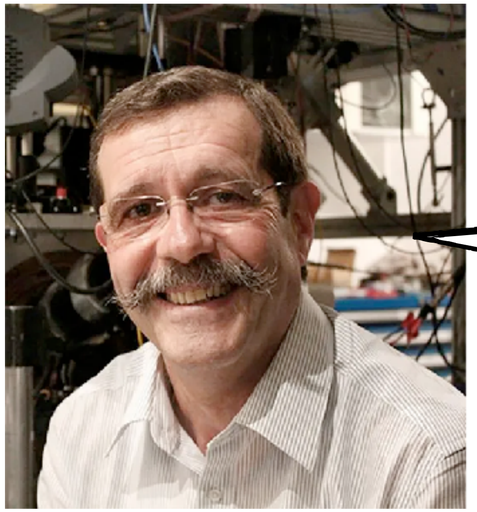
CHSH Inequality

Interpreting Entanglement

1974, CERN

1964

Bell's Inequality



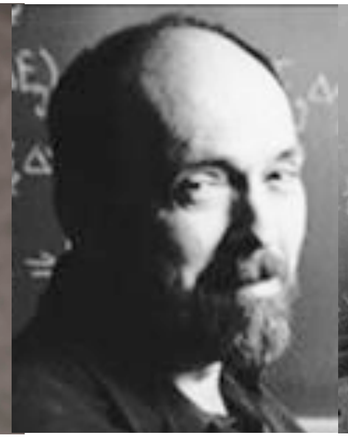
1982

Entanglement cannot be explained by a hidden variable theory!

EXPERIMENTALLY VERIFIED

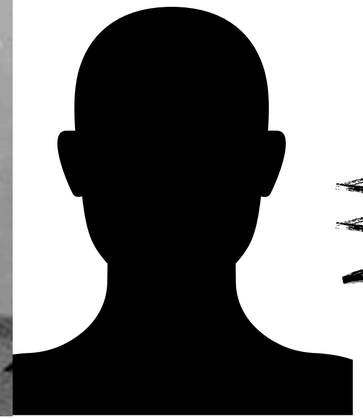
1969

John Clauser



Michael Horne

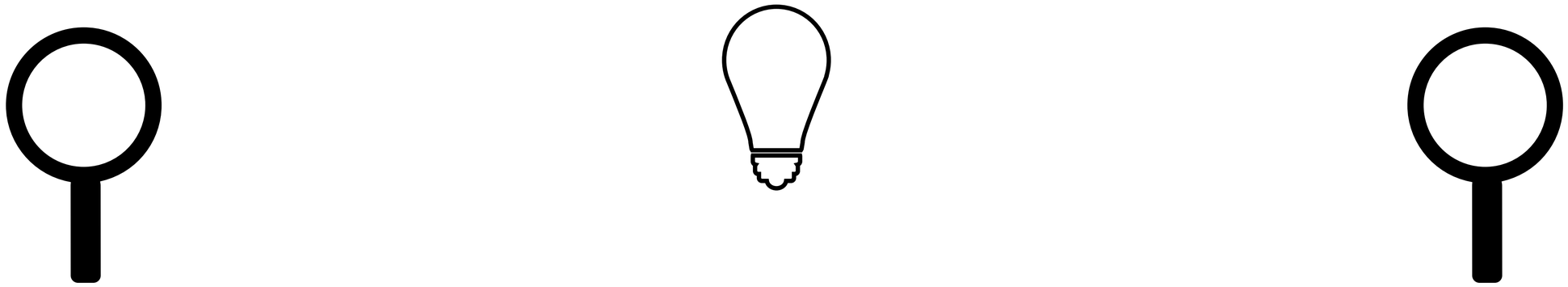
Abner Shimony



Richard Holt

CHSH Inequality

Bell Test



A

Bases: a_1, a_2

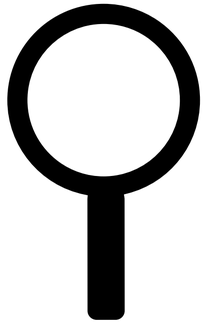
Results: {0, 1}

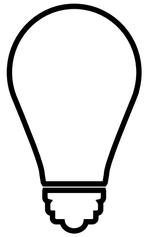
B

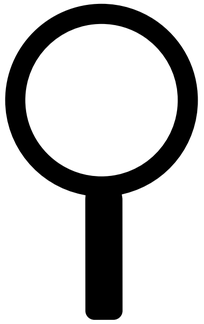
Bases: b_1, b_2

Results: {0, 1}

Bell Test







A

Bases: a_1, a_2

Results: ~~{0, 1}~~

{+1, -1}

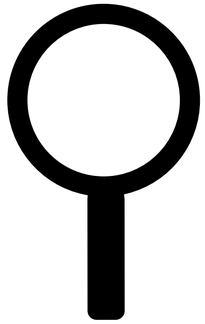
B

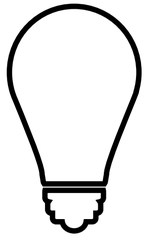
Bases: b_1, b_2

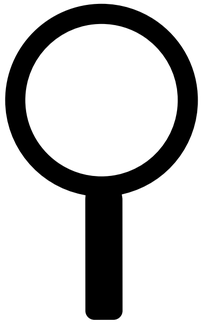
Results: ~~{0, 1}~~

{+1, -1}

Bell Test







A

Bases: a_1, a_2

Results: ~~{0, 1}~~

{+1, -1}

a_i	b_j	$a_i b_j$
+1	+1	+1
+1	-1	-1
-1	+1	-1
-1	-1	+1

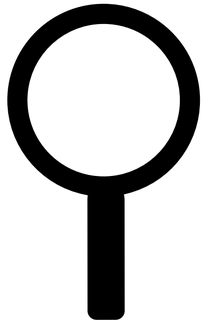
B

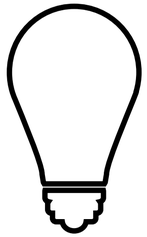
Bases: b_1, b_2

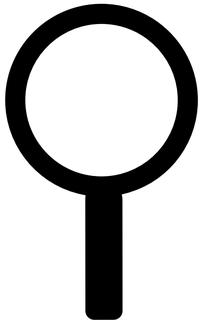
Results: ~~{0, 1}~~

{+1, -1}

Bell Test







A

Bases: a_1, a_2

Results: ~~{0, 1}~~

{+1, -1}

a_i	b_j	$a_i b_j$
+1	+1	+1
+1	-1	-1
-1	+1	-1
-1	-1	+1

B

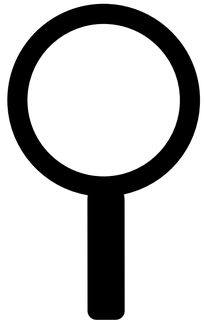
Bases: b_1, b_2

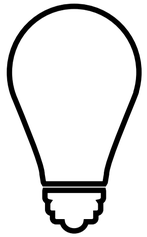
Results: ~~{0, 1}~~

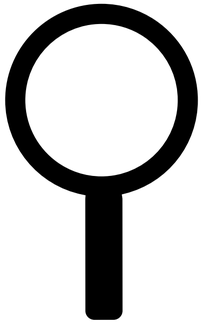
{+1, -1}

Same values detected at A and B

Bell Test







A

Bases: a_1, a_2

Results: ~~{0, 1}~~

{+1, -1}

a_i	b_j	$a_i b_j$
+1	+1	+1
+1	**-1**	**-1**
-1	**+1**	**-1**
-1	-1	+1

Different values detected at A and B

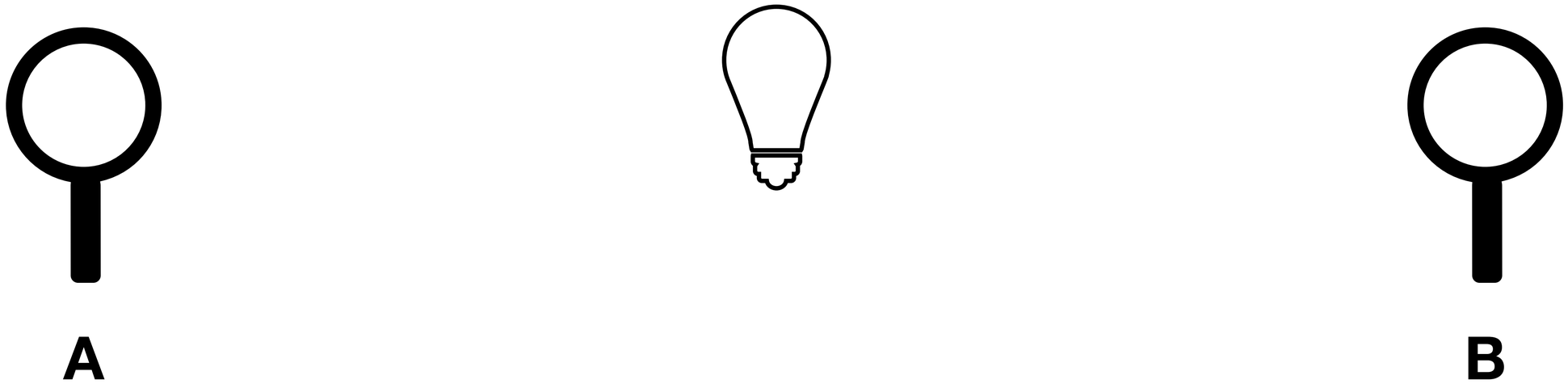
B

Bases: b_1, b_2

Results: ~~{0, 1}~~

{+1, -1}

Bell Test



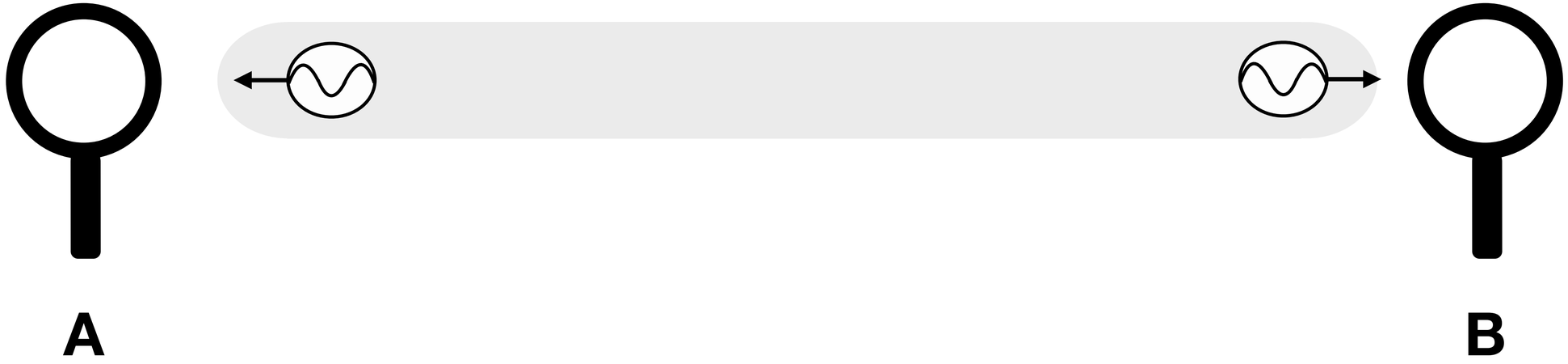
Bases: a_1, a_2

Results: {+1, -1}

Bases: b_1, b_2

Results: {+1, -1}

Bell Test



Bases: a_1, a_2

Results: {+1, -1}

Bases: b_1, b_2

Results: {+1, -1}

Bell Test

Bases: a_1, a_2

Results: {+1, -1}

Bases: b_1, b_2

Results: {+1, -1}

Bell Test

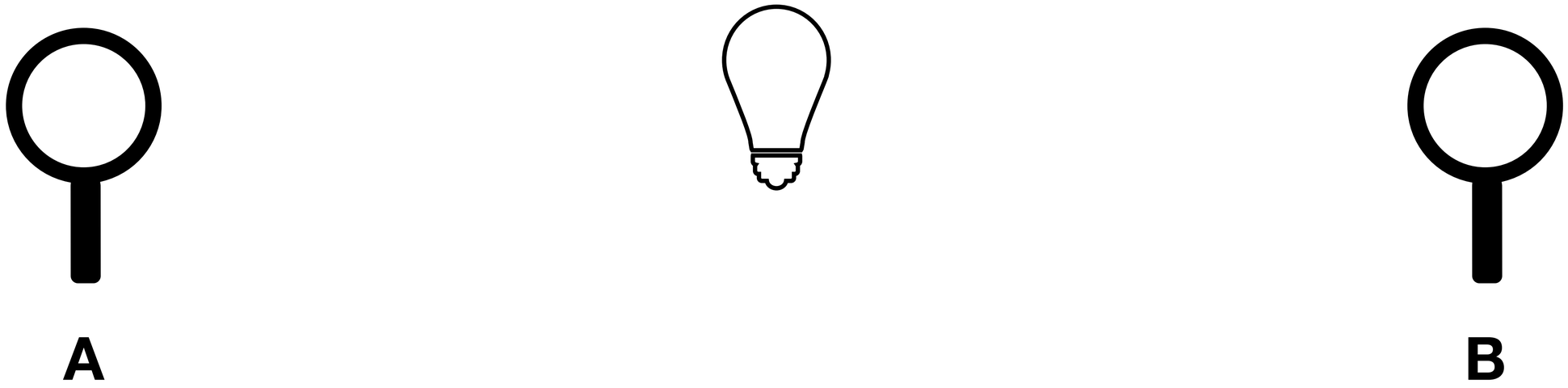
Bases: a_1, a_2

Results: {+1, -1}

Bases: b_1, b_2

Results: {+1, -1}

Bell Test



Bases: a_1, a_2

Results: {+1, -1}

Bases: b_1, b_2

Results: {+1, -1}

x **N**

CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

E_{a_i,b_j}	**Interpretation**
1	$a_i = b_j$ is always true
-1	$a_i = -b_j$ is always true
0	a_i and b_j are independant of each other

CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$S' = a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2$$

CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$\begin{aligned} S' &= a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2 \\ &= a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$S' = a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2$$
$$= a_1(b_1 - b_2) + a_2(b_1 + b_2)$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$S' = a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2$$
$$= a_1(b_1 - b_2) + a_2(b_1 + b_2)$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$S' = a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2$$
$$= a_1(b_1 - b_2) + a_2(b_1 + b_2)$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

$$|S'| \leq 2$$

CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$S' = a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2$$
$$= a_1(b_1 - b_2) + a_2(b_1 + b_2)$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

$$|S'| \leq 2$$

The results could be explained by hidden variables

CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$S' = a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2$$
$$= a_1(b_1 - b_2) + a_2(b_1 + b_2)$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

$$|S'| \leq 2$$

Classical

The results could be explained by hidden variables

CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classical} \end{cases}$$

CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classical} \\ \in \,]2, 2\sqrt{2}] & \text{With Bell Pairs!} \end{cases}$$

CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classical} \\ \in \,]2, 2\sqrt{2}] & \text{Quantum Maximum} \end{cases}$$

Computing the CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classical} \\ \in \,]2, 2\sqrt{2}] & \text{Quantum Maximum} \end{cases}$$

A		B		
Basis	Result	Basis	Result	$a_i \cdot b_j$
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_i,b_j} = \frac{1}{n} \sum_{k=0}^{n} a_i b_j$$

Computing the CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classical} \\ \in \,]2, 2\sqrt{2}] & \text{Quantum Maximum} \end{cases}$$

A		B		
Basis	Result	Basis	Result	$a_i \cdot b_j$
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1 - 1}{3} = 0$$

Computing the CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classical} \\ \in \,]2, 2\sqrt{2}] & \text{Quantum Maximum} \end{cases}$$

A		B		
Basis	Result	Basis	Result	$a_i \cdot b_j$
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1
a_2	+1	b_2	+1	+1

$$E_{a_1,b_1} = \frac{1-1+1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1-1}{3} = 0$$

$$E_{a_2,b_2} = \frac{1}{1} = 1$$

Computing the CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classical} \\ \in \,]2, 2\sqrt{2}] & \text{Quantum Maximum} \end{cases}$$

A		B		
Basis	**Result**	**Basis**	**Result**	$a_i \cdot b_j$
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1
a_2	+1	b_2	+1	+1

$$E_{a_1,b_1} = \frac{1-1+1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1-1}{3} = 0$$

$$E_{a_2,b_2} = \frac{1}{1} = 1$$

$$E_{a_1,b_2} = 0$$

Computing the CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classical} \\ \in \,]2, 2\sqrt{2}] & \text{Quantum Maximum} \end{cases}$$

A		B		
Basis	Result	Basis	Result	$a_i \cdot b_j$
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1
a_2	+1	b_2	+1	+1

$$E_{a_1,b_1} = \frac{1-1+1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1-1}{3} = 0$$

$$E_{a_2,b_2} = \frac{1}{1} = 1$$

$$E_{a_1,b_2} = 0$$

$$\boxed{S = 0.33 + 0 + 1 - 0 = 1.33 \leq 2}$$

Computing the CHSH Inequality

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classical} \\ \in \,]2, 2\sqrt{2}] & \text{Quantum Maximum} \end{cases}$$

A		B		
Basis	Result	Basis	Result	$a_i \cdot b_j$
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1
a_2	+1	b_2	+1	+1

$$E_{a_1,b_1} = \frac{1-1+1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1-1}{3} = 0$$

$$E_{a_2,b_2} = \frac{1}{1} = 1$$

$$E_{a_1,b_2} = 0$$

$$\boxed{S = 0.33 + 0 + 1 - 0 = 1.33 \leq 2}$$

Not enough measurements
to draw a conclusion!

BREAK

Back at

00:00

INSTITUT QUANTIQUE UdS

USHERBROOKE.CA/IQ

Plan

- ✓ Presentation
- ✓ Cryptography
- ✓ The qubit
- ✓ The photon: messenger of quantum information
- Entanglement and CHSH inequality
- Protocol E91
- Hands-on session

Plan

- ✓ Presentation
- ✓ Cryptography
- ✓ The qubit
- ✓ The photon: messenger of quantum information
- ✓ Entanglement and CHSH inequality
- ○ Protocol E91
- ○ Hands-on session

Plan

- ✓ Presentation
- ✓ Cryptography
- ✓ The qubit
- ✓ The photon: messenger of quantum information
- ✓ Entanglement and CHSH inequality
- ○ Protocol E91
- ○ Hands-on session

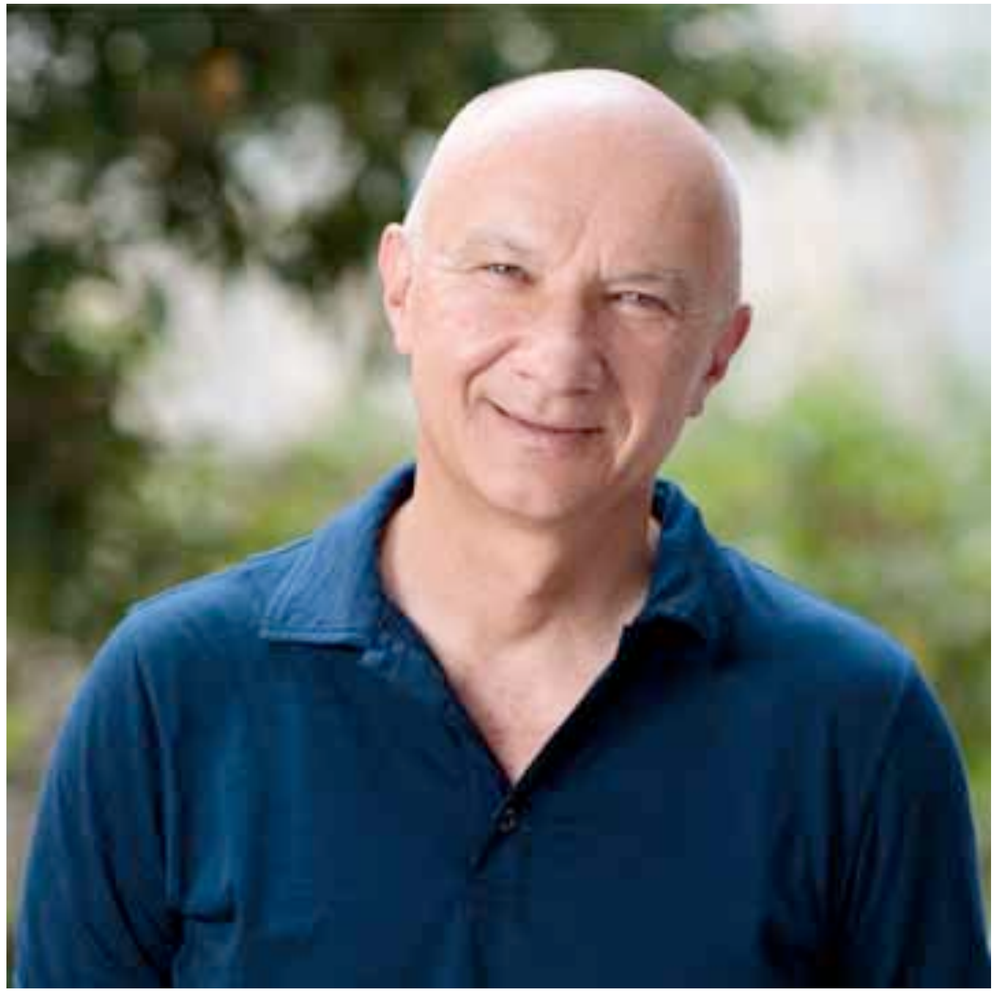
Protocol E91

Created by **Artur Ekert** in **1991**

Quantum Symmetric Key Distribution Protocol

Perfect theoretical security

ensured by:



https://www.cqt.sg/groups/artur-ekert/

Protocol E91

Created by **Artur Ekert** in **1991**

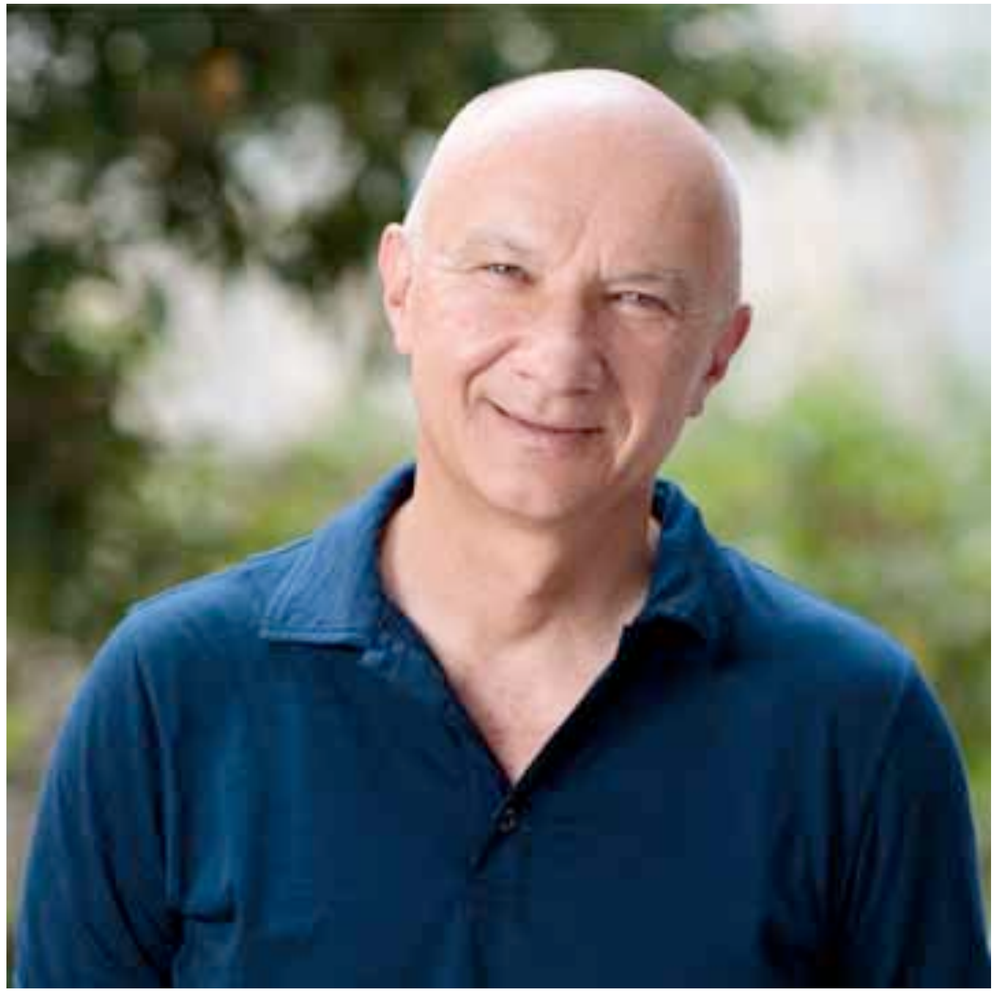
Quantum Symmetric Key Distribution Protocol

Perfect theoretical security

ensured by:

Quantum Measurement

Distribution of the symmetric key



https://www.cqt.sg/groups/artur-ekert/

Protocol E91

Created by **Artur Ekert** in **1991**

Quantum Symmetric Key Distribution Protocol

Perfect theoretical security

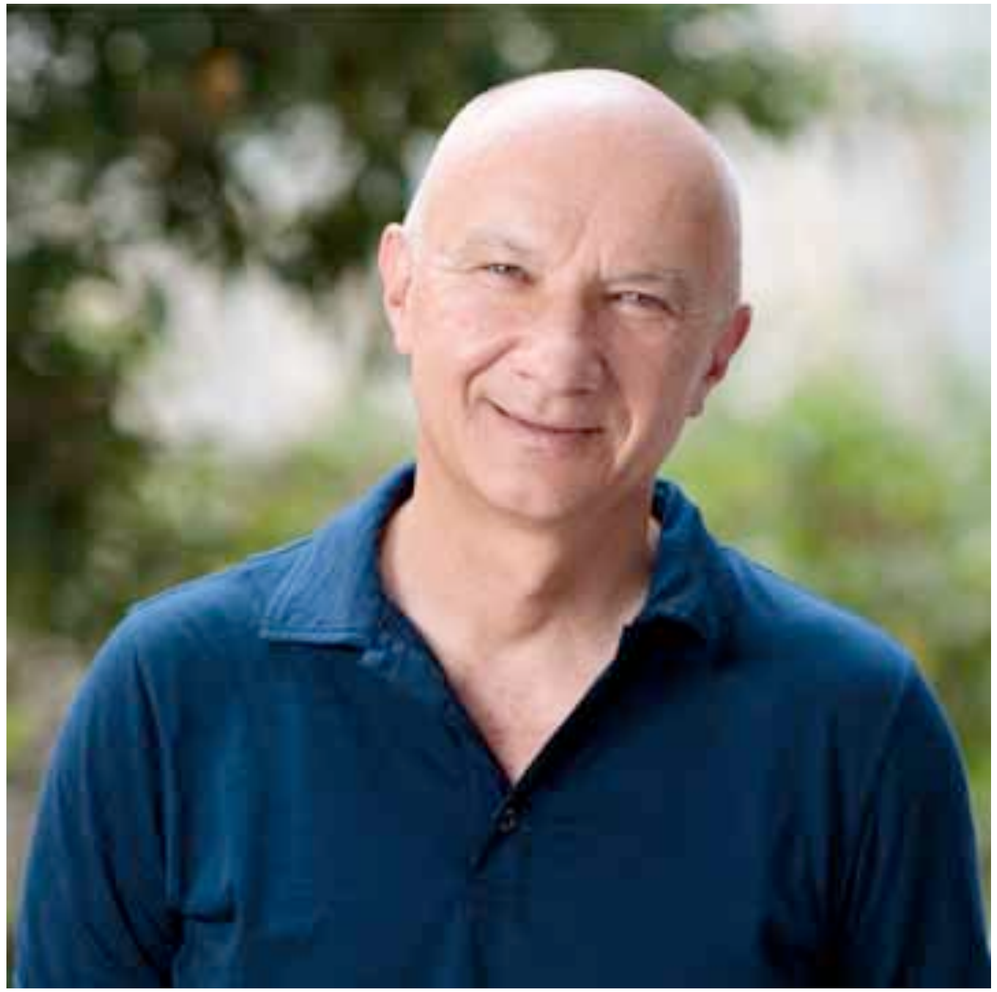
ensured by:

Quantum Measurement

Distribution of the symmetric key

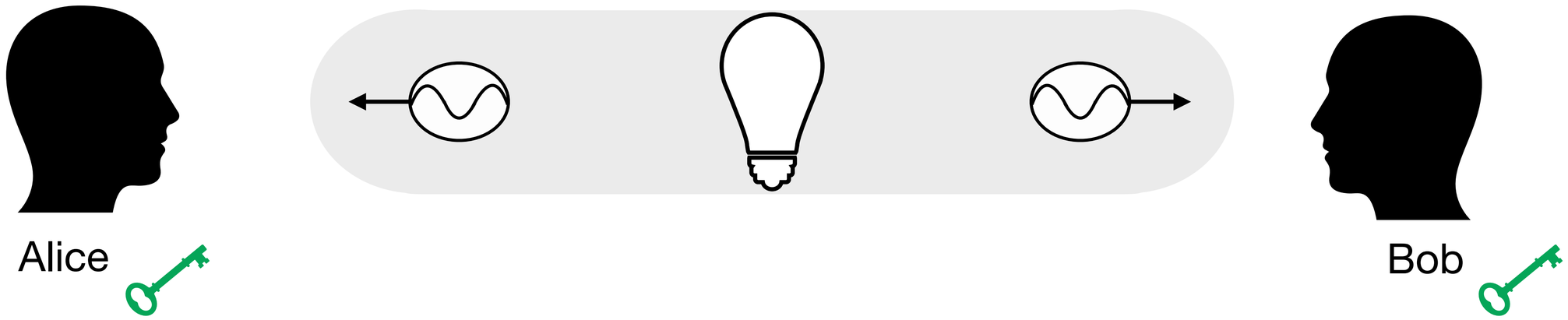
Entanglement and CHSH Inequality

Spy detection



https://www.cqt.sg/groups/artur-ekert/

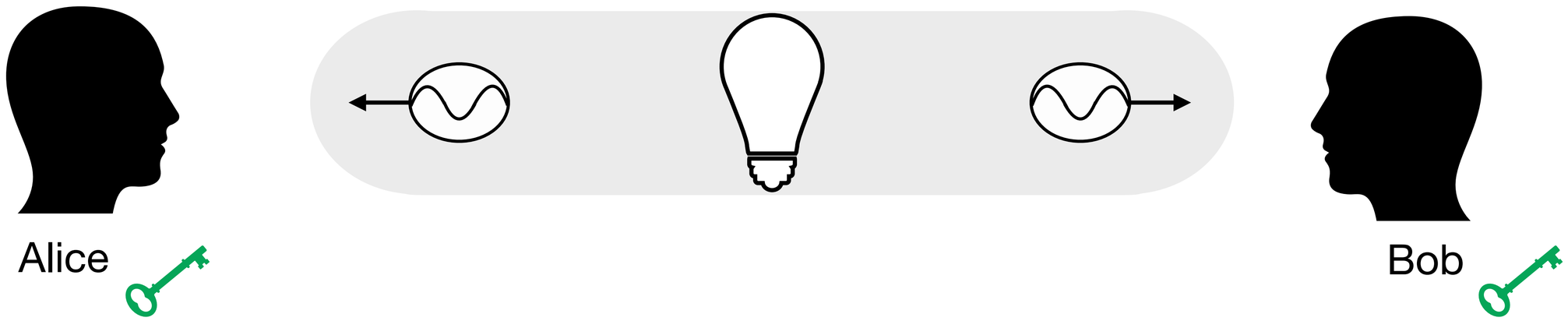
Protocol steps



Goal

Establish a secret symmetric key between Alice and Bob

Protocol steps

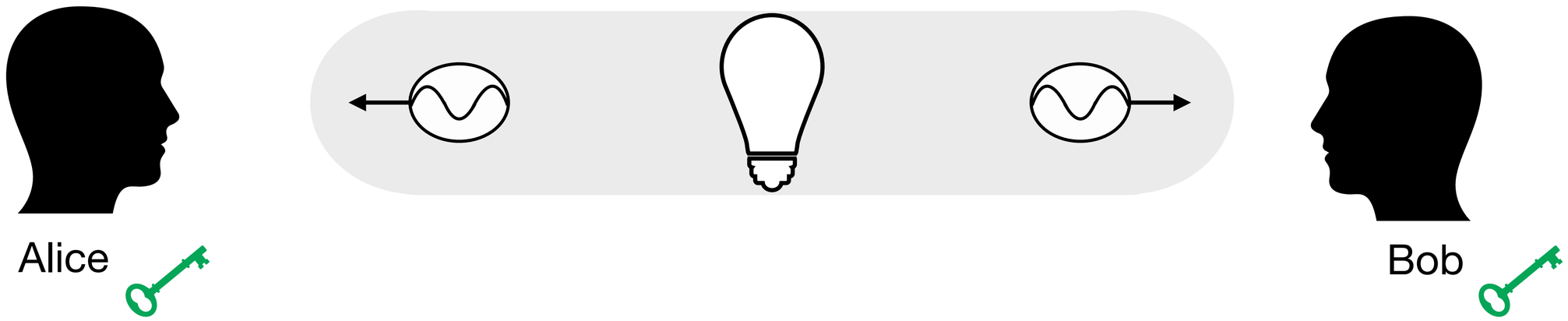


Goal

Establish a secret symmetric key between Alice and Bob

1. Reception of the entangled photons

Protocol steps

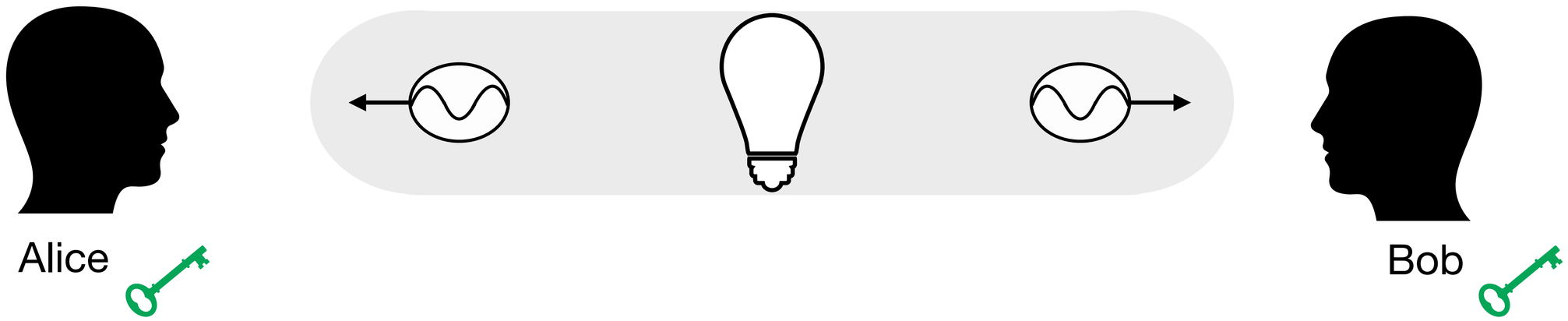


Goal

Establish a secret symmetric key between Alice and Bob

1. Reception of the entangled photons
2. Announcement of the bases

Protocol steps



Goal

Establish a secret symmetric key between Alice and Bob

1. Reception of the entangled photons
2. Announcement of the bases
3. Spy/Error Detection

Step 1: Reception of the entangled photons

Alice and Bob each receive one photon of an entangled pair

Alice

(0°, 45°, 90°)

Bob

(45°, 90°, 135°)

Step 1: Reception of the entangled photons

Alice and Bob each receive one photon of an entangled pair

Alice

(0°, 45°, 90°)

Bob

(45°, 90°, 135°)

Choose a basis randomly

0°

90°

Step 1: Reception of the entangled photons

Alice and Bob each receive one photon of an entangled pair

Alice

(0°, 45°, 90°)

Bob

(45°, 90°, 135°)

Choose a basis randomly

0°

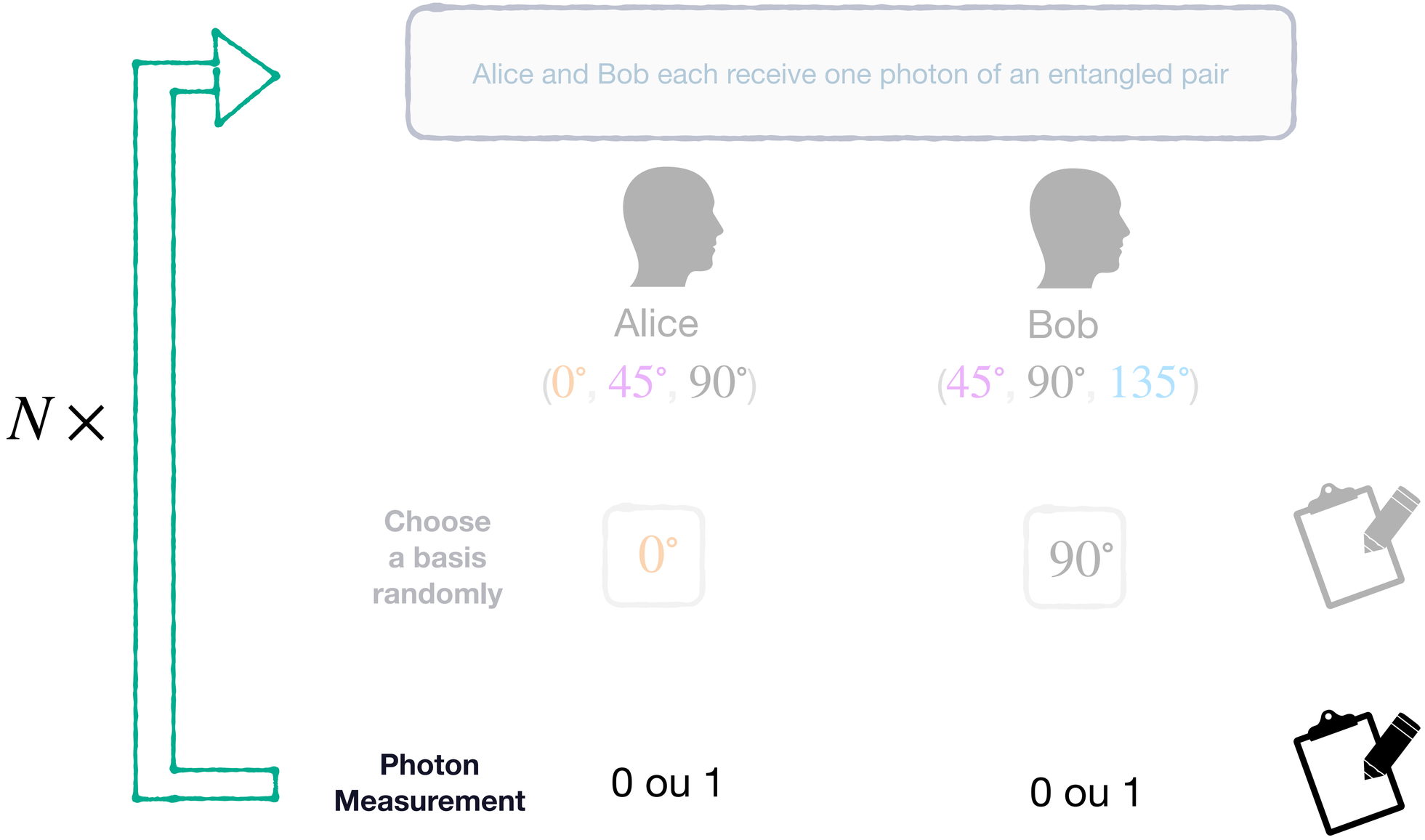
90°

Photon Measurement

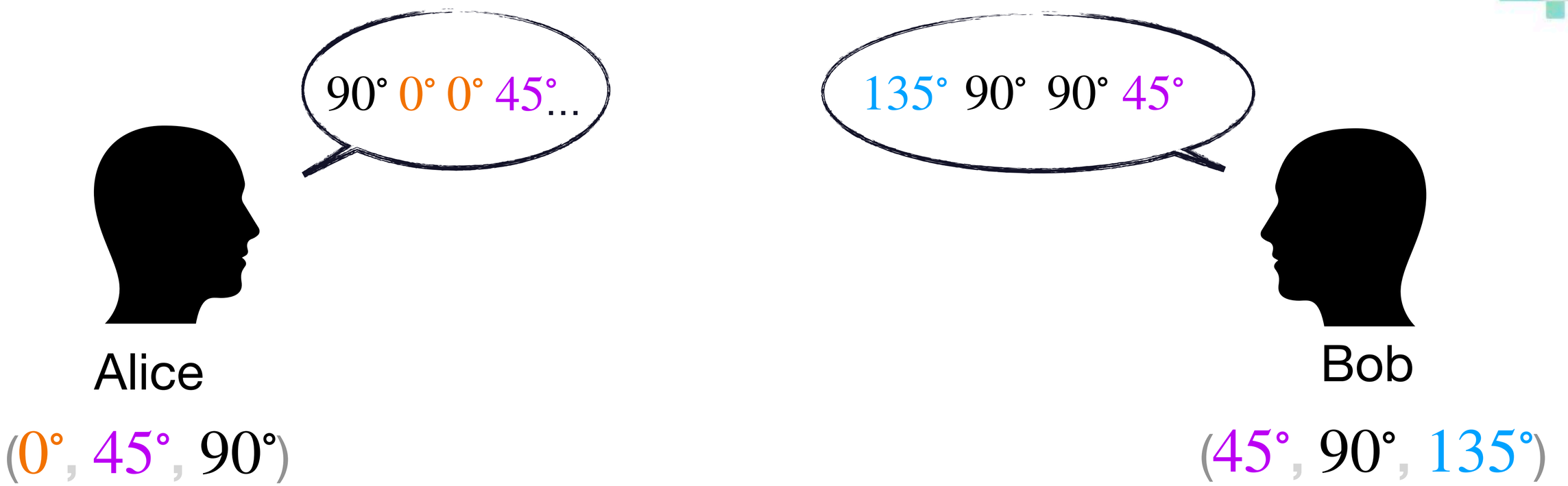
0 ou 1

0 ou 1

Step 1: Reception of the entangled photons



Step 2: Announcement of the bases



Step 2: Announcement of the bases

(0°, 45°, 90°)

(45°, 90°, 135°)

9 combinations

(0°, 45°) (0°, 90°) (0°, 135°) (45°, 45°) (45°, 90°) (45°, 135°) (90°, 45°) (90°, 90°) (90°, 135°)

Step 2: Announcement of the bases

Creation of the symmetric key

Alice	Bob
45°	45°
90°	90°

Step 2: Announcement of the bases

Creation of the symmetric key

Alice	Bob
45°	45°
90°	90°

Spy Detection

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

Step 2: Announcement of the bases

Creation of the symmetric key

Alice	Bob
45°	45°
90°	90°

Spy Detection

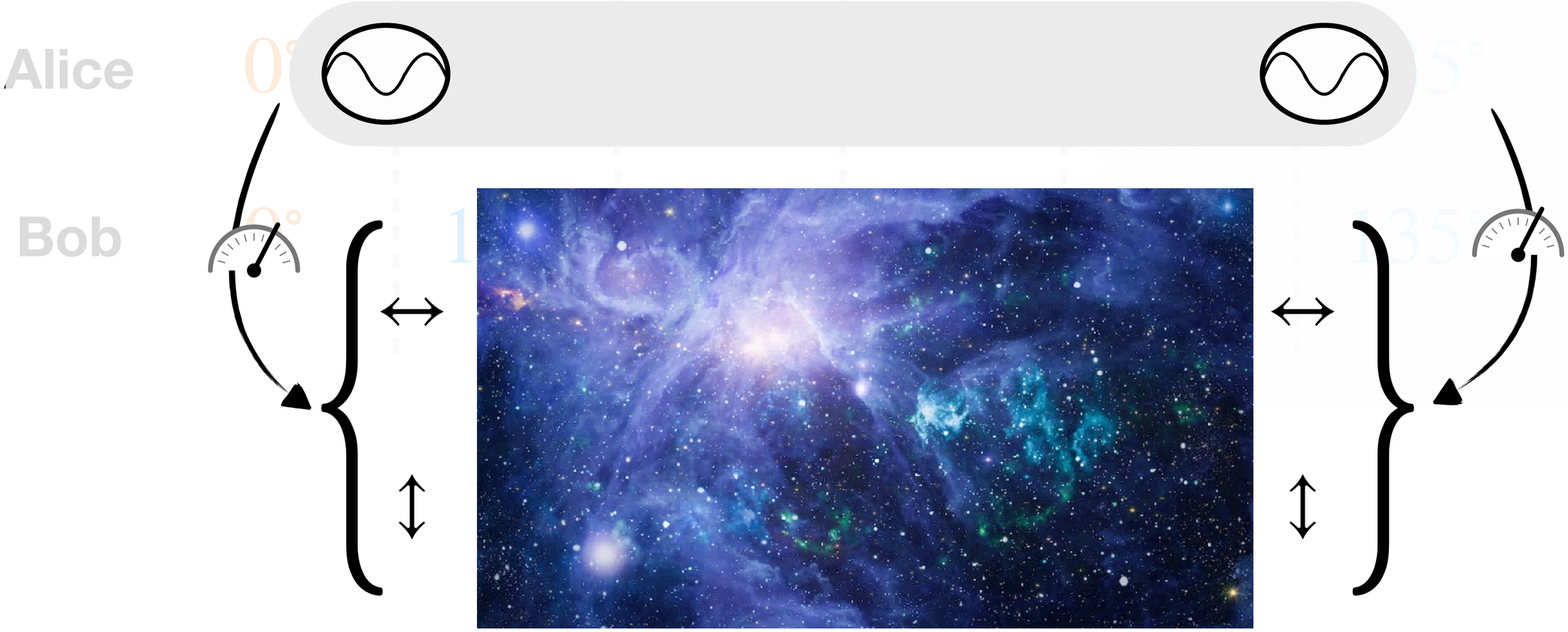
Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

Generating the symmetric key

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
Alice	0°	135°	0°	45°	90°	135°	90°
Bob	0°	135°	0°	45°	90°	135°	90°

Generating the symmetric key

$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle+\frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$



© Shutterstock

Generating the symmetric key

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
Alice	0°	135°	0°	45°	90°	135°	90°
Bob	0°	135°	0°	45°	90°	135°	90°

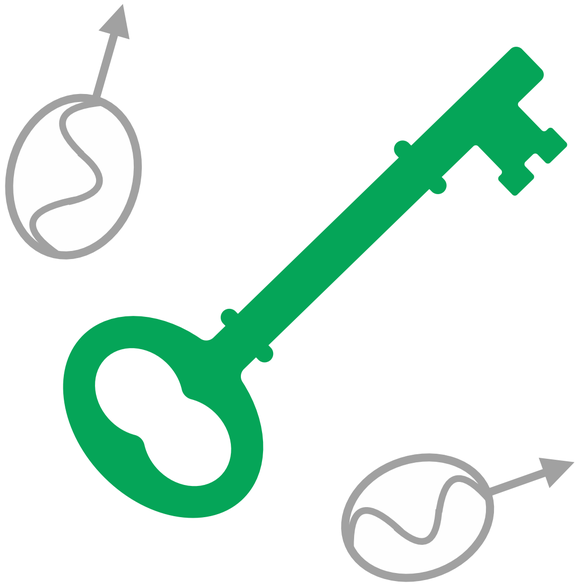
Generating the symmetric key

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
Alice	0°	135°	0°	45°	90°	135°	90°
Bob	0°	135°	0°	45°	90°	135°	90°
	1	1	0	0	1	0	0

Properties of the quantum symmetric key

Binary

The quantum measurement results are labeled 0 or 1.



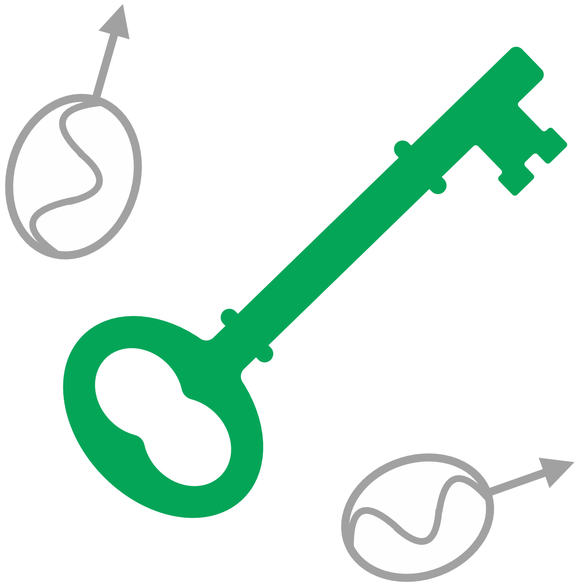
Properties of the quantum symmetric key

Binary

The quantum measurement results are labeled 0 or 1.

Identical

Measuring the photons of an entangled pair in the same basis, guarantees the same measurement result for Alice and Bob.



Properties of the quantum symmetric key

Binary

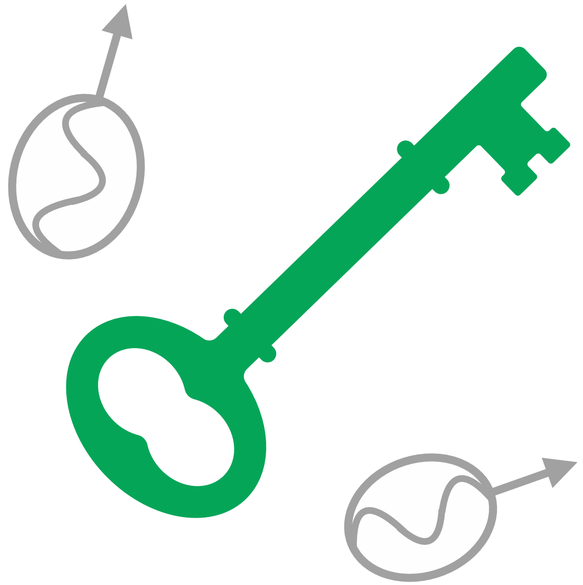
The quantum measurement results are labeled 0 or 1.

Identical

Measuring the photons of an entangled pair in the same basis, guarantees the same measurement result for Alice and Bob.

Truly Random

La mesure quantique d’une paire intriquée garantie l’aléatoire.



Creation of the symmetric key

Alice	Bob
45°	45°
90°	90°

Spy Detection

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

Creation of the symmetric key

Alice	Bob
45°	45°
90°	90°

Spy Detection

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

Step 3: Spy/Error Detection

Creation of the symmetric key

Alice	Bob
45°	45°
90°	90°

Spy Detection

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

Step 3: Spy/Error Detection

Bases combinations used: (0°, 45°) (0°, 135°) (90°, 45°) (90°, 135°)

Alice { 0°, 90° }

Bob { 45°, 135° }

Step 3: Spy/Error Detection

Bases combinations used: (0°, 45°) (0°, 135°) (90°, 45°) (90°, 135°)

Alice { 0°, 90° } { a_1, a_2 }

Bob { 45°, 135° } { b_1, b_2 }

Step 3: Spy/Error Detection

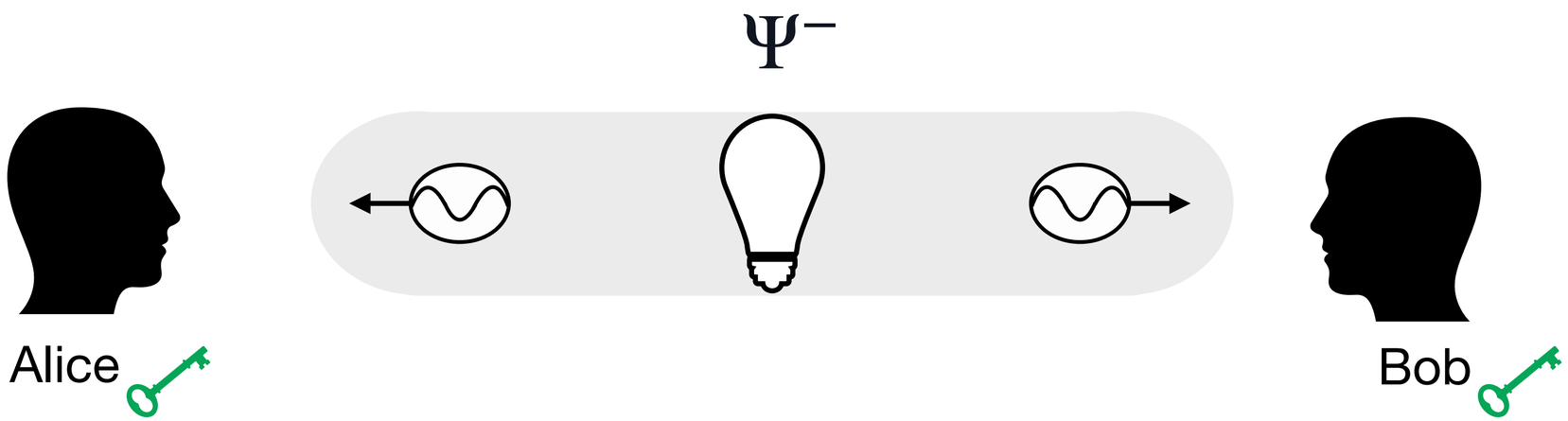
Bases combinations used: $(0°, 45°)$ $(0°, 135°)$ $(90°, 45°)$ $(90°, 135°)$

Alice $\{0°, 90°\}$ $\{a_1, a_2\}$

Bob $\{45°, 135°\}$ $\{b_1, b_2\}$

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classical} \\ \in \,]2, 2\sqrt{2}] & \text{Quantum maximum} \end{cases}$$

Case 1: Using Bell Pairs



$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classical} \\ \in \,]2, 2\sqrt{2}] & \text{Quantum maximum} \end{cases}$$

Case 2: Eve spies on the conversation

Case 2: Eve spies on the conversation

Choice of Basis

45°

135°

90°

Case 2: Eve spies on the conversation

Choice of Basis	Measurement Result
45°	{0 ,1}
135°	{0 ,1}
90°	{0 ,1}

Case 2: Eve spies on the conversation

Choice of Basis	Measurement Result	Encoding
45°	{0 ,1}	{ $\lvert\nwarrow\rangle$, $\lvert\nearrow\rangle$ }
135°	{0 ,1}	{ $\lvert\nwarrow\rangle$, $\lvert\nearrow\rangle$ }
90°	{0 ,1}	{ $\lvert\leftrightarrow\rangle$, $\lvert\updownarrow\rangle$ }

Case 2: Eve spies on the conversation

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classical} \\ \in \,]2, 2\sqrt{2}] & \text{Quantum Maximum} \end{cases}$$

Case 2: Eve spies on the conversation

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classical} \\ \in \,]2, 2\sqrt{2}] & \text{Quantum Maximum} \end{cases}$$

Number of Measurements

Creation of the symmetric key

Alice	Bob
45°	45°
90°	90°

Spy Detection

Alice	Bob	
0°	45°	✓
0°	90°	
0°	135°	✓
45°	90°	
45°	135°	
90°	45°	✓
90°	135°	✓

Number of Measurements

Creation of the symmetric key

Alice	Bob
45°	45°
90°	90°

Spy Detection

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

$\frac{2}{9}$ ~ 22% Generating the symmetric key

Keypoints

Key length

Number of Measurements

Creation of the symmetric key

Alice	Bob
45°	45°
90°	90°

Spy Detection

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

$\frac{2}{9}$ ~ 22% Generating the symmetric key

$\frac{4}{9}$ ~ 45% Spy detection

Keypoints

Key length

Security of the key

Number of Measurements

Creation of the symmetric key

Alice	Bob
45°	45°
90°	90°

Spy Detection

Alice	Bob	
0°	45°	✓
0°	90°	
0°	135°	✓
45°	90°	
45°	135°	
90°	45°	✓
90°	135°	✓

$\frac{2}{9}$ ~ 22% Generating the symmetric key

$\frac{4}{9}$ ~ 45% Spy detection

$\frac{3}{9}$ ~ 33% Thrown away

Keypoints

Key length

Security of the key

Plan

- ✓ Presentation
- ✓ Cryptography
- ✓ The qubit
- ✓ The photon: messenger of quantum information
- ✓ Entanglement and CHSH inequality
- ○ Protocol E91
- ○ Hands-on session

Plan

- ✓ Presentation
- ✓ Cryptography
- ✓ The qubit
- ✓ The photon: messenger of quantum information
- ✓ Entanglement and CHSH inequality
- ✓ Protocol E91
- ○ Hands-on session

Plan

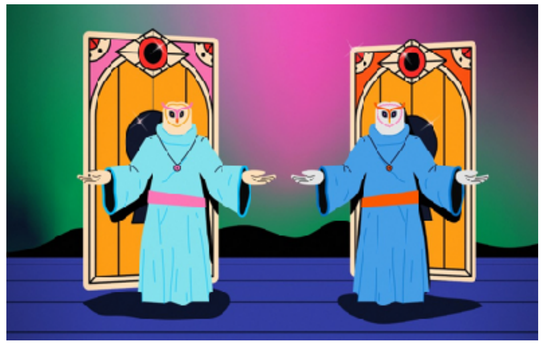
- ✓ Presentation
- ✓ Cryptography
- ✓ The qubit
- ✓ The photon: messenger of quantum information
- ✓ Entanglement and CHSH inequality
- ✓ Protocol E91
- ○ Hands-on session

Hands-On Session

https://github.com/algolab-quantique/CMAI-E91-Students.git

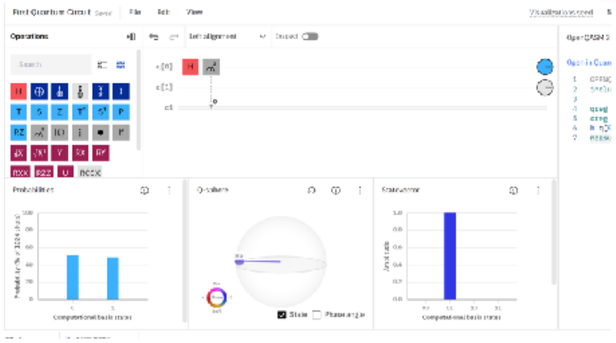
Conclusion

References

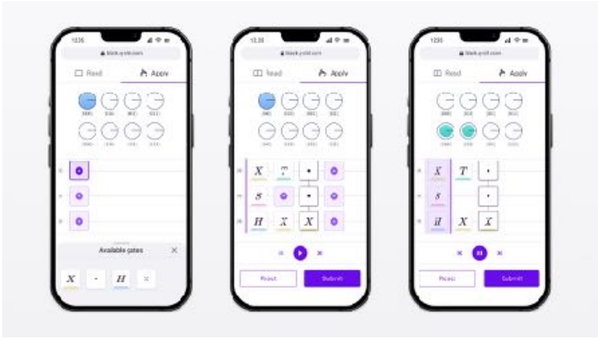


Quantum Enigmas (link)

SkillsBuild (lien)



IBM Quantum learning (lien)



Black Opal de Q-CTRL (lien)

Azure Quantum katas (lien)

Subscribe to the newsletter!

Link to the Assignment

https://forms.office.com/r/LshFpNT8nE?origin=lprLink

You have 24 hours to complete the assignment.

INSTITUT QUANTIQUE UdS

INSTITUT POUR LA MOBILITÉ ET L'AÉROSPATIALE AU CANADA