Quantum Computation & Cryptography
Day 1

Introduction

Andru Gheorghiu

About me

- I'm a theoretical computer scientist
- Postdoctoral researcher at Caltech
- Completed PhD, MSc at University of Edinburgh
- BSc at UPB, Automatica si Calculatoare

Feel free to ask me questions

gheorghiuandru@gmail.com

About the workshop

- Not a course
- Not a *formal* introduction into quantum information
- … but there will be maths!
- Intention is to convey the general ideas and principles

Quantum computation

Crypto quantum post-quantum

Physics

Schedule

1. Monday, 20 Aug
    - **Introduction**: A brief history of quantum computation and quantum cryptography, what makes them interesting and the current state of the art.
    - **What's quantum about quantum computing?**: A simple explanation of what makes quantum special and why quantum algorithms could outperform classical algorithms at certain tasks.
2. Tuesday, 21 Aug
    - **How to make a physical theory 101**: We'll discuss the core elements that characterize a physical theory, how these apply to quantum mechanics and how this takes us to quantum information.
    - **Quantum information basics**: Qubits and quantum gates and how to use them to make quantum algorithms. We'll also look at a simple quantum computation on the IBM quantum chip.
3. Wednesday 22 Aug
    - **Quantum algorithms**: Continuing with algorithms, we'll look at the quantum algorithms of Simon and Shor.
    - **Post-quantum cryptography**: Given that Shor's algorithm compromises the security of many public-key crypto protocols, we'll discuss a potential fix, namely post-quantum cryptography.
4. Thursday, 23 Aug
    - **Quantum cryptography**: An introduction to quantum cryptography and the BB84 quantum key distribution protocol.
    - **Entanglement and device-independence**: We'll see how quantum entanglement allows us to have secure protocols even in the presence of untrusted quantum devices, or so-called device-independent protocols.
5. Friday, 24 Aug
    - **Quantum hardware**: How do we physically realize qubits and quantum gates? A look at the basics of quantum hardware.
    - **Fault tolerance and the future**: We end by discussing how quantum devices can cope with noise and imperfections as well as discuss the outlook for future implementations.

Romanian Quantum Network

https://roqnet.ro/about/

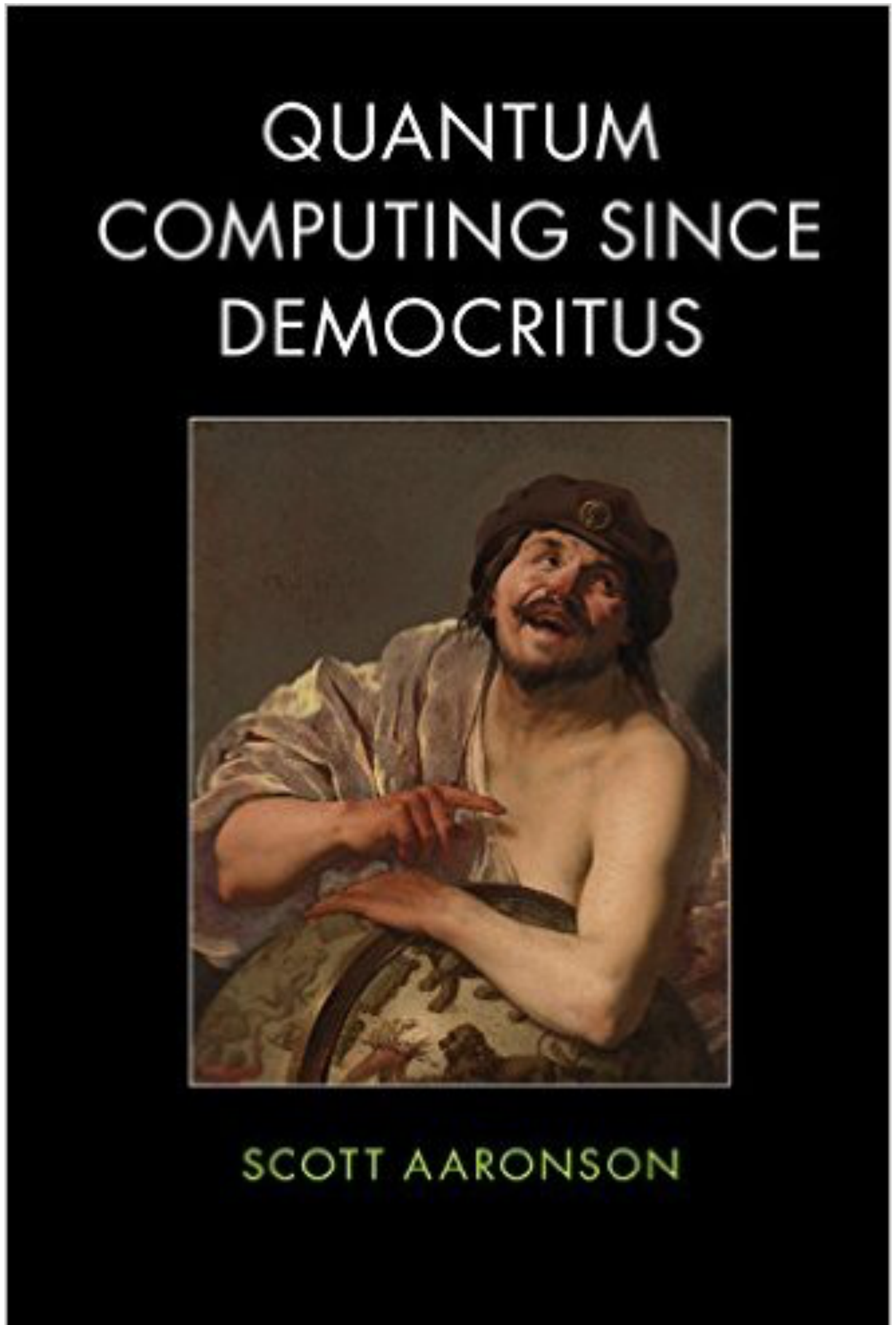
Dezvoltarea informatiei cuantice si a tehnologiilor cuantice in Romania

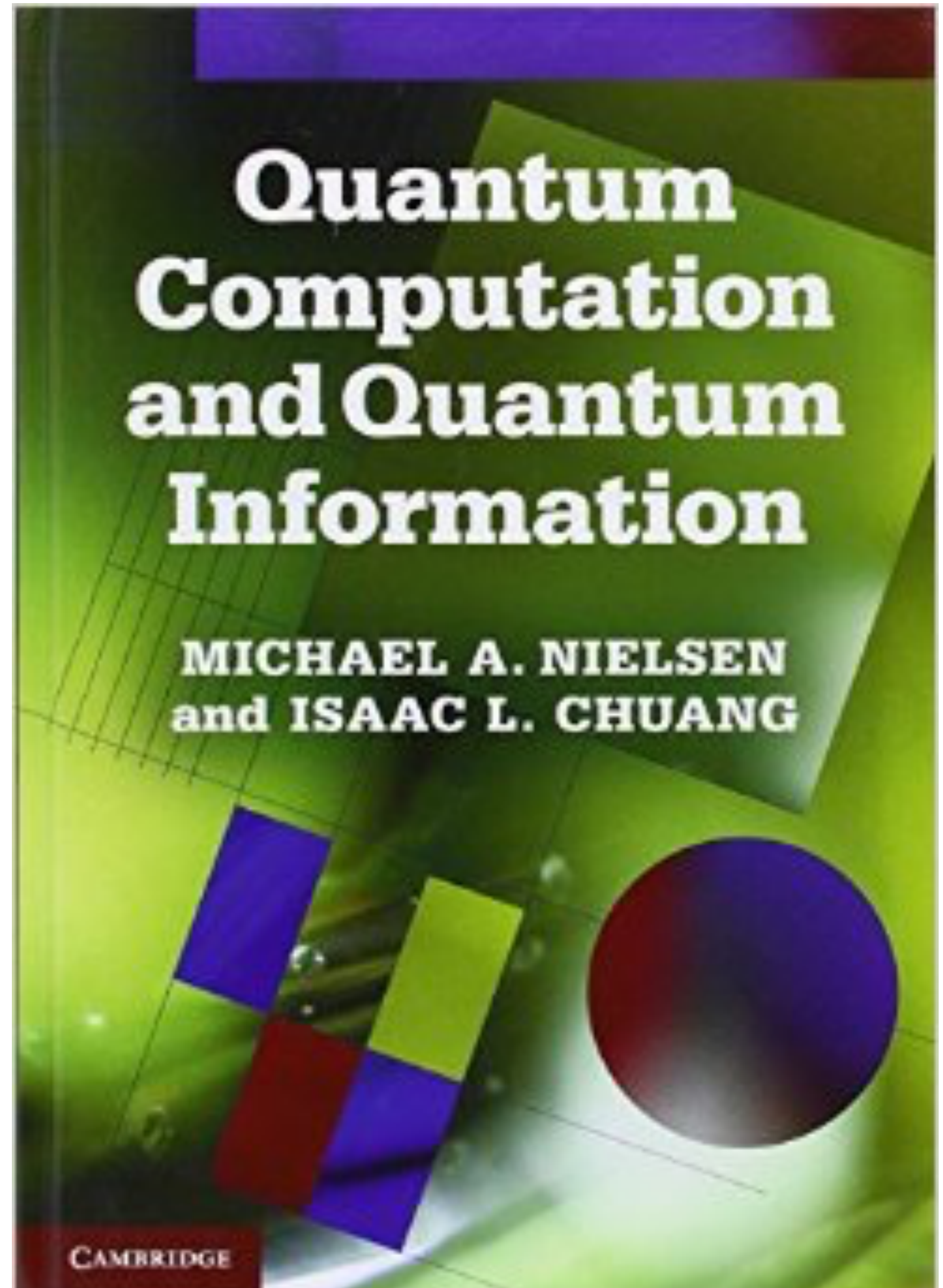
1. Metode teoretice si computationale pentru informatie cuantica
2. Dispozitive optice integrate pentru tehnologii cuantice fabricate prin litografie 3D
3. Informatie cuantica cu vortexuri optice
4. Laboratoare de cercetare pentru tehnologii cuantice
5. Calcul cuantic cu fermioni Majorana

Dr. Radu Ionicioiu
r.ionicioiu@theory.nipne.ro

Dr. Mona Mihailescu
mona.mihailescu@physics.pub.ro

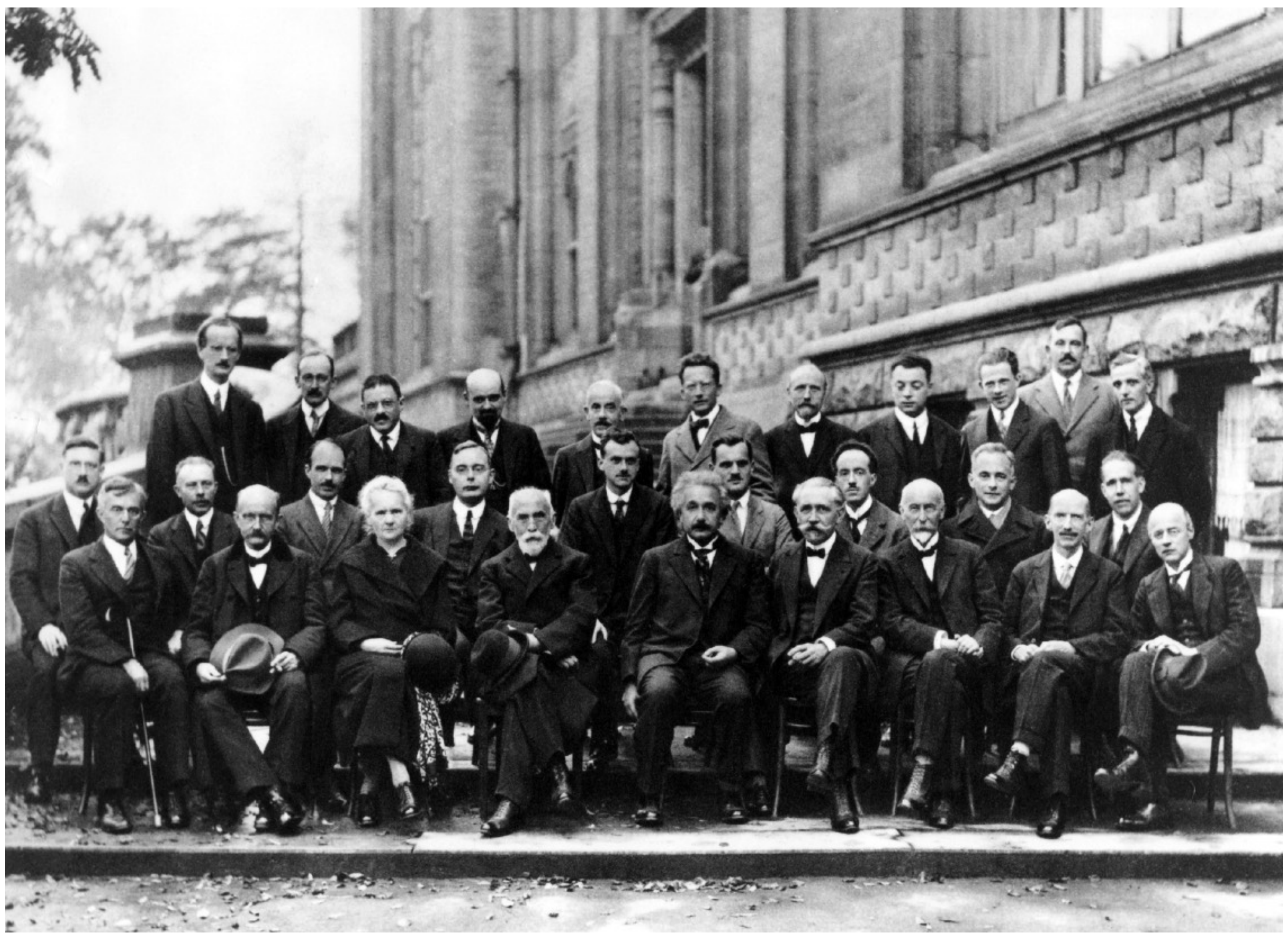
Recommended reading



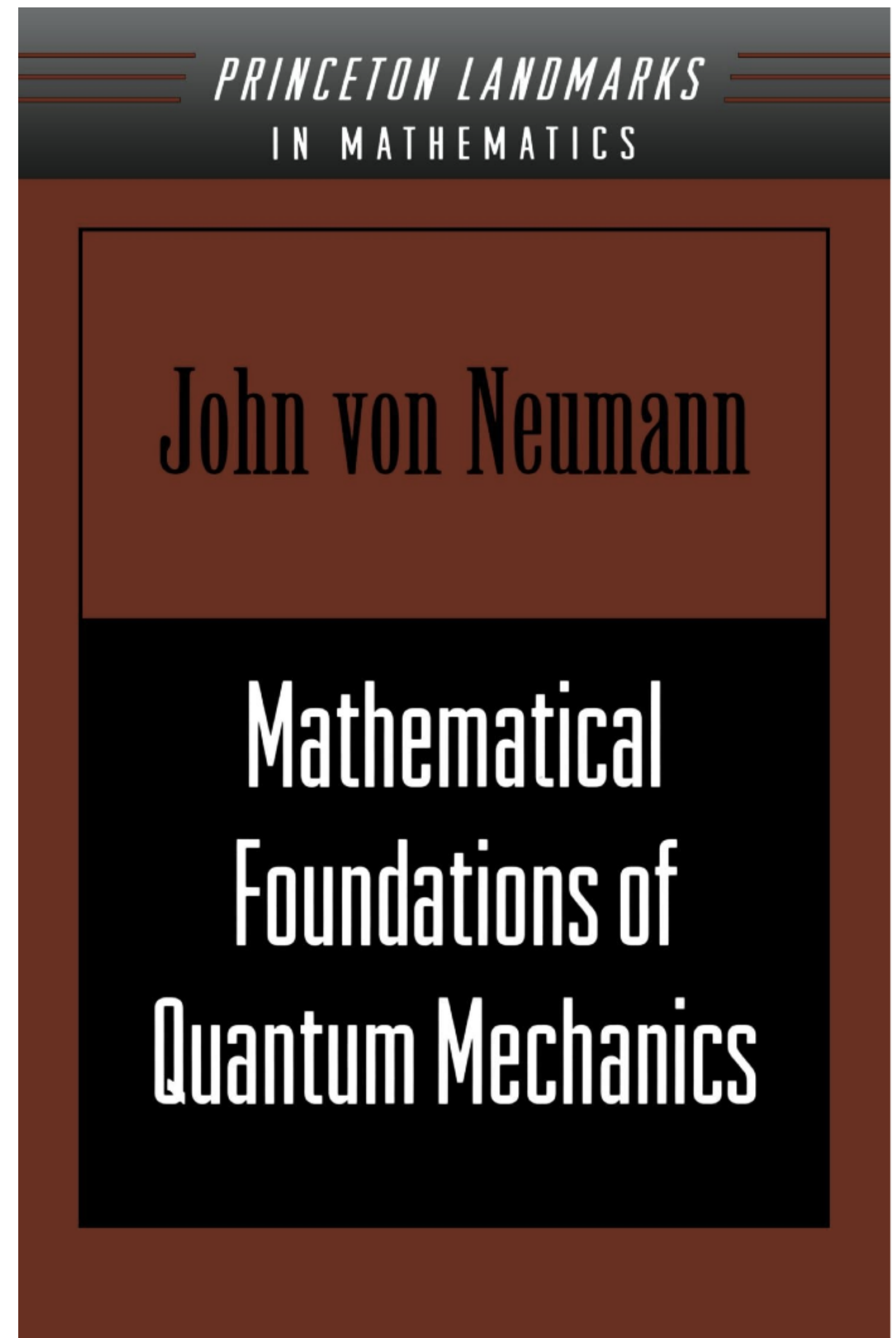


Quantum mechanics

Inception of QM **1900-1932**



Solvay conference 1927



Quantum mechanics

- Best model we have for small scales, high energies
- Semiconductors, lasers, NMR, superconductors etc
- Quantum mechanics is a **framework** for physics

Quantum physics → Particles, fields, hamiltonians, spin, polarisation

Quantum mechanics → Vector spaces, linear operators, hermitian operators, probability

"*Quantum mechanics is remarkably simple, once you take all the physics out of it*"
Scott Aaronson

Classical vs. quantum

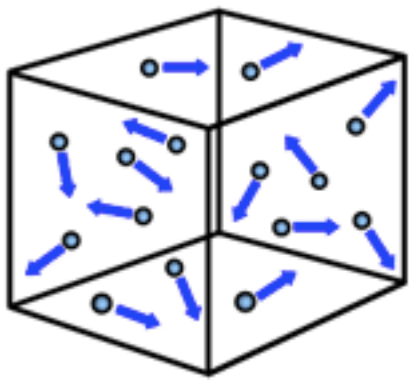
Simulating physics with computers - **1981**

"What kind of computer are we going to use to simulate physics?"

Simulating quantum systems

Classical vs. quantum

Classical



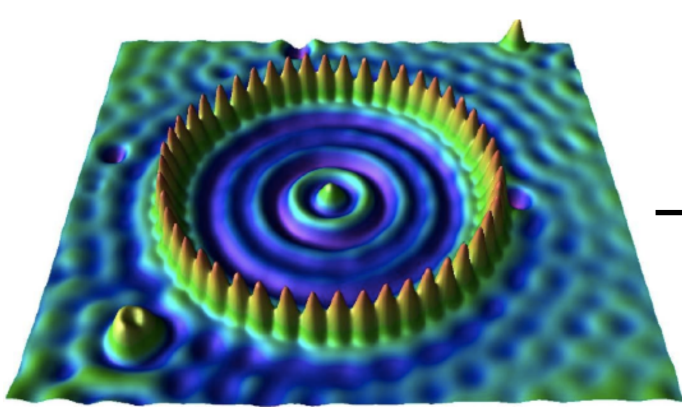
State →

$$(x_1, y_1, z_1), (x_2, y_2, z_2), \ldots (x_N, y_N, z_N)$$
$$(p_{x_1}, p_{y_1}, p_{z_1}), (p_{x_2}, p_{y_2}, p_{z_2}), \ldots (p_{x_N}, p_{y_N}, p_{z_N})$$

N particles

$O(N)$ variables

Quantum



State →

$$|\psi\rangle = \begin{pmatrix} \psi_0 \\ \psi_1 \\ \psi_2 \\ \ldots \\ \psi_{2^{O(N)}} \end{pmatrix}$$

$2^{O(N)}$ variables

N particles

Classical vs. quantum

Simulating physics with computers - **1981**

"What kind of computer are we going to use to simulate physics?"

Simulating quantum systems

Inefficient classically

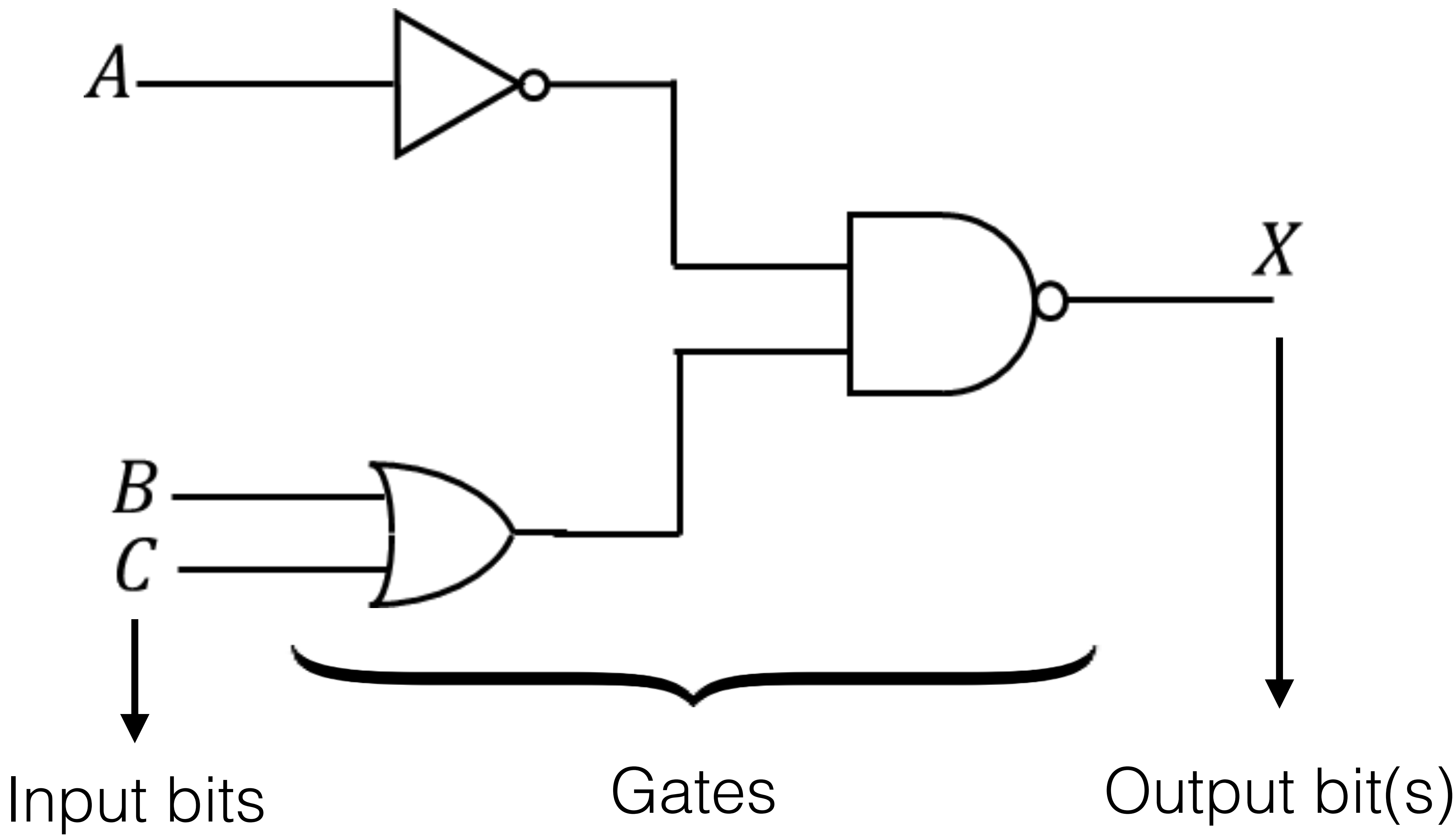
"Can you do it with a new kind of computer - a quantum computer?"

"I believe that with a suitable class of quantum machines you could imitate any quantum system, including the physical world"

A brief history of quantum computing

- **1980s** - Idea of quantum computation. Benioff, Manin, Feynman, Deutsch.
- **1990s** - Theory of efficient quantum simulation. Lloyd.
- **1994** - Efficient quantum algorithm for factoring and discrete log (breaking RSA, Diffie-Hellman, ECC, etc). Shor.
- **2000s** - Many small scale experiments; quantum complexity theory; quantum machine learning.
- **2010s** - Quantum supremacy? Small scale devices (IBM, Rigetti, Google).

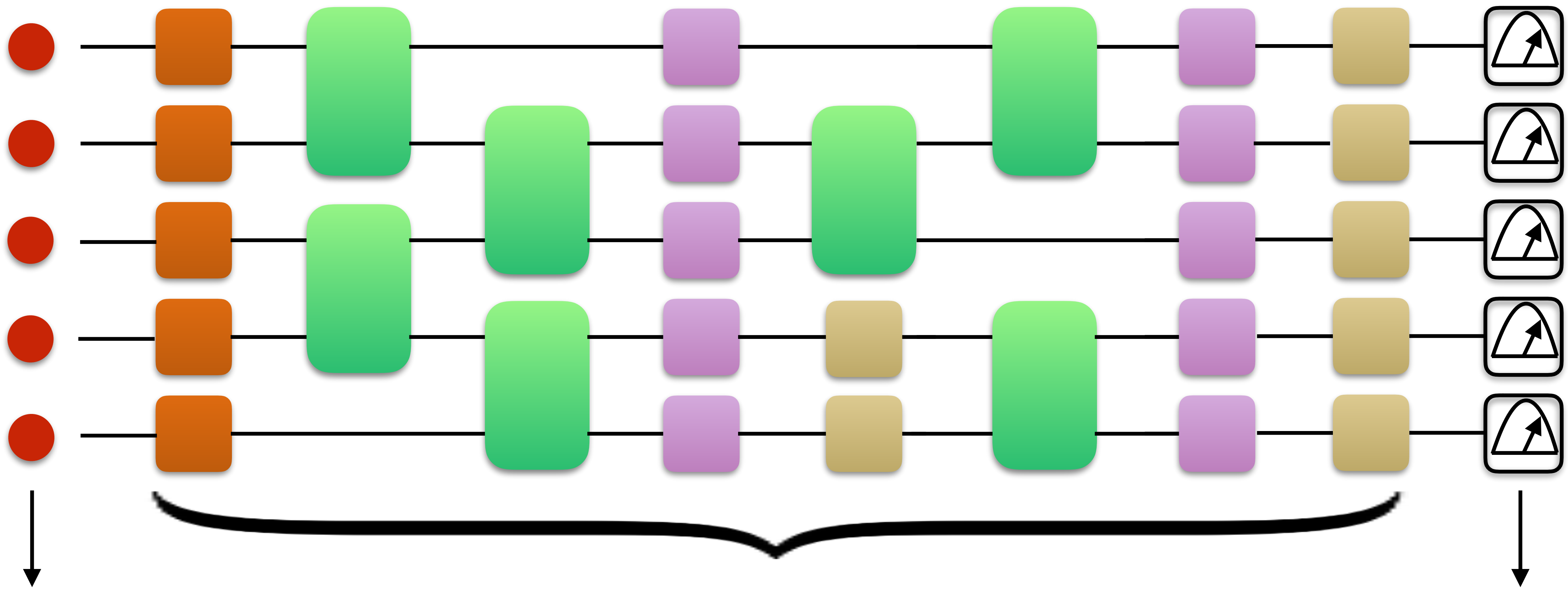
A new kind of computer…



$$X = NAND(OR(B,C), NOT(A))$$

Boolean functions

A new kind of computer...



Qubits

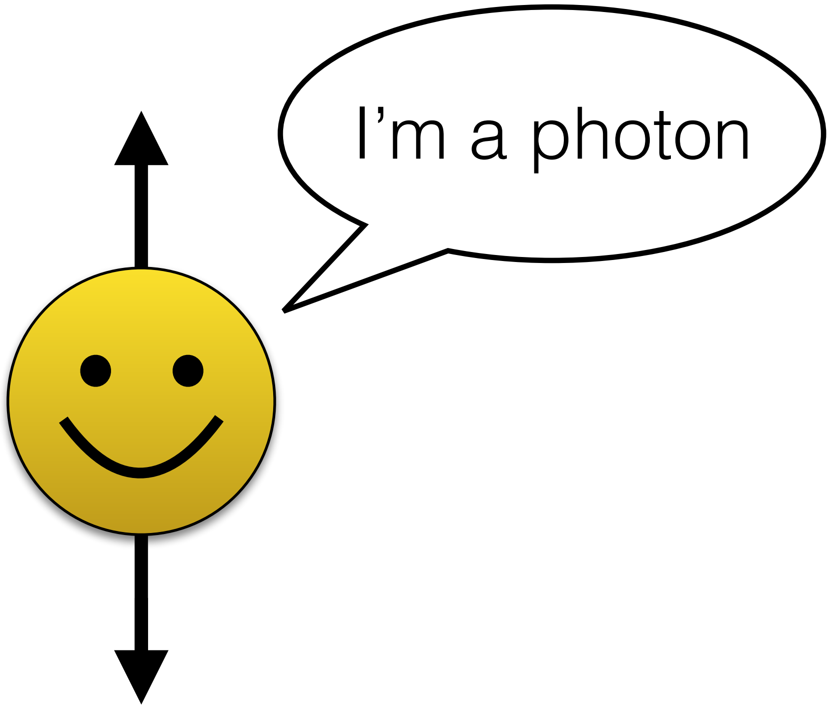
Quantum gates

Measurement

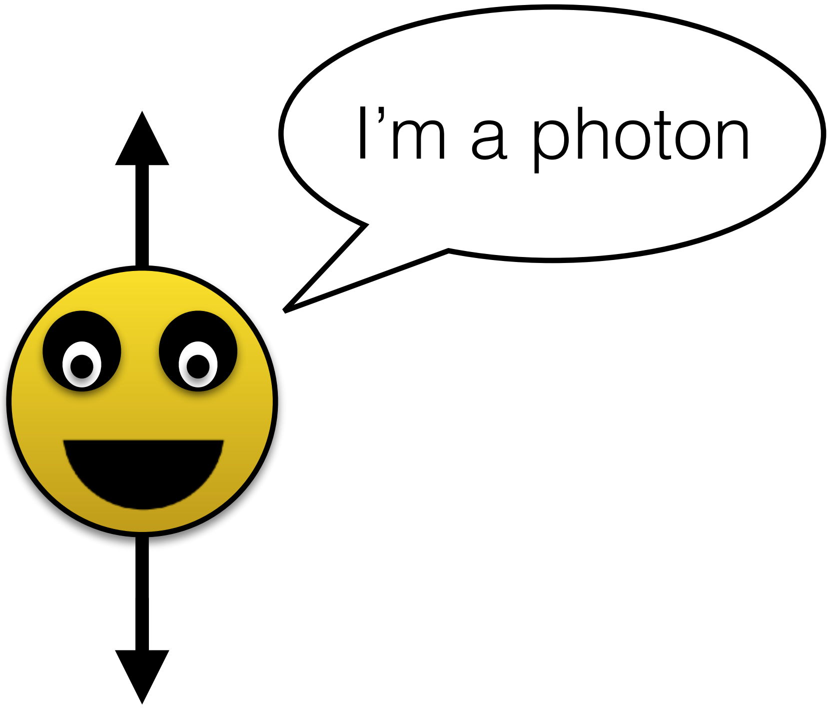
$$\begin{pmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{2^N-1} \end{pmatrix} \qquad \begin{pmatrix} \mathcal{C}_{0,0} & \cdots & \mathcal{C}_{0,2^N-1} \\ \mathcal{C}_{1,0} & \cdots & \mathcal{C}_{1,2^N-1} \\ \vdots & & \vdots \\ \mathcal{C}_{2^N-1,0} & \cdots & \mathcal{C}_{2^N-1,2^N-1} \end{pmatrix} \qquad \begin{matrix} |\phi_0|^2 \rightarrow 00...0 \\ |\phi_1|^2 \rightarrow 00...1 \\ \vdots \\ |\phi_{2^N-1}|^2 \rightarrow 11...1 \end{matrix}$$

$$|\psi\rangle \qquad |\phi\rangle = \mathcal{C}|\psi\rangle \qquad |\phi\rangle \rightarrow b_1 b_2 ... b_N$$

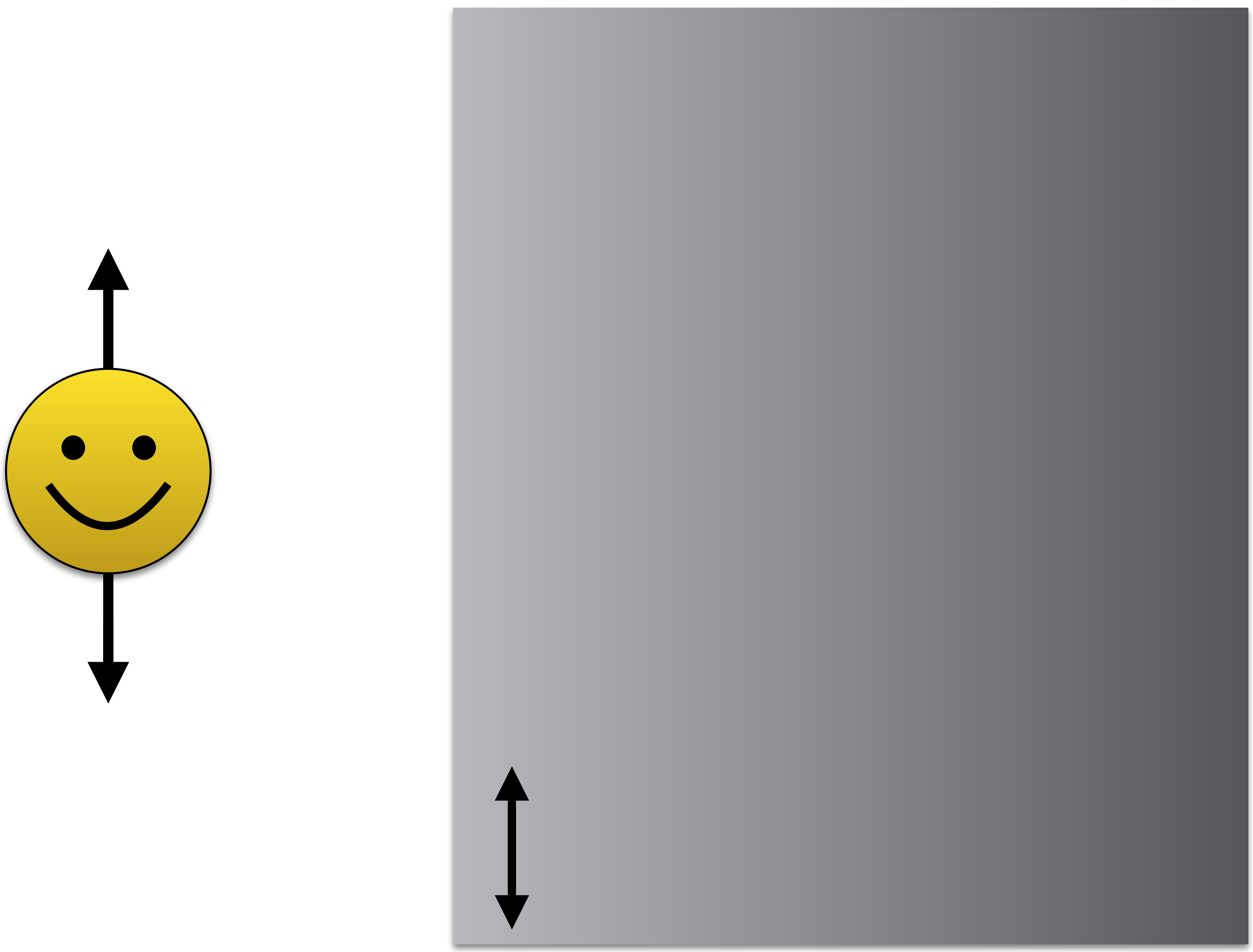
Example with polarisation



Example with polarisation



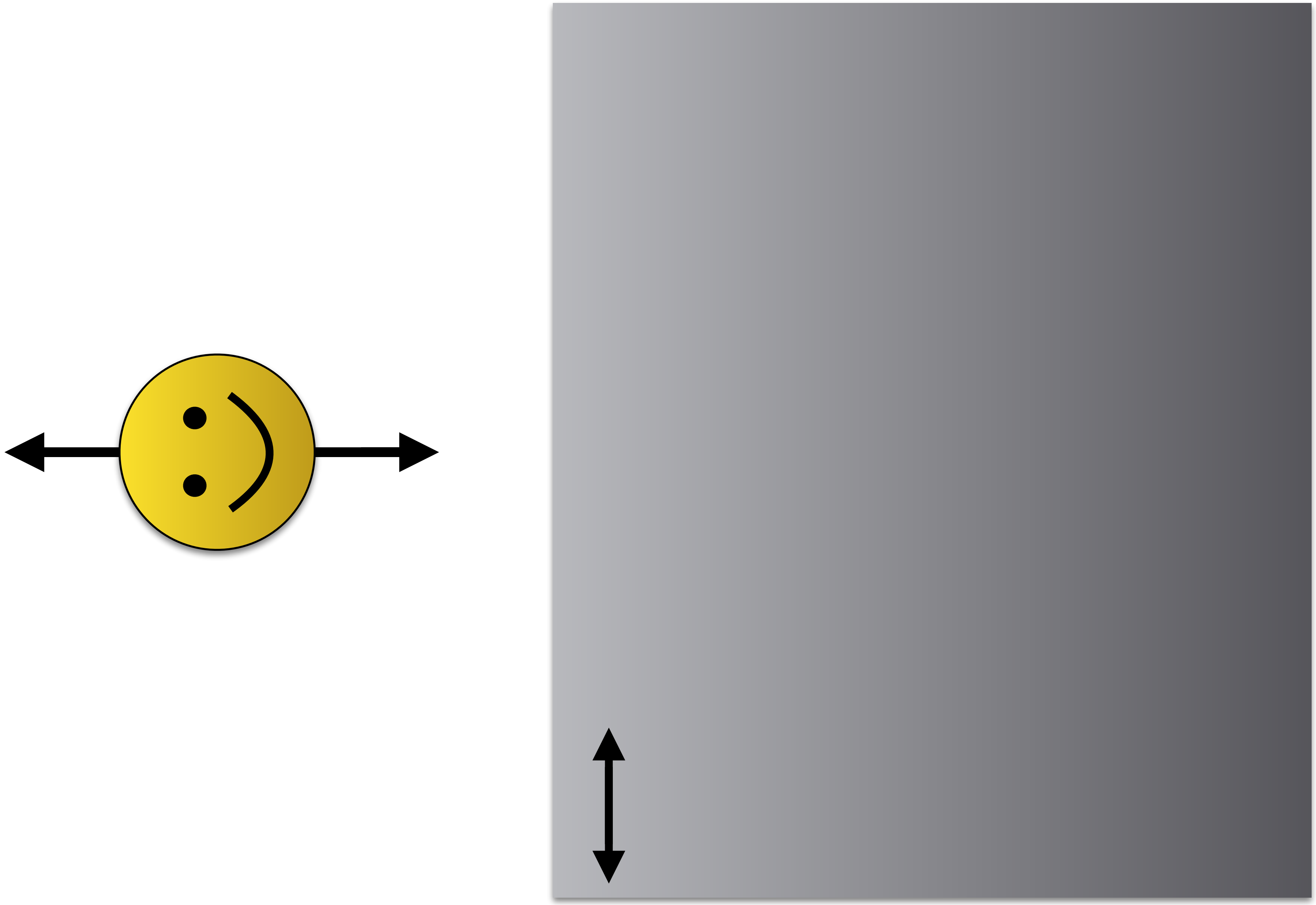
Example with polarisation



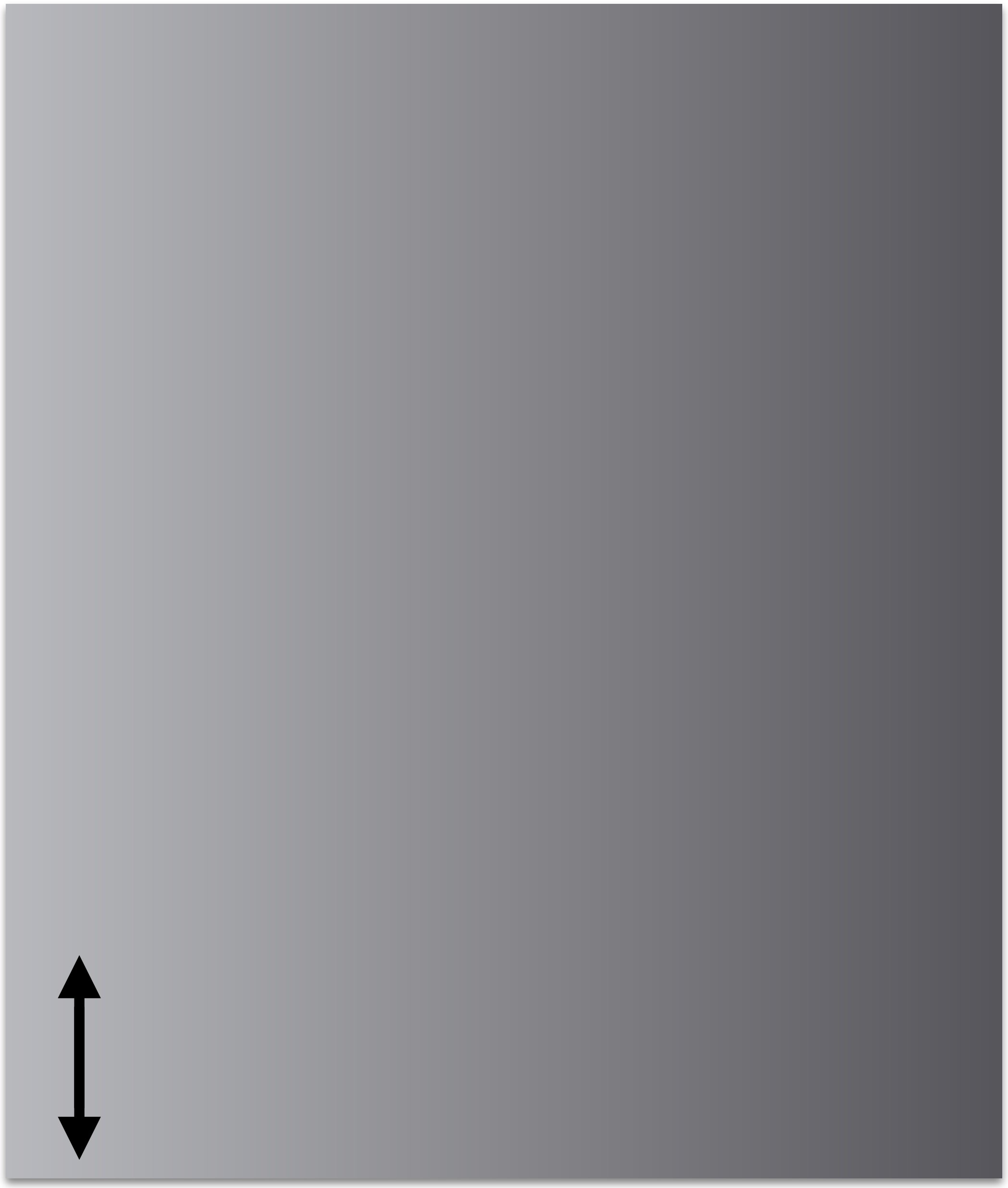
Example with polarisation

Passes

Example with polarisation

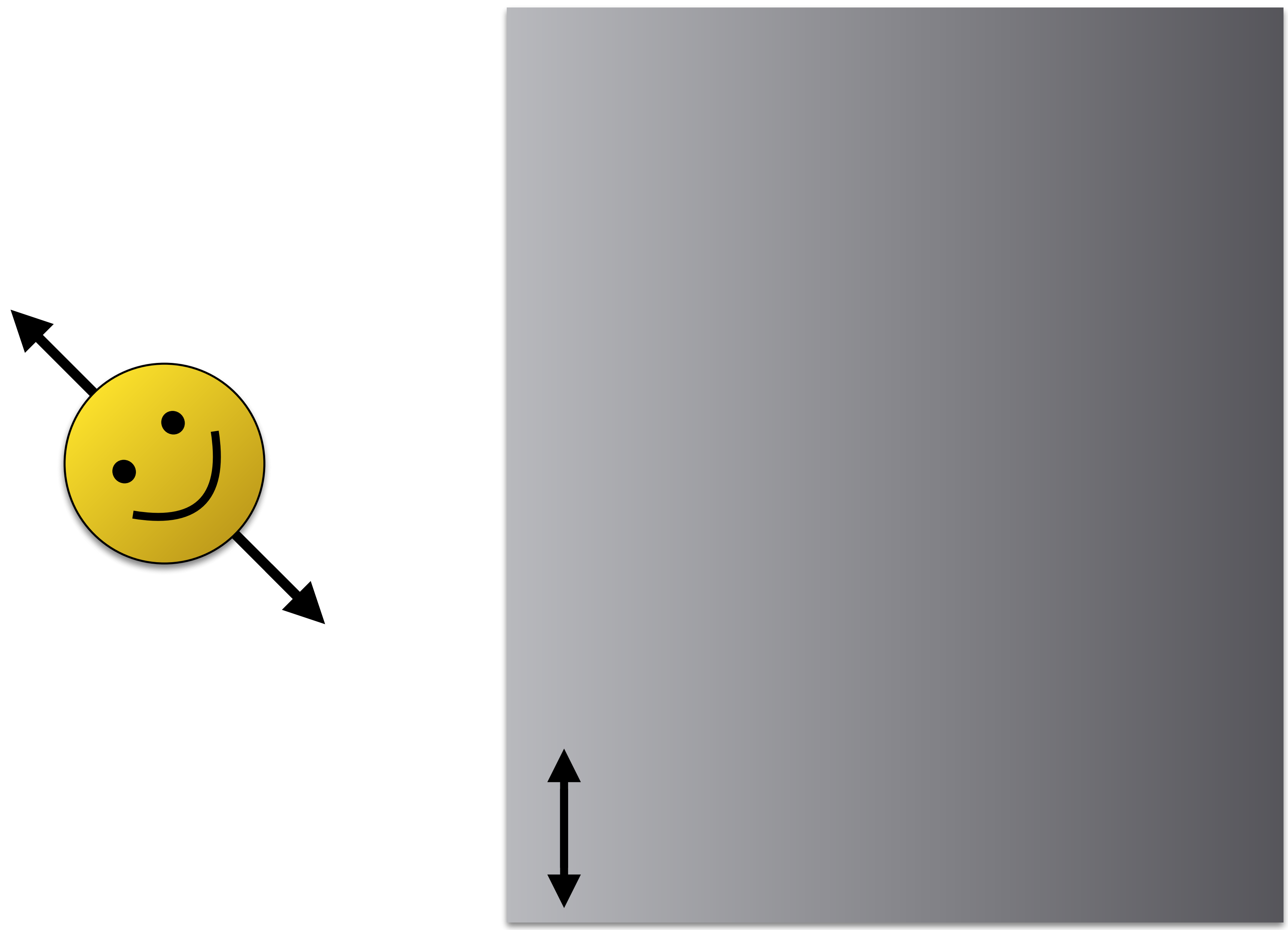


Example with polarisation

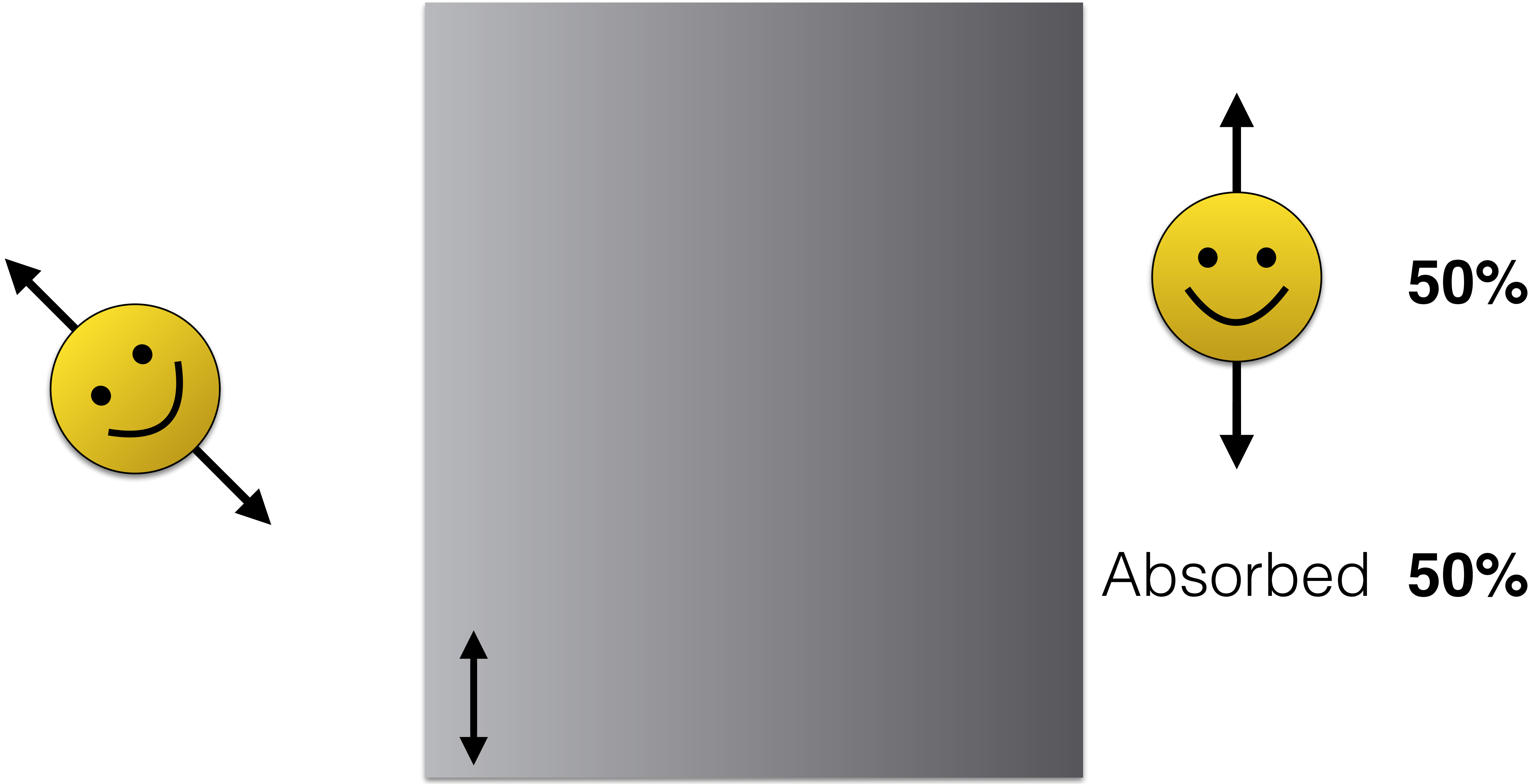


Absorbed

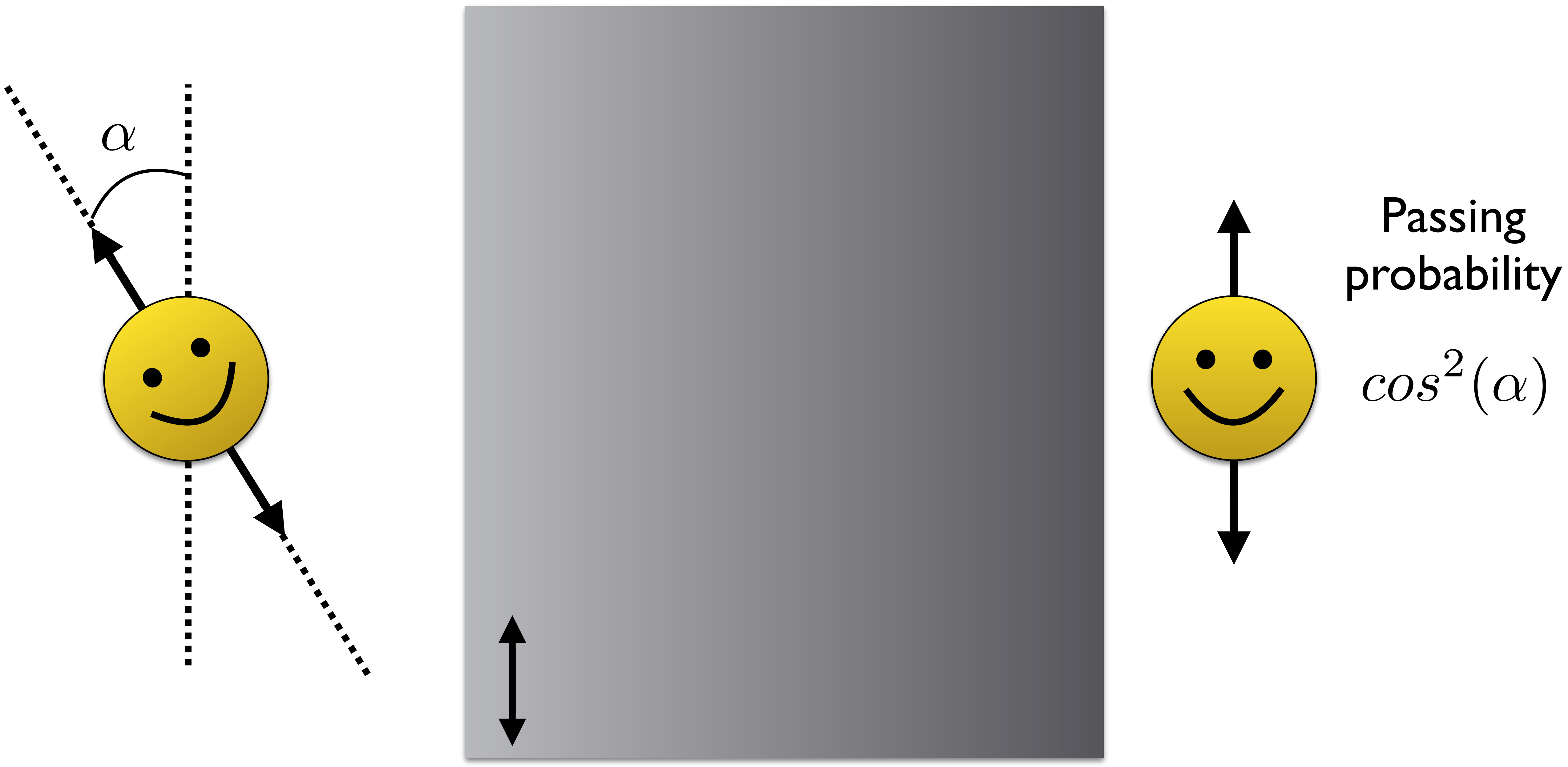
Example with polarisation



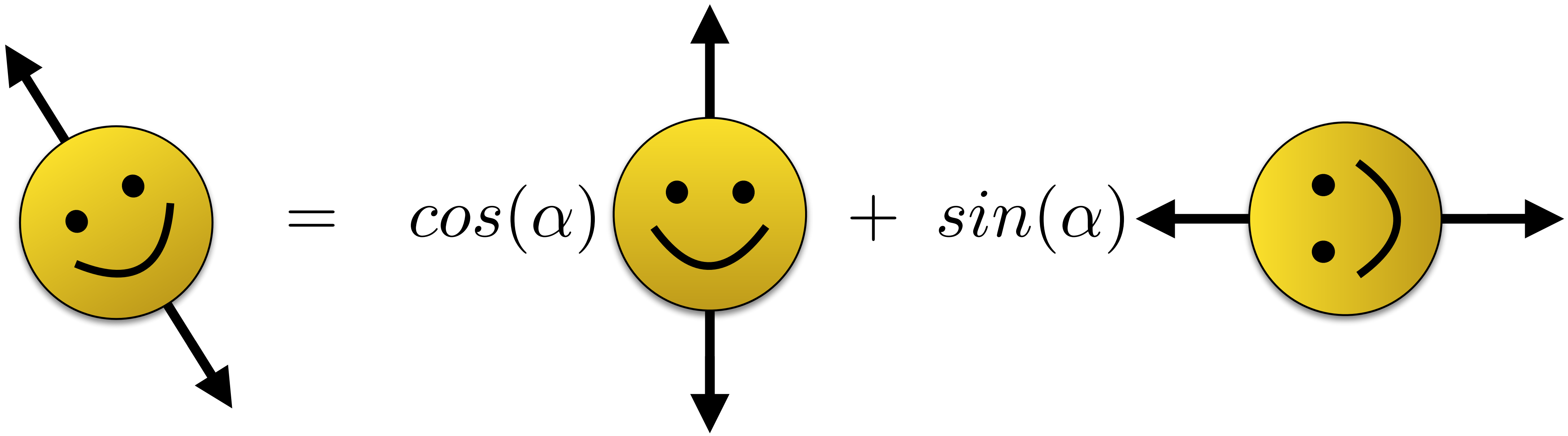
Example with polarisation



Example with polarisation



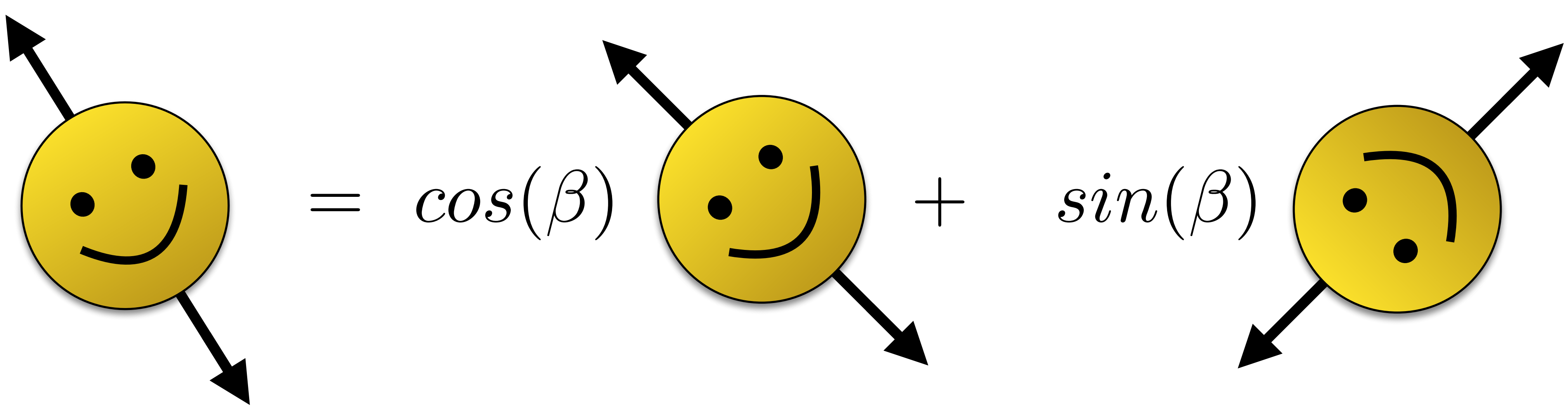
Example with polarisation



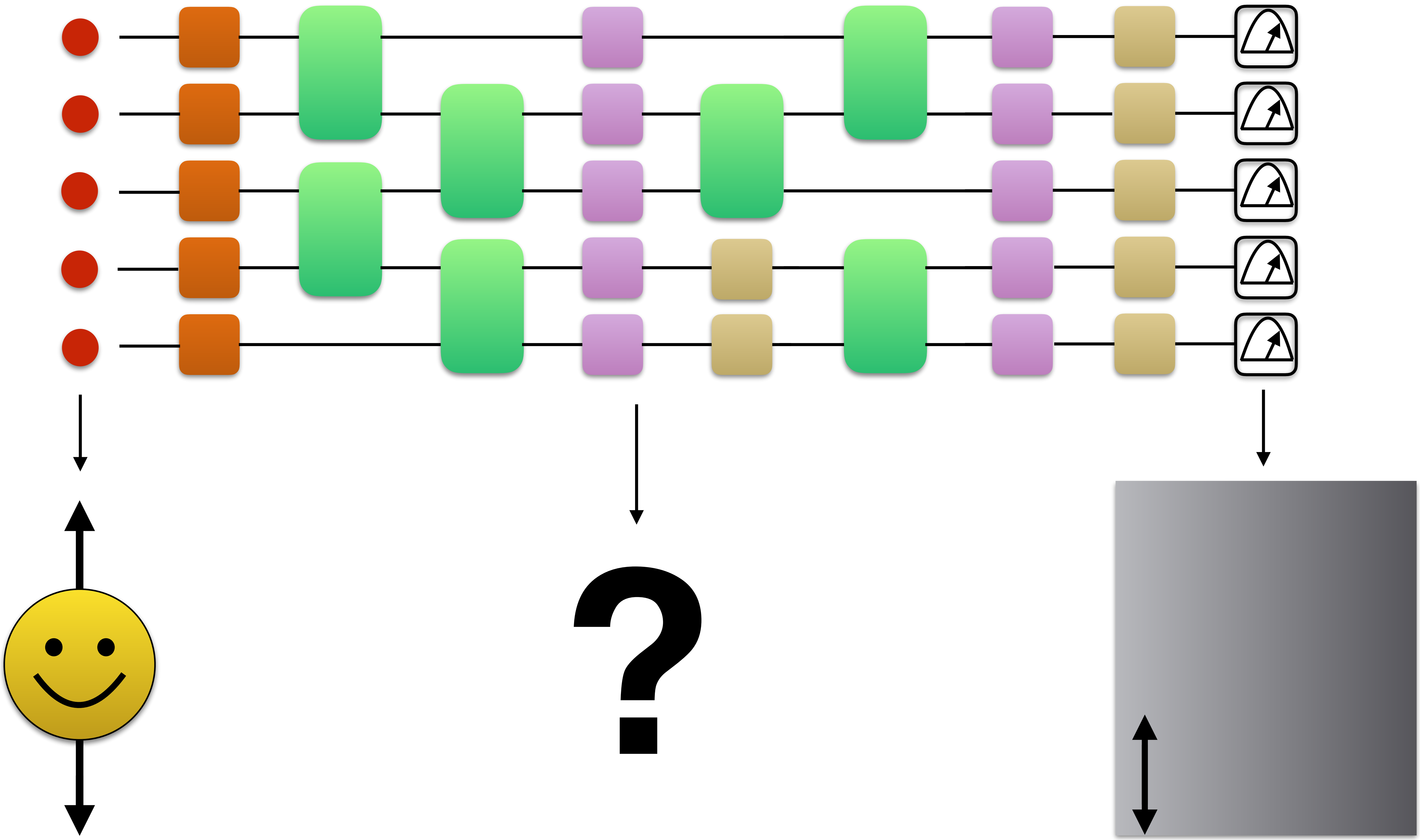
$$|\psi\rangle = cos(\alpha)|0\rangle + sin(\alpha)|1\rangle$$

Superposition

Can choose a different basis

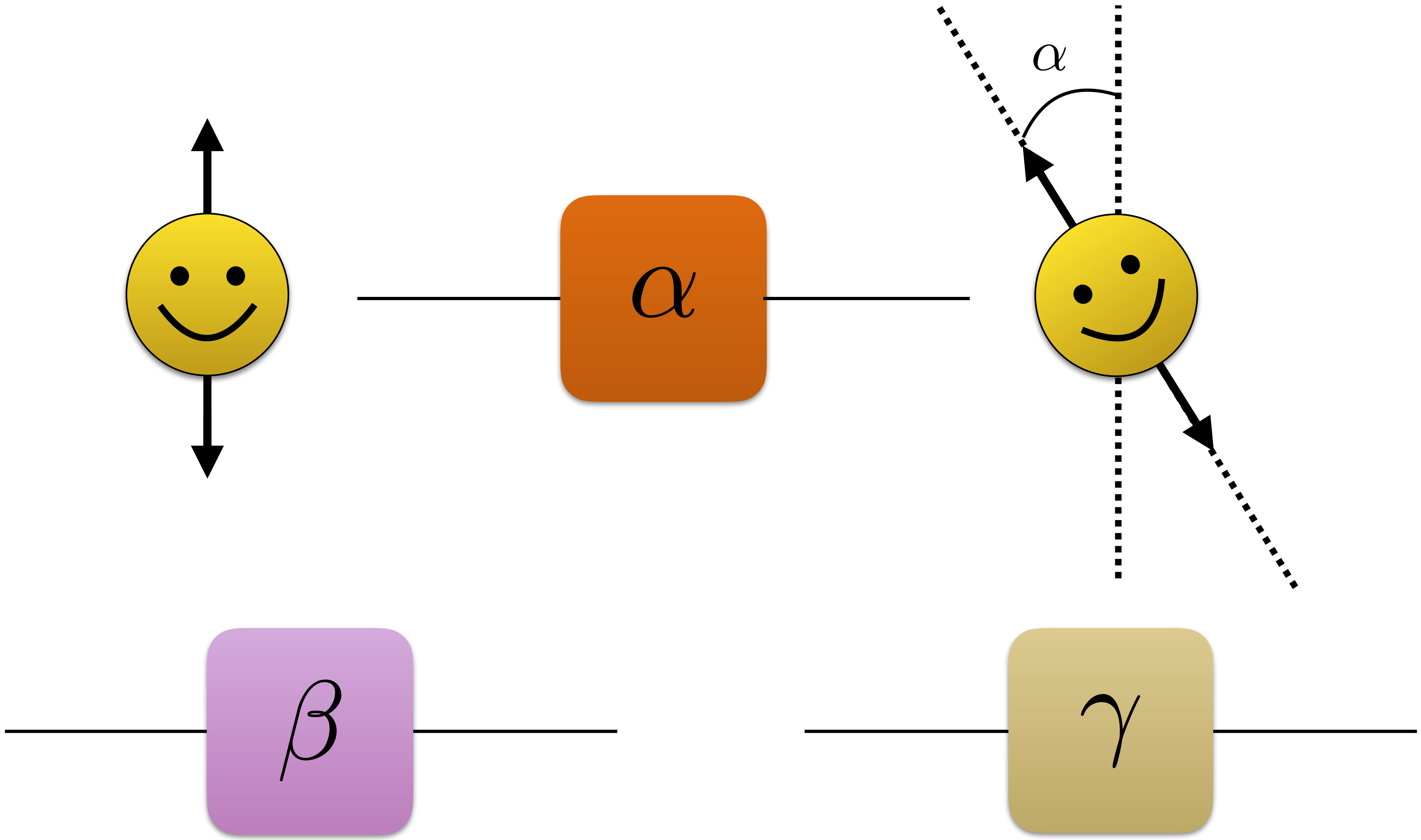


Example with polarisation



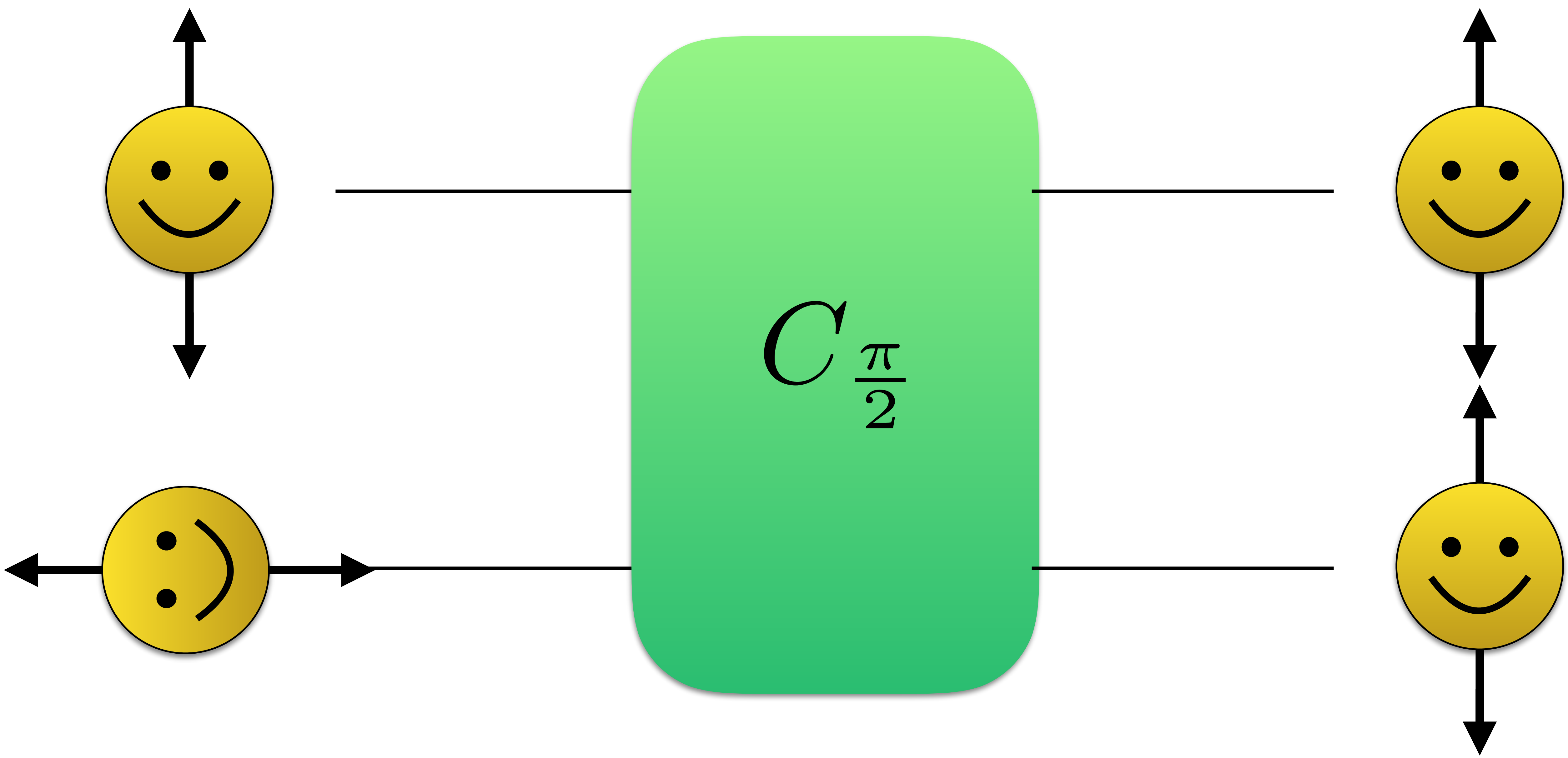
Example with polarisation

Single-qubit gates perform rotations



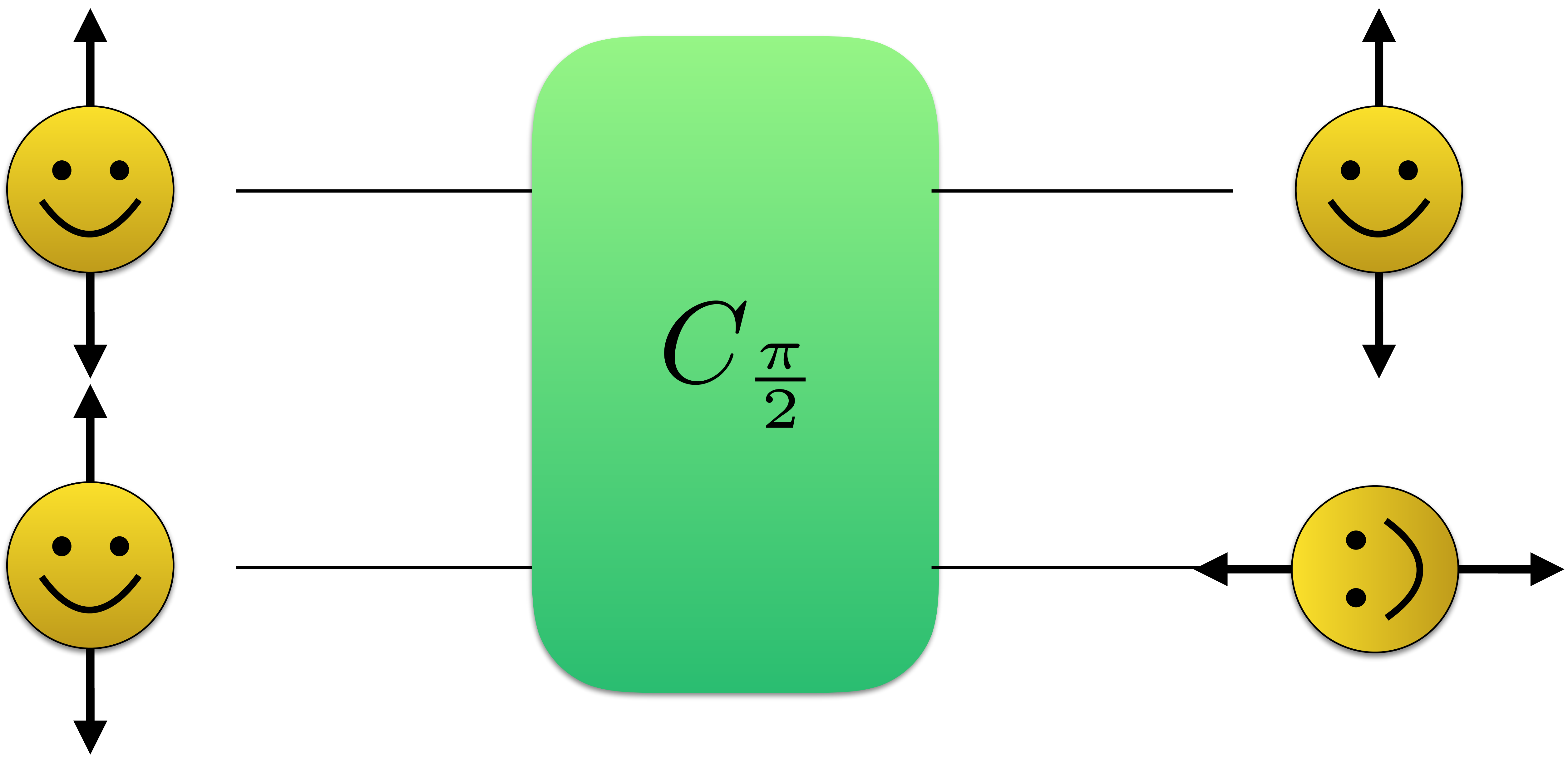
Example with polarisation

Two-qubit gates create **controlled** rotations



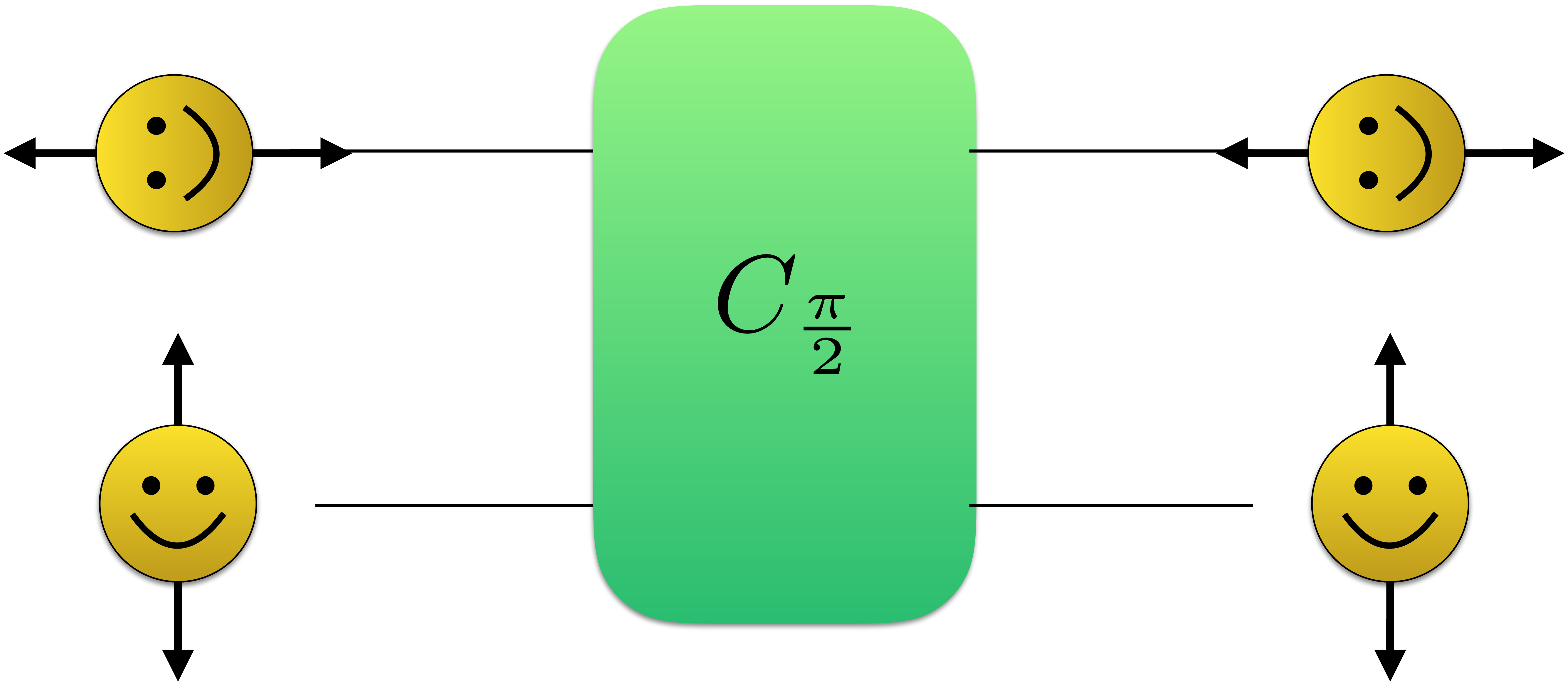
Example with polarisation

Two-qubit gates create **controlled** rotations



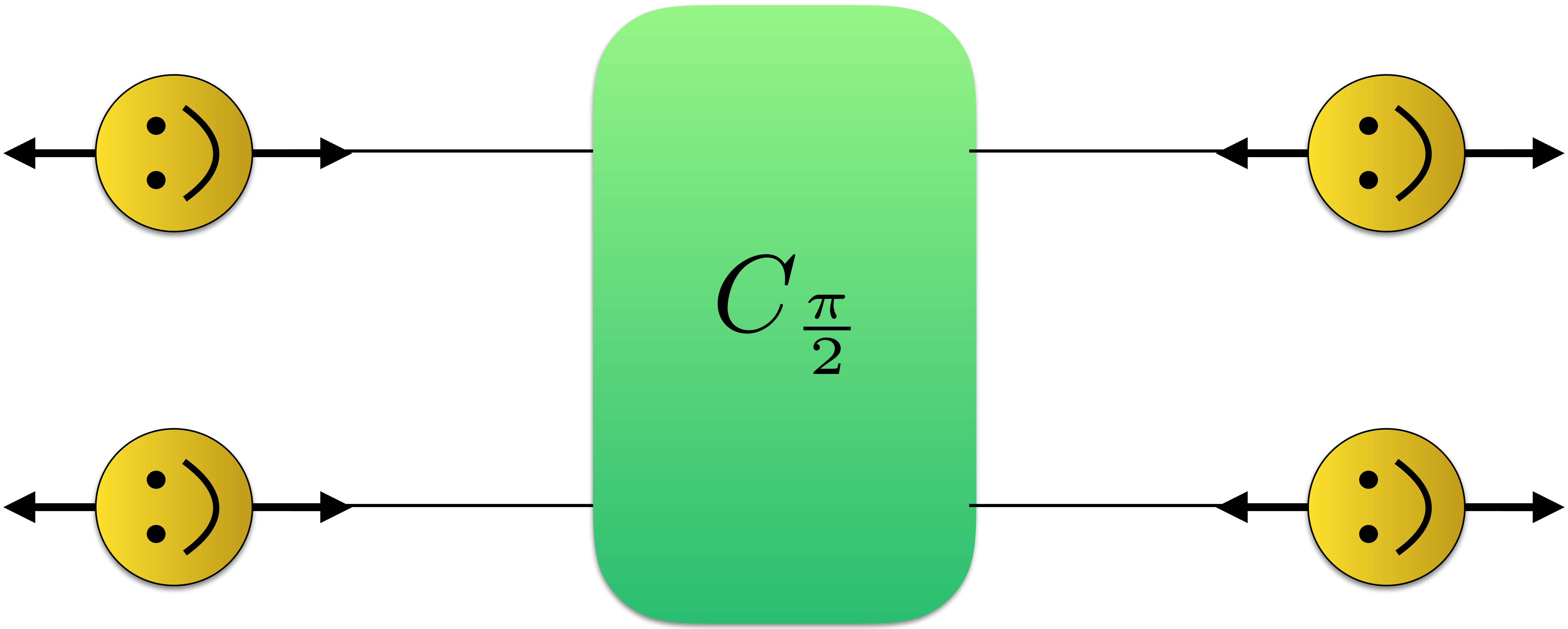
Example with polarisation

Two-qubit gates create **controlled** rotations



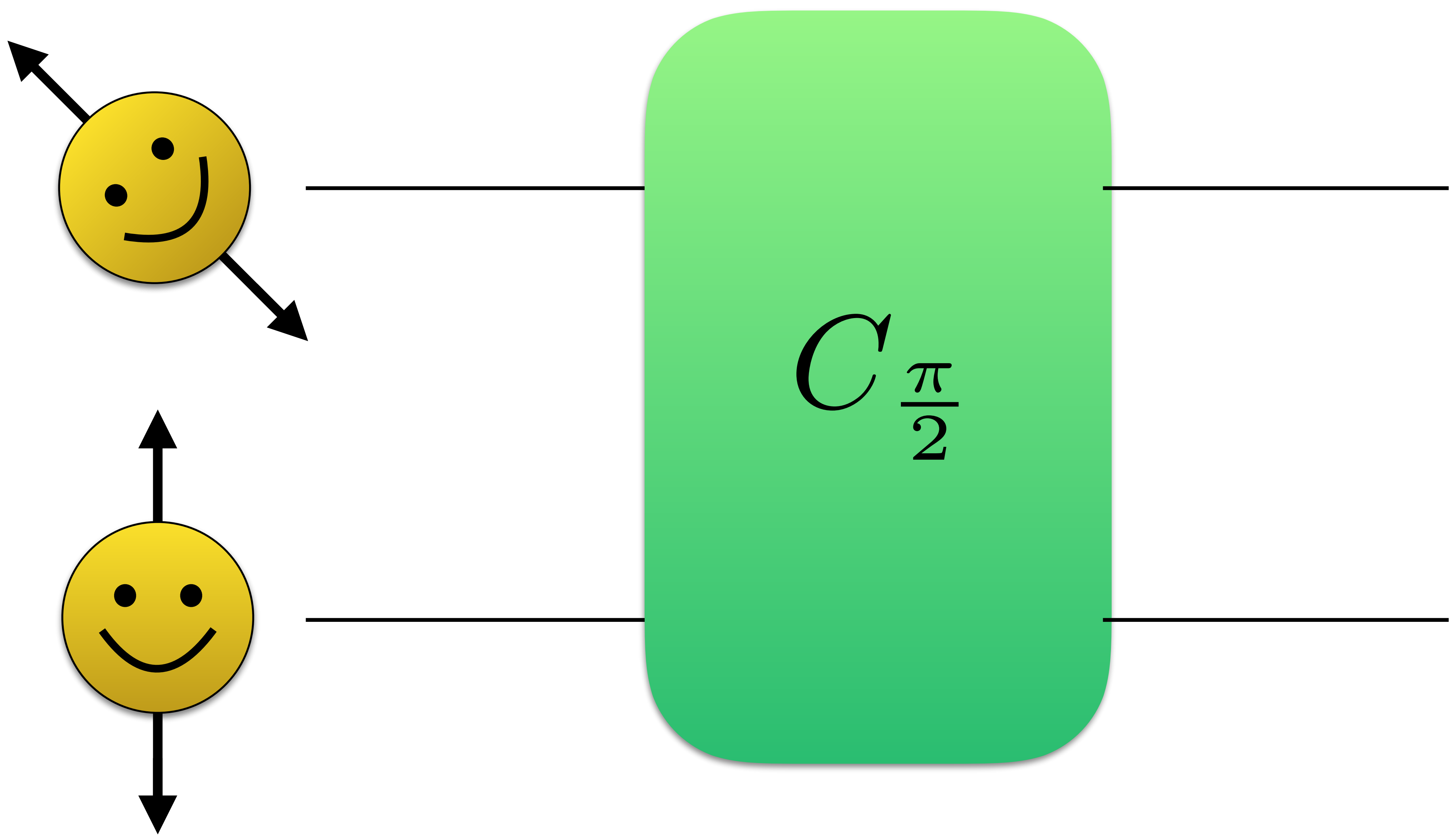
Example with polarisation

Two-qubit gates create **controlled** rotations

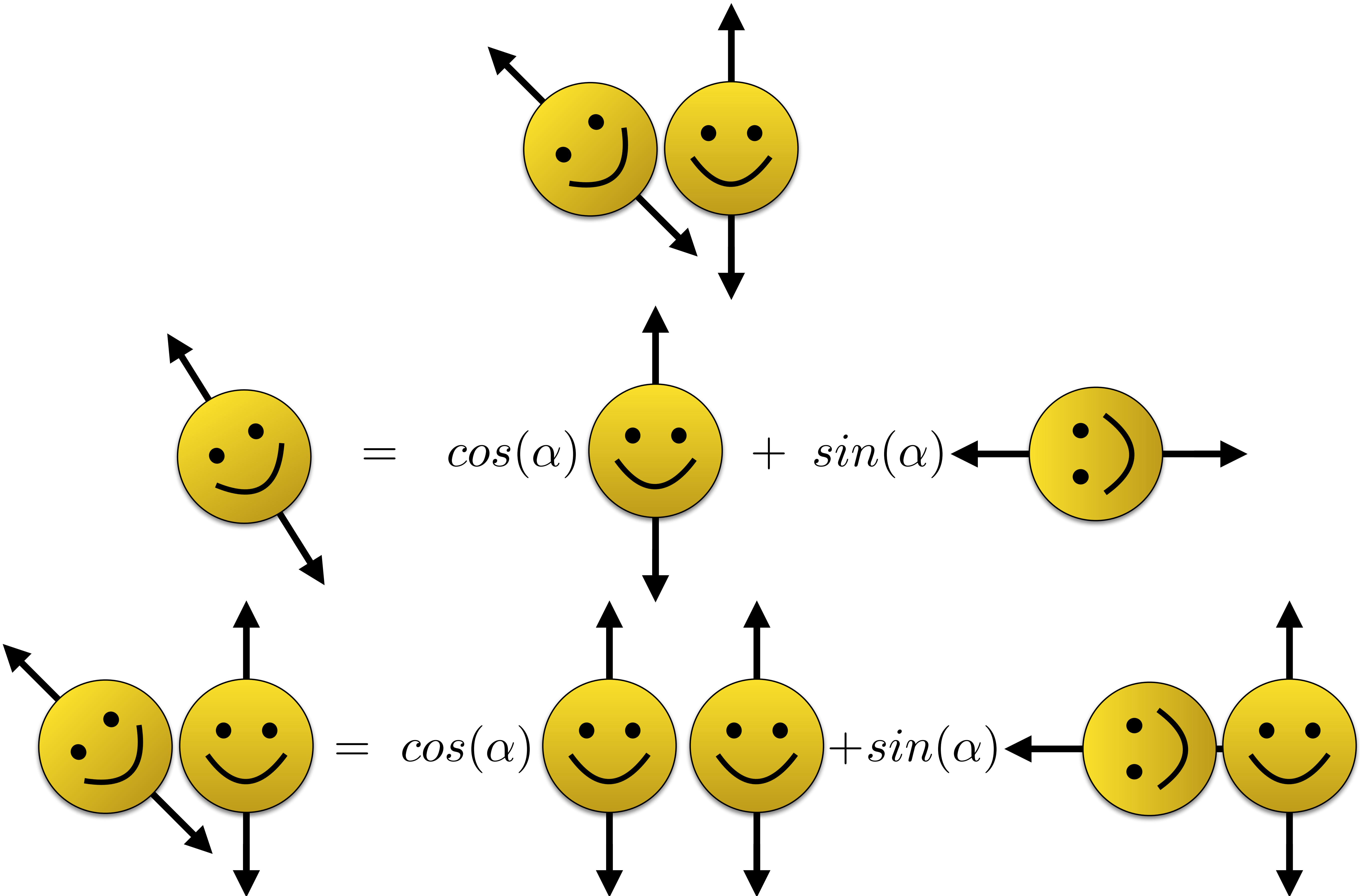


Example with polarisation

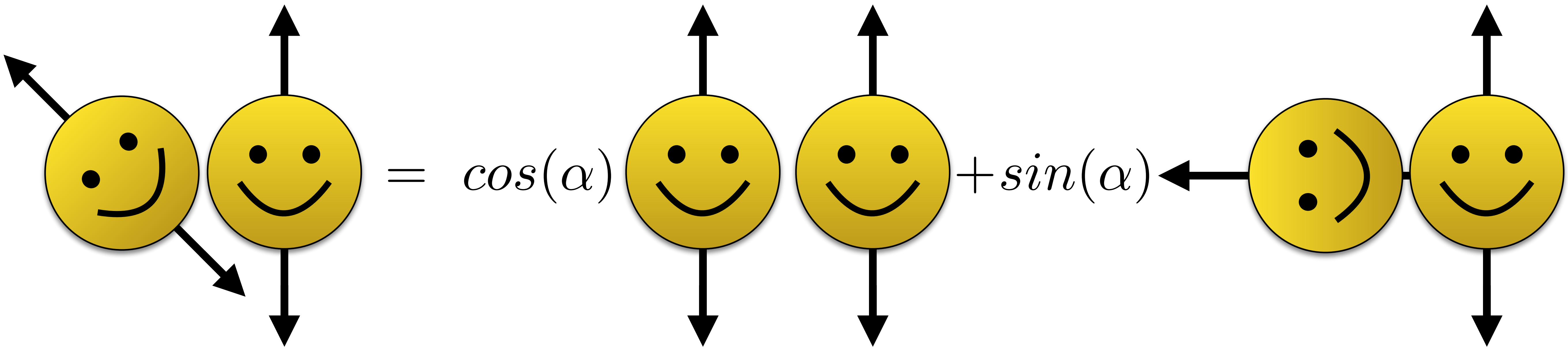
What about this…



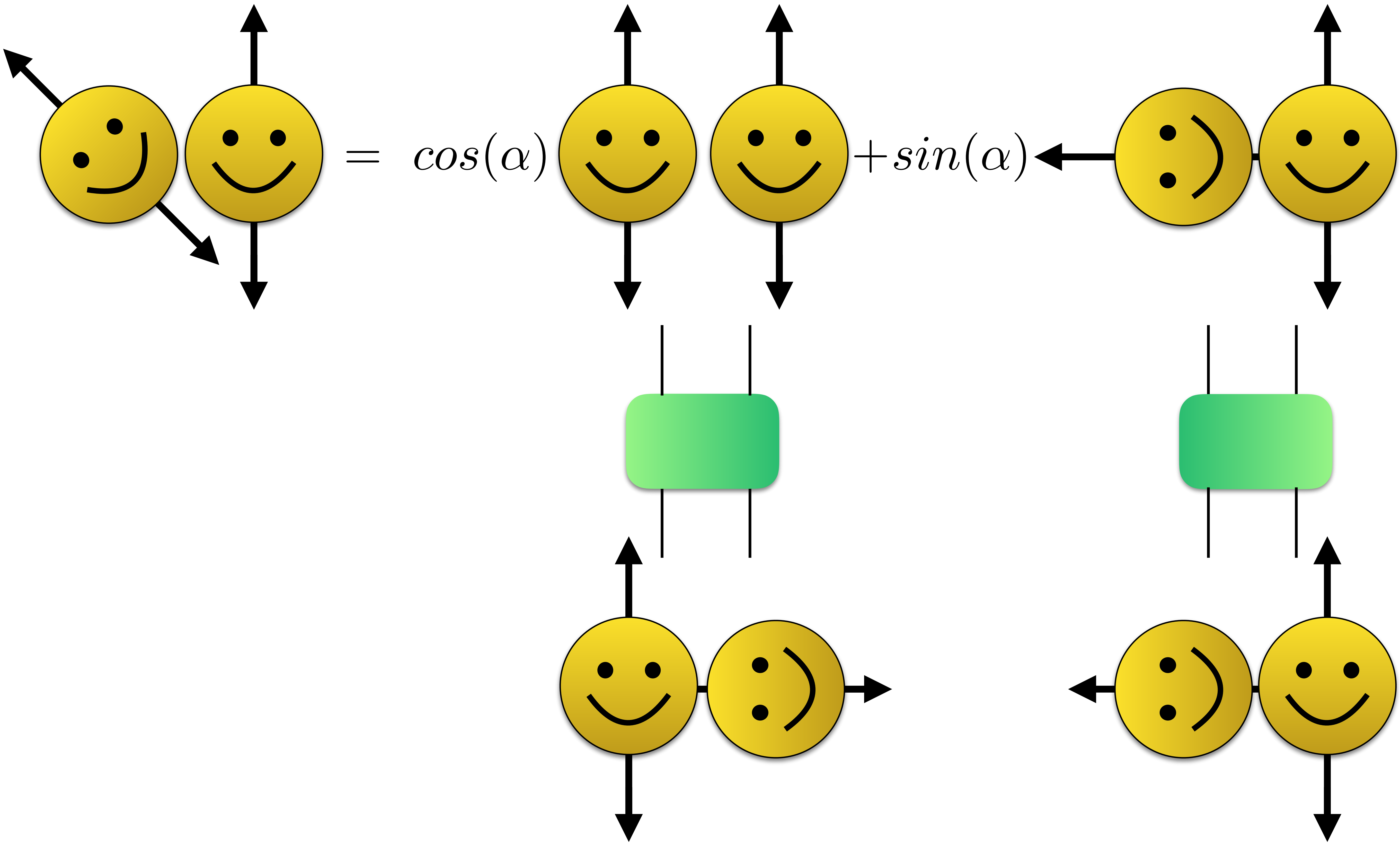
Example with polarisation



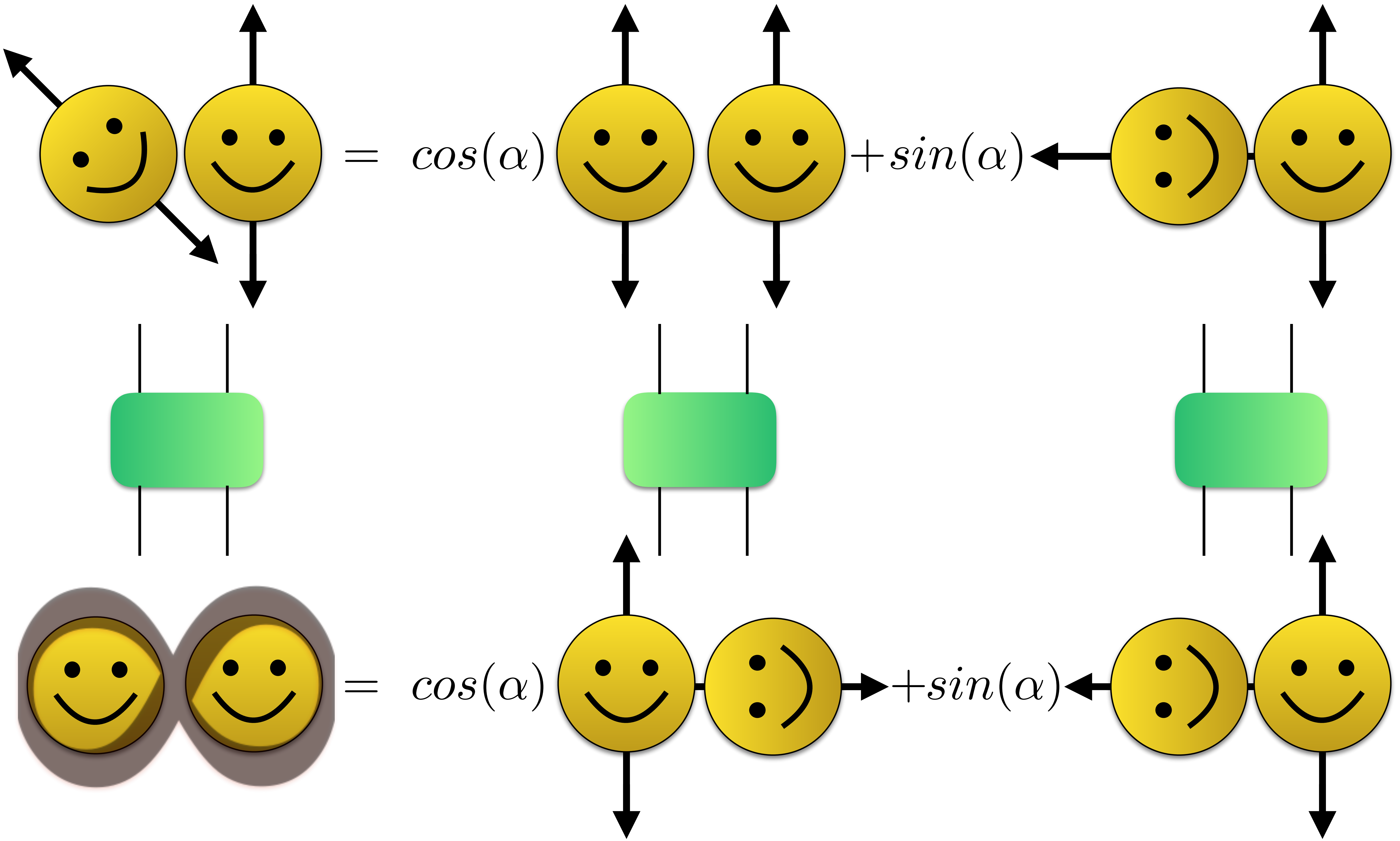
Example with polarisation



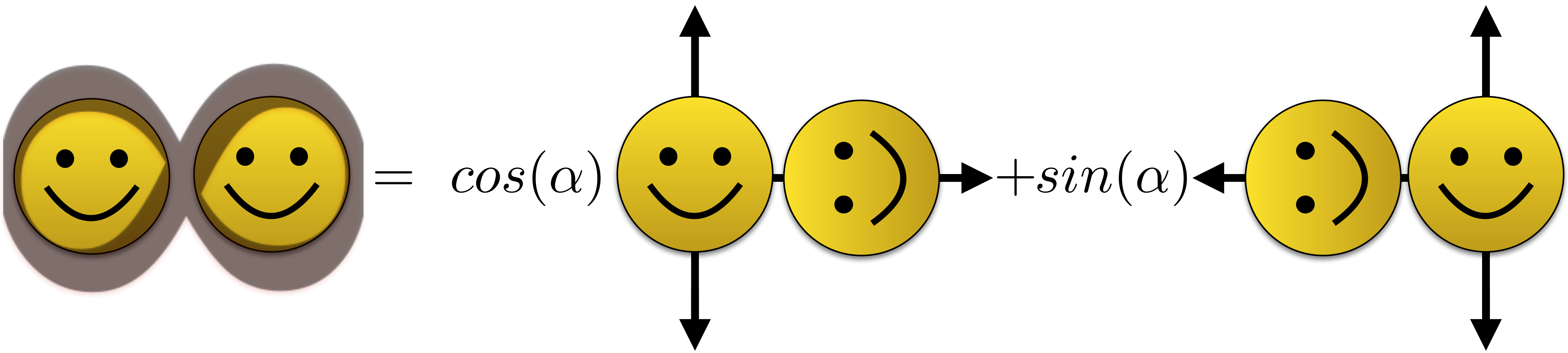
Example with polarisation



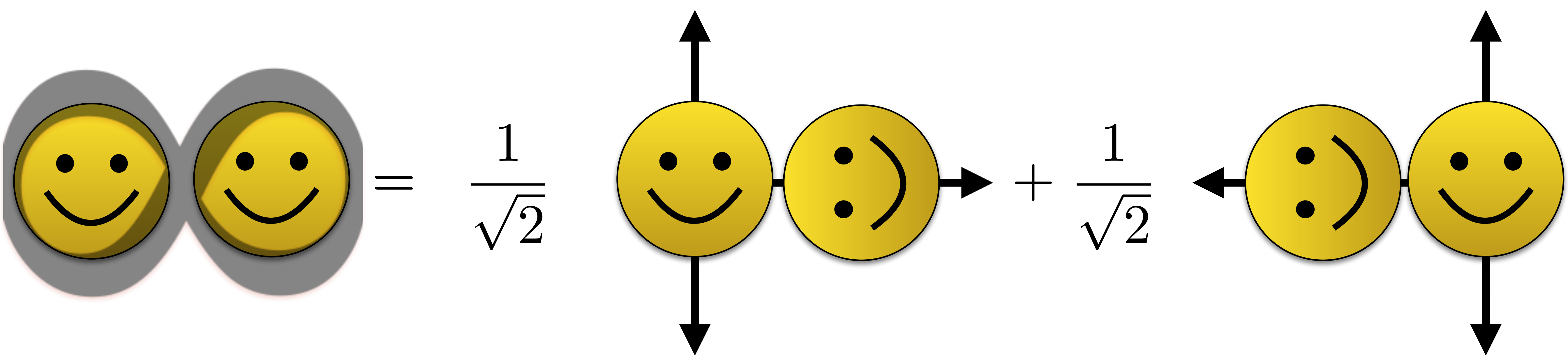
Example with polarisation



Example with polarisation

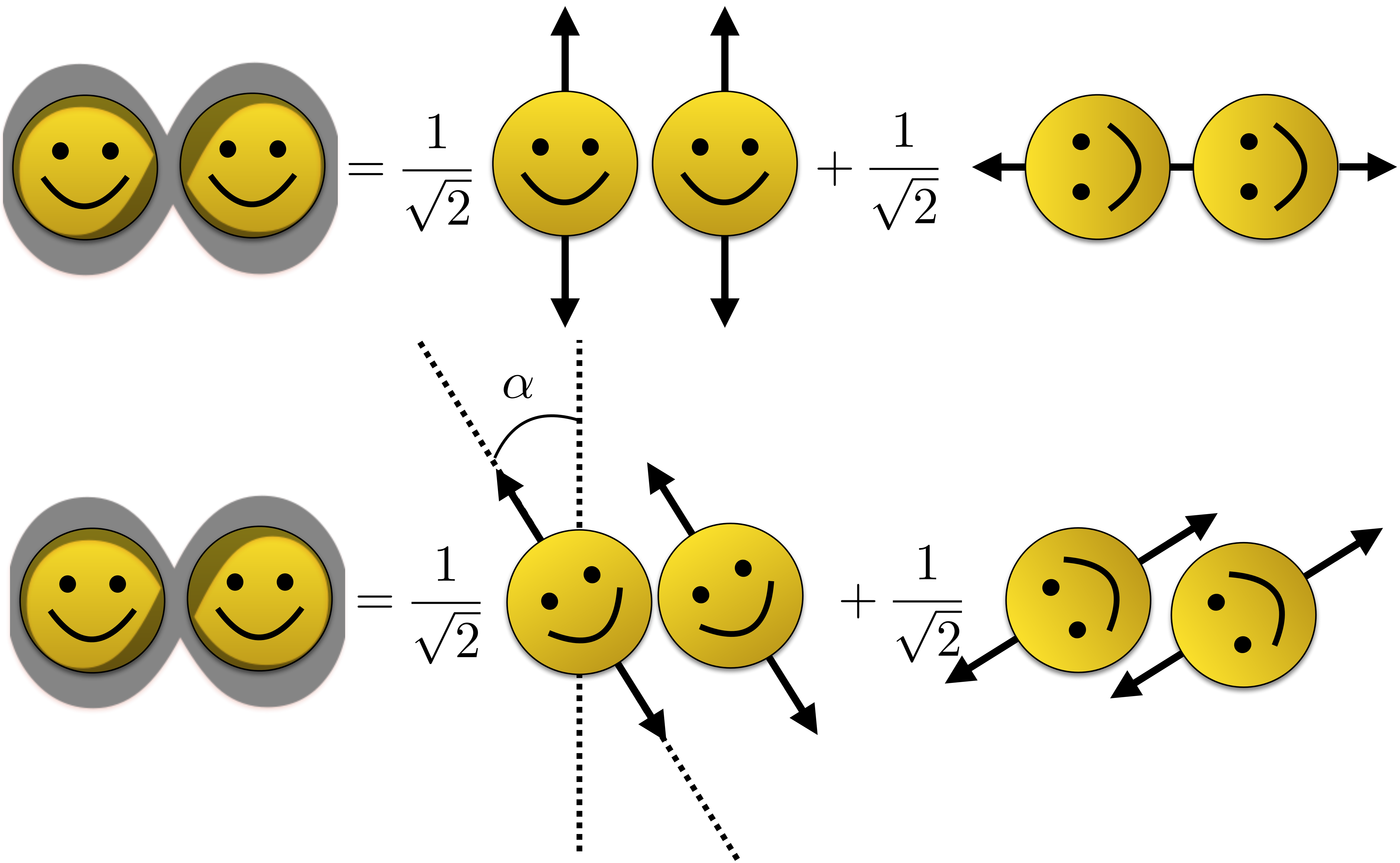


Take $\alpha = \pi/4$



The photons are **entangled**

Example with polarisation



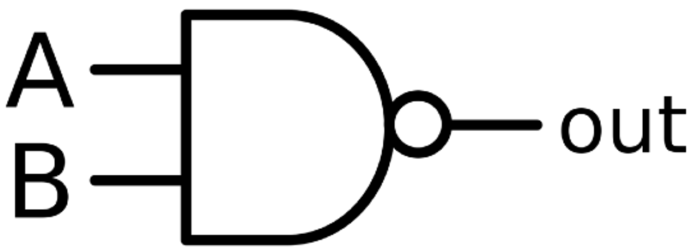
This is true for any α

Universality

Classical

Set of gates that can implement any boolean function

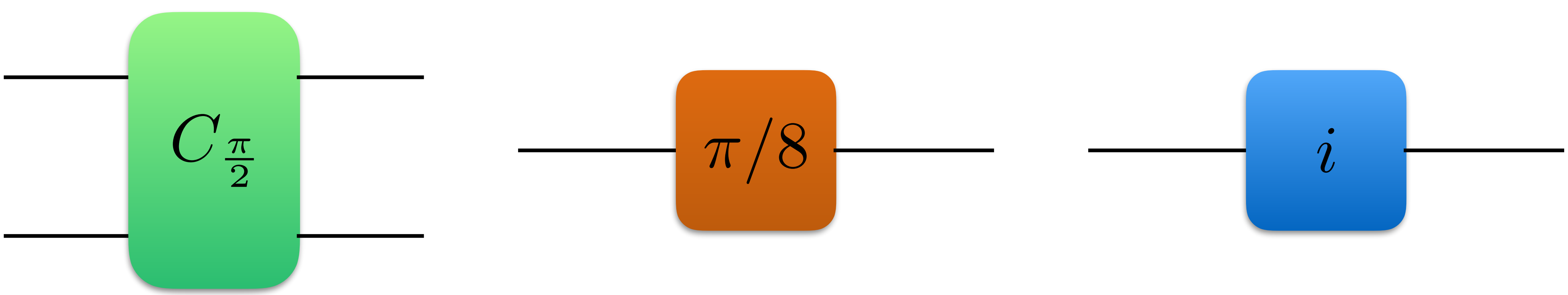
$$\{AND, OR, NOT\}$$



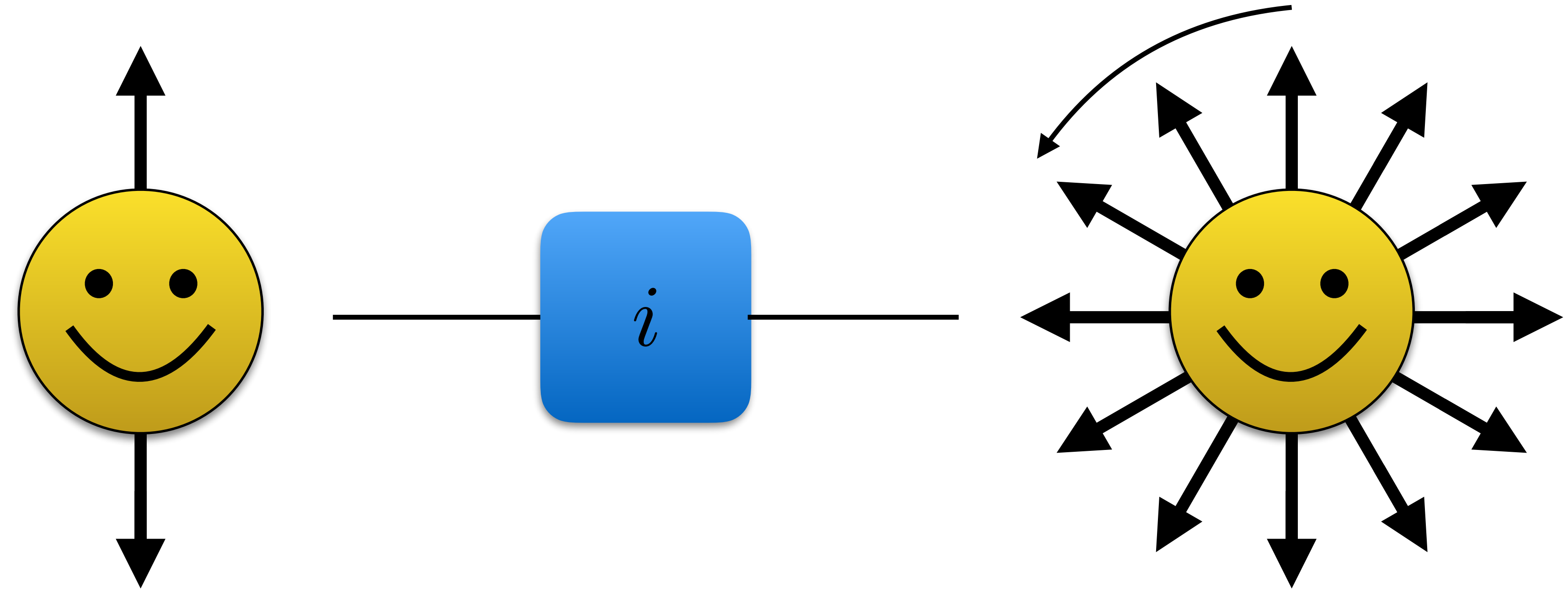
$$\{NAND\} \quad out = NOT(AND(A, B))$$

Quantum

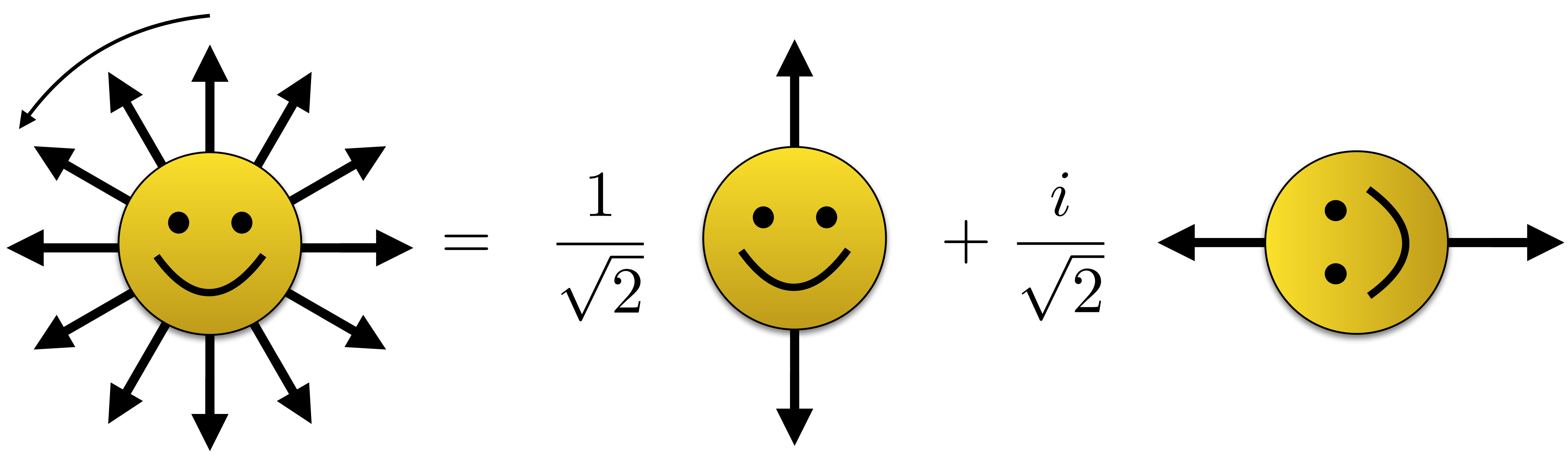
Set of gates that can implement any quantum operation



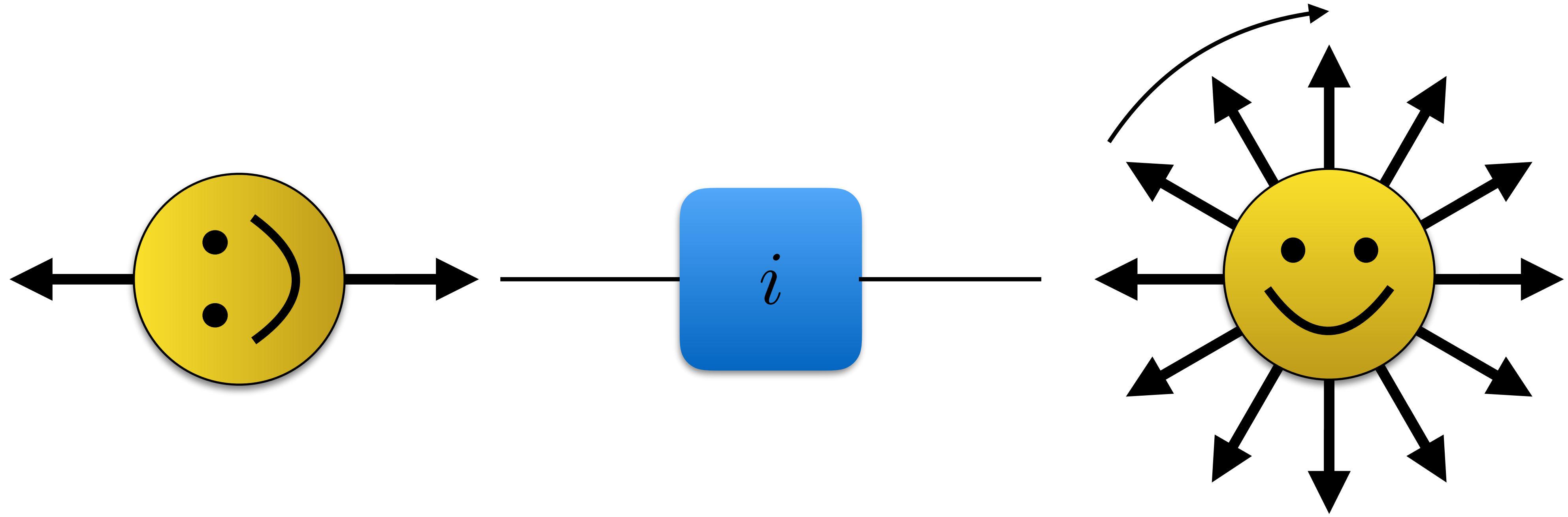
The i gate



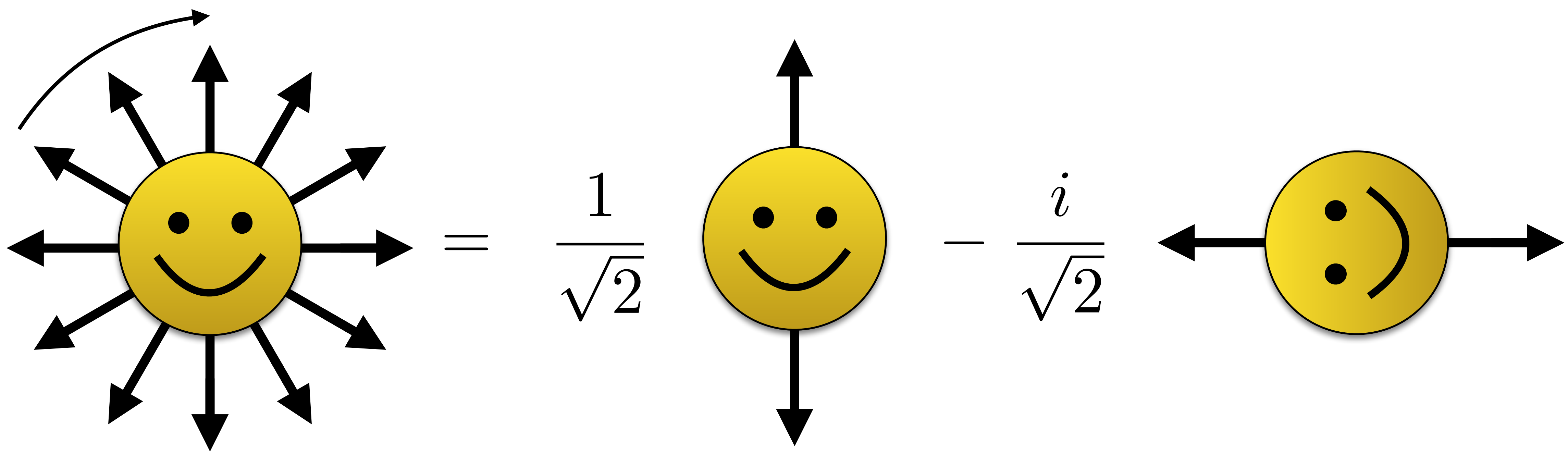
Circular polarisation



The i gate

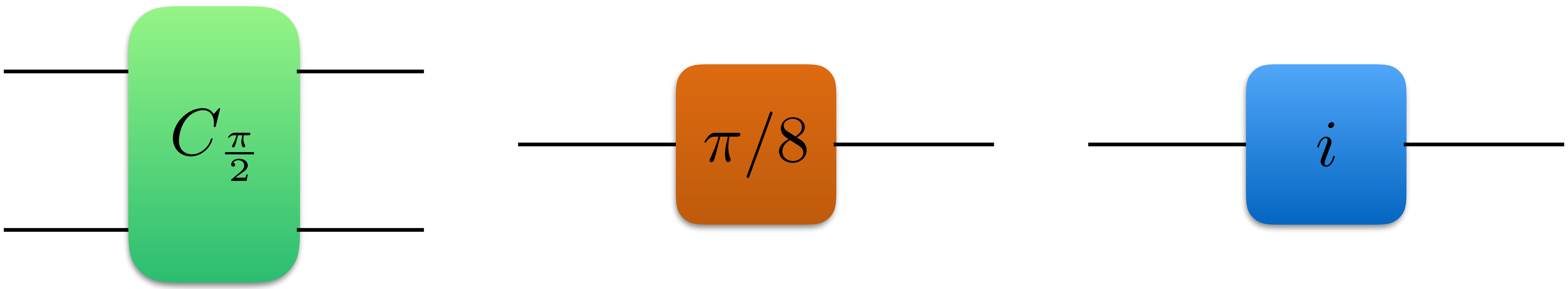


Circular polarisation



Imperfections

Gates are usually imperfect



10% of the time acts **correctly**
90% of the time does something else

Two-qubit gates are especially problematic!

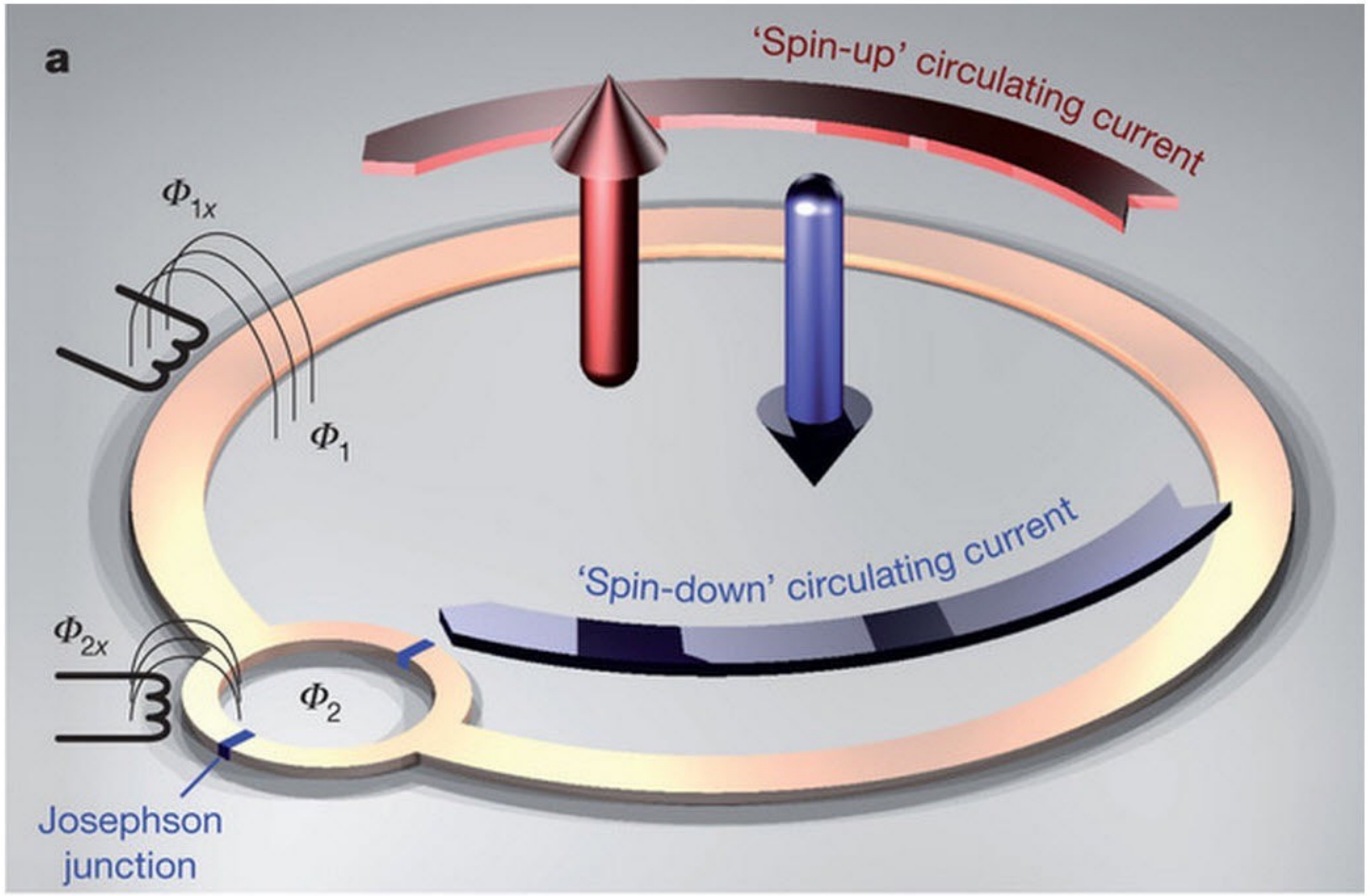
For large circuits, gates should be almost perfect

Fault tolerant protocols can handle small errors

Other hardware implementations

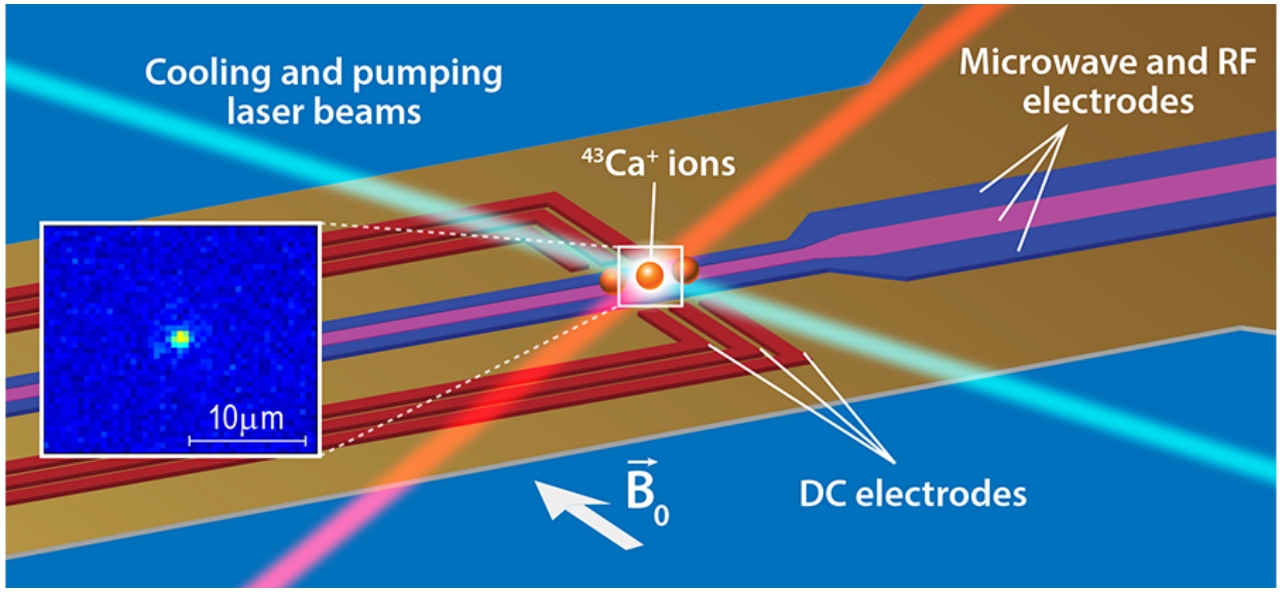
Superconducting qubits (SQUIDs)

Encoding information in current



Ion traps

Encoding information in electron spins

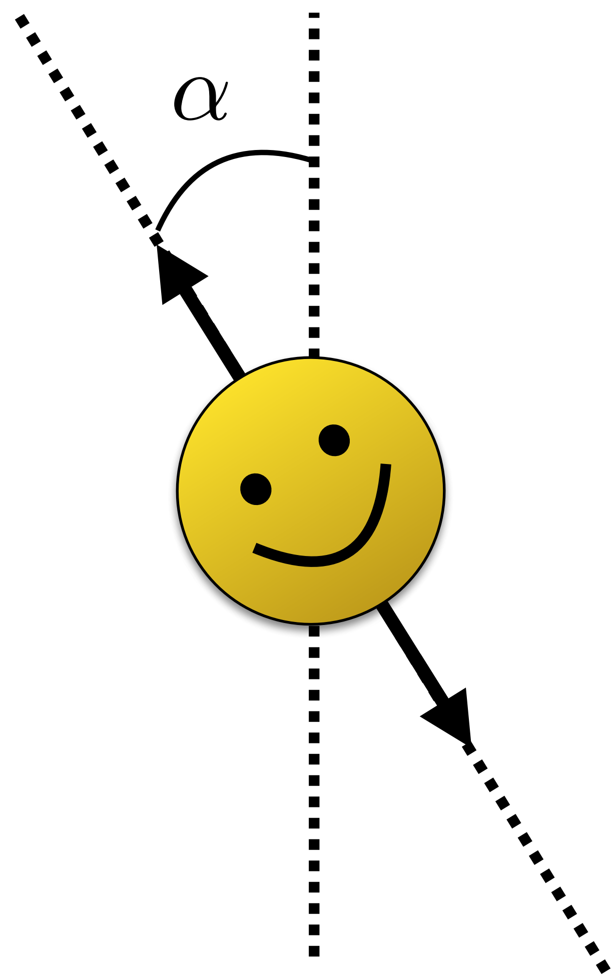


Existing devices

	# Qubits	Universal	Fault tolerant
D-Wave	2048	✗	✗
IBM	50	✓	✗
Rigetti	18	✓	✗
Google	72?	✓	✗
Others	<20	Depends	Depends

Pick α at random from $\{-\pi/4, 0, \pi/4, \pi/2\}$

Given **one** photon
in the state



Can you find α?

QM says no!

Cannot guess α with probability greater than $\frac{1}{2}$

Measurements disturb quantum states

Cannot copy unknown quantum states

Quantum cryptography

Leveraging “quantum uncertainty” for cryptography

Quantum key distribution (QKD)

Quantum digital signatures (QDS)

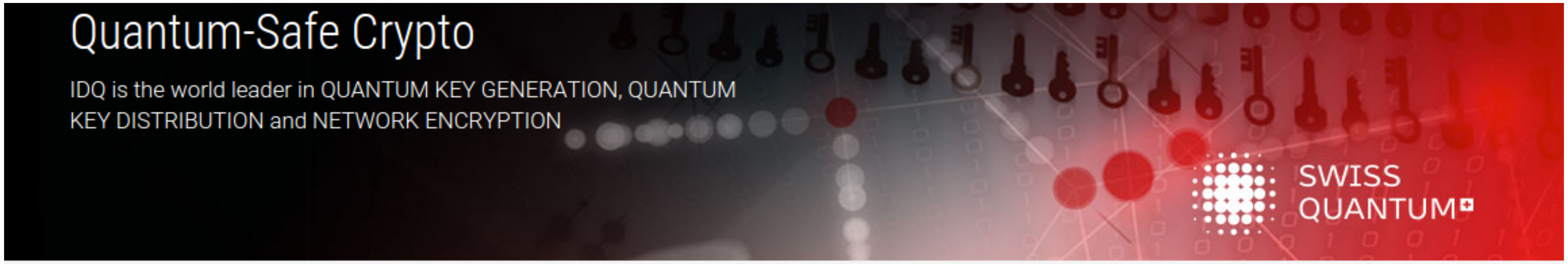
Quantum secure random number generation (QRNG)

Quantum money

Blind quantum computation

Quantum secure multi-party computation

Quantum cryptography



HOME > QUANTUM-SAFE CRYPTO

Quantum-Safe Crypto

ID Quantique provides high-performance network encryption solutions for the protection of data in transit. IDQ's encryption platform can encrypt high throughput traffic up to 100Gbps on local and storage area networks for data back-up and recovery, as well as on fully meshed global WAN networks for international operations.

IDQ uses state-of-the-art algorithms and highly secure quantum key generation and quantum key distribution (quantum cryptography), ensuring that the solutions are "quantum-safe" for the long-term protection of sensitive data into and beyond the quantum era.

CENTAURIS CN8000
MULTI-LINK, MULTI-PROTOCOL 100G DATA CENTER ENCRYPTION

CENTAURIS LINK ENCRYPTORS
HIGH PERFORMANCE ETHERNET & FIBRE CHANNEL ENCRYPTION

ARCIS
MPLS AND CLOUD ENCRYPTION

CERBERIS
QUANTUM KEY DISTRIBUTION SERVER

Contact

TEL: +41 22 301 83 71
EMAIL: info@idquantique.com

Name

Company

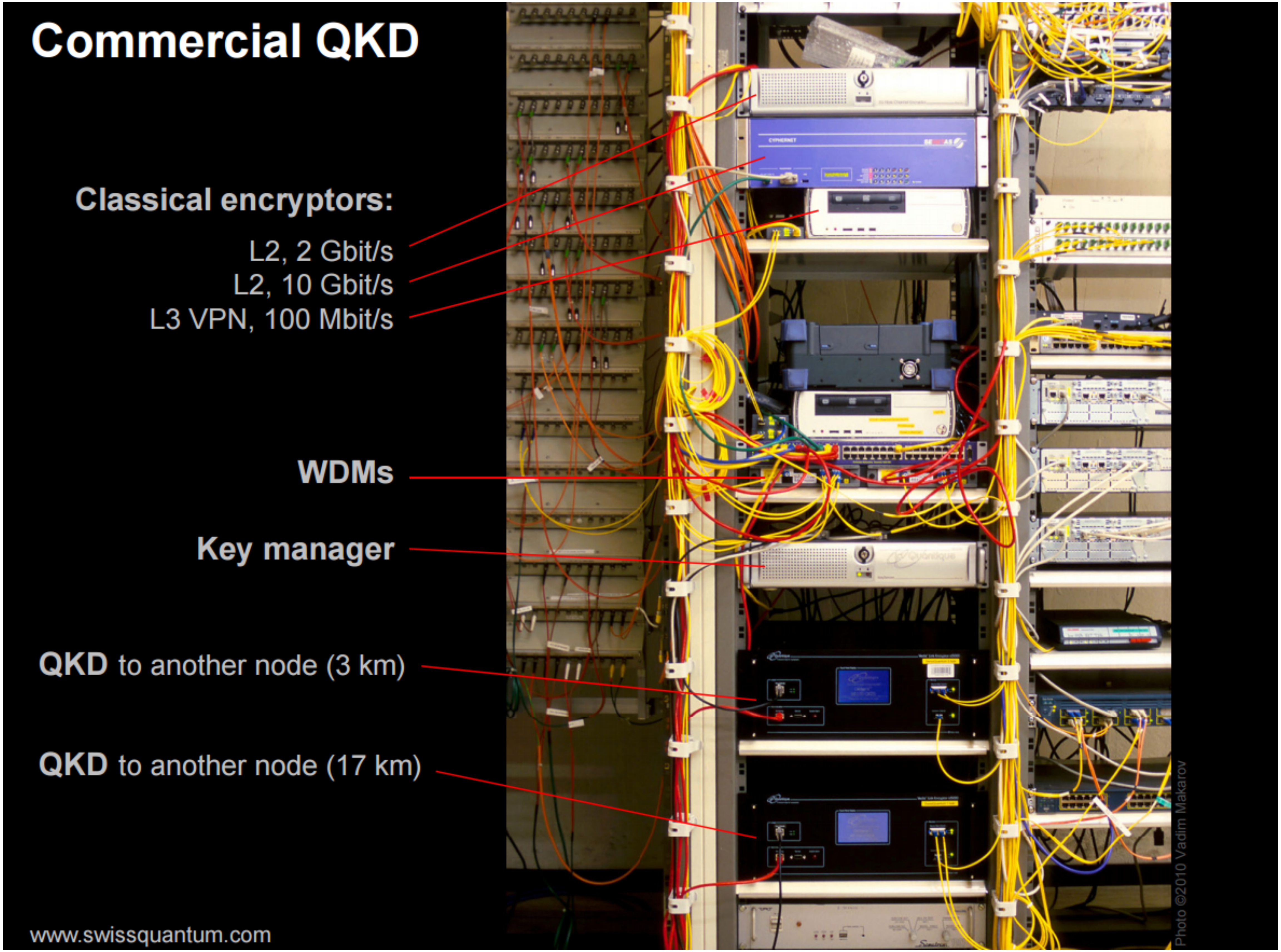
Email

Phone

ARRANGE A CALL BACK

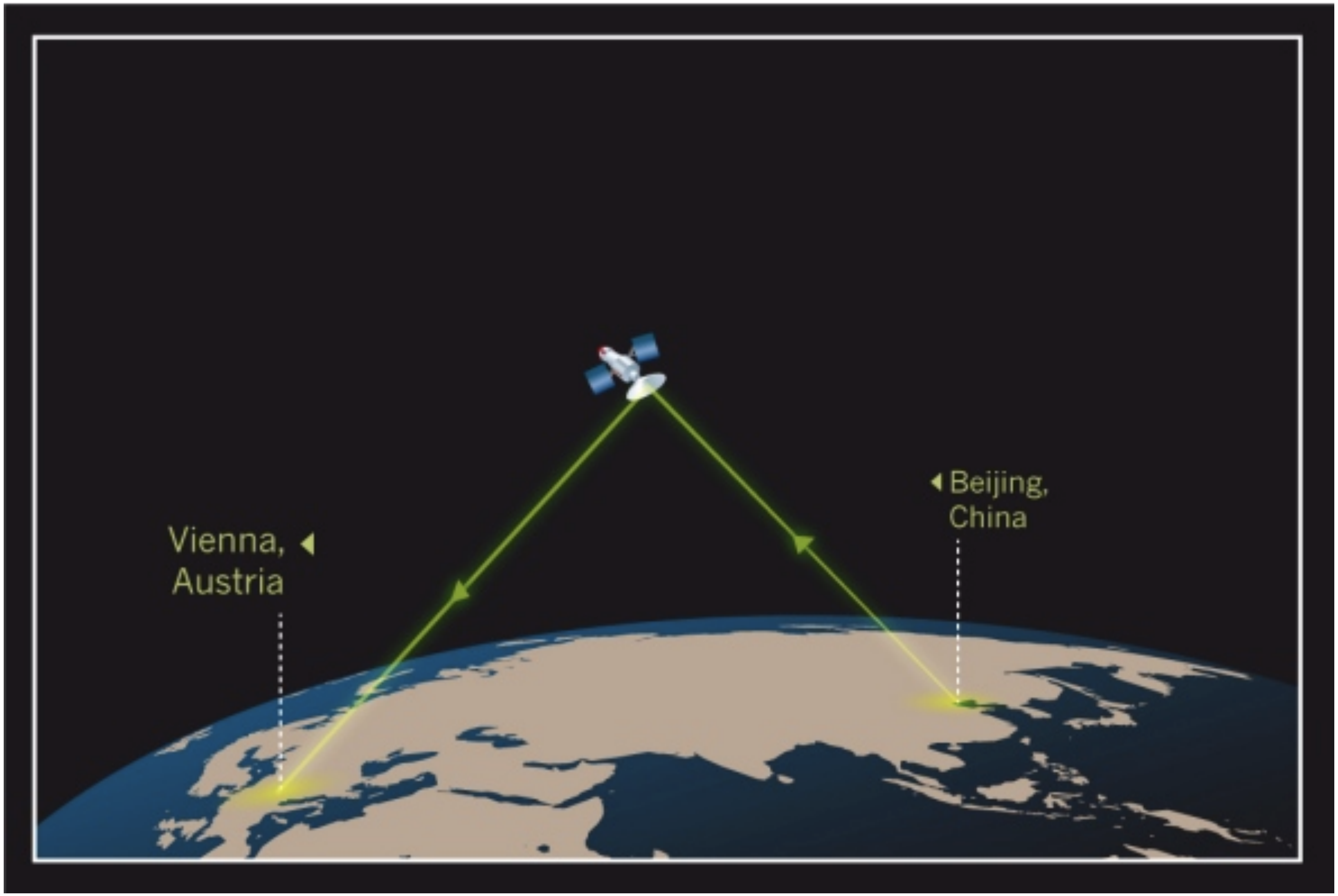
RESOURCE CENTRE

Quantum cryptography



Quantum cryptography

Satellite QKD

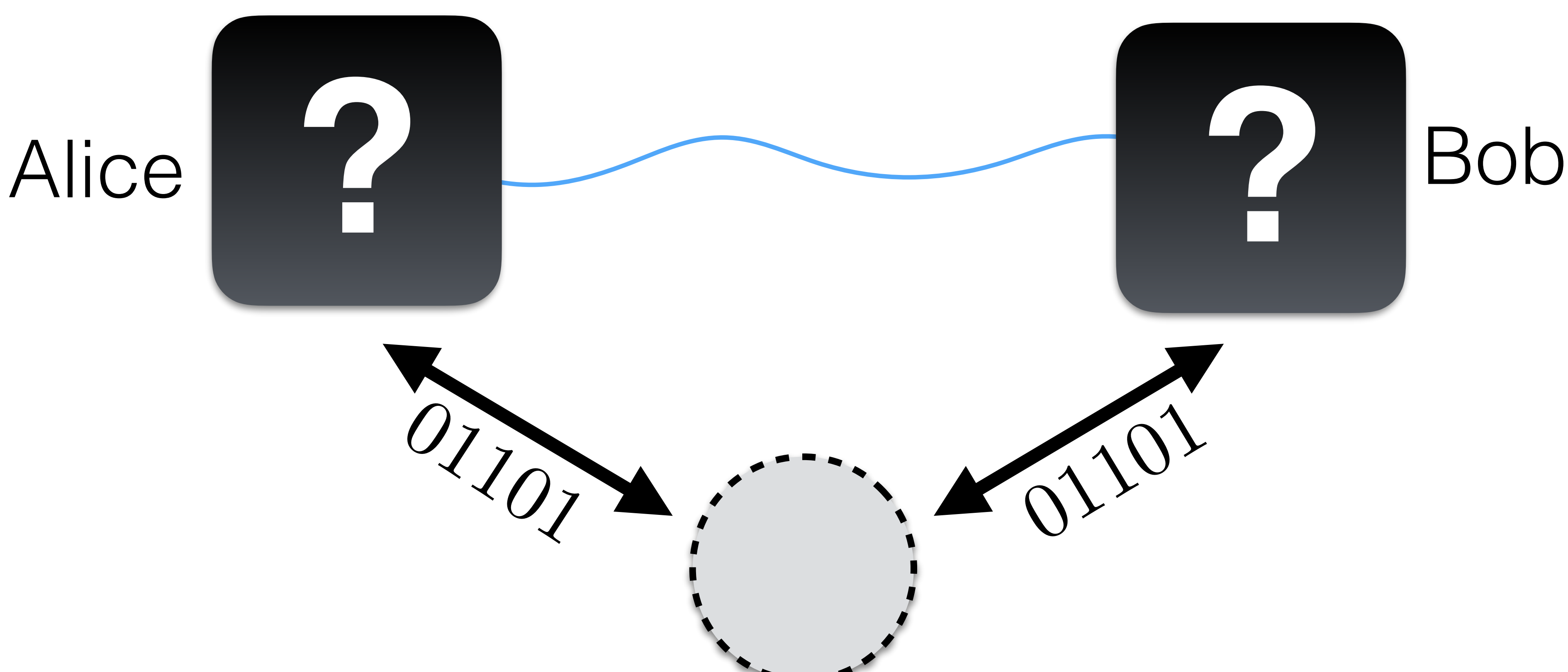


First QKD-based video conference
29th September 2017

Quantum cryptography

Entanglement → **non-local correlations**

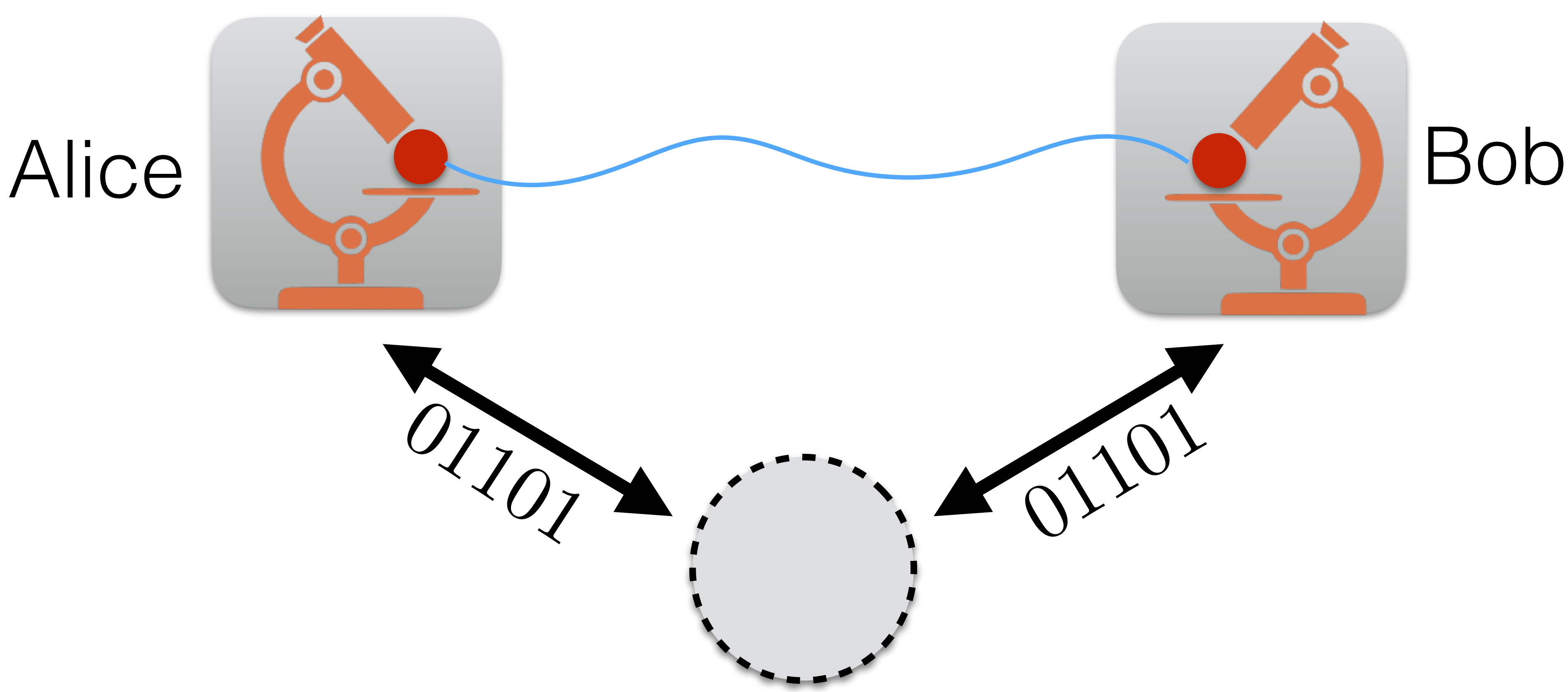
Non-local correlations → entanglement



Quantum cryptography

Entanglement → **non-local correlations**

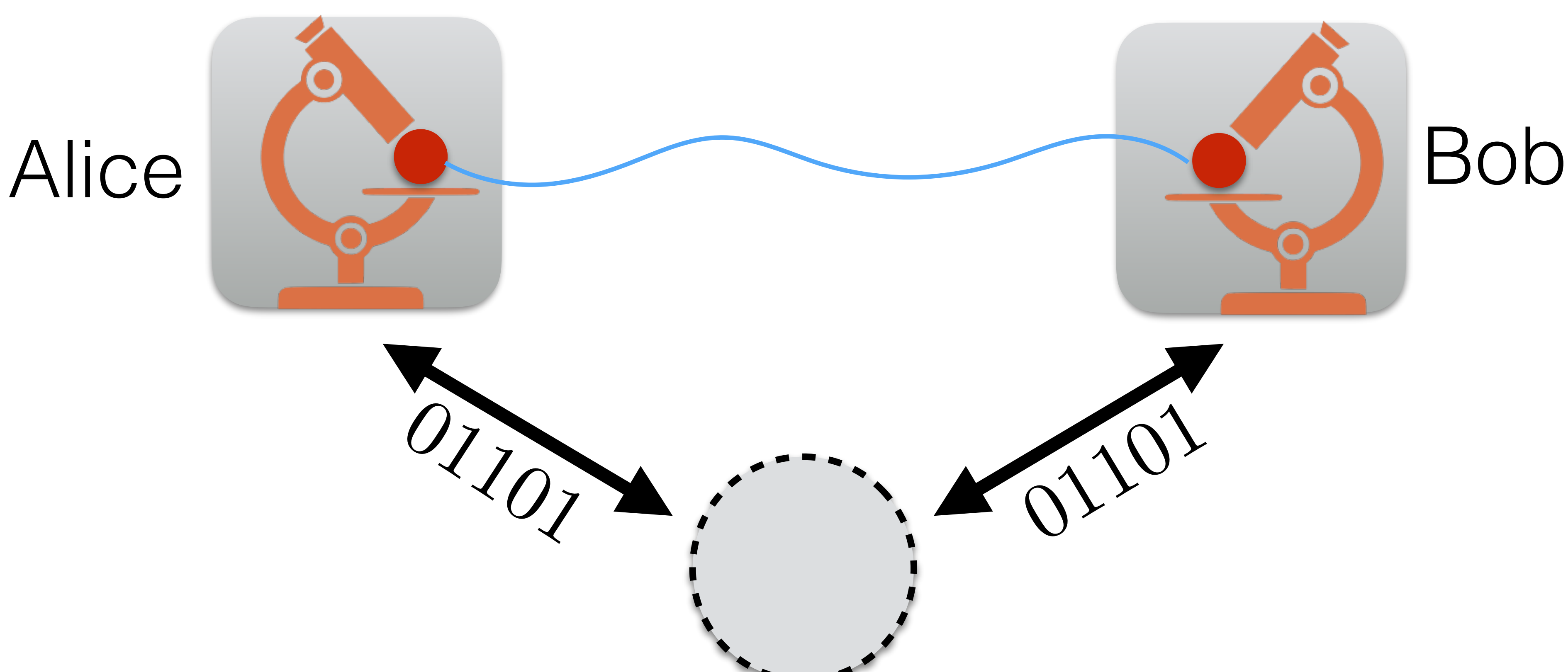
Non-local correlations → entanglement



Device-independent quantum cryptography

Entanglement → **non-local correlations**

Non-local correlations → entanglement



A brief history of quantum cryptography

- **1980s** - Ideas for quantum money and quantum key distribution. Wiesner, Bennett, Brassard.
- **1990s** - Idea for device-independent cryptography. Mayers, Yao, Ekert.
- **2000s** - First commercial quantum crypto devices; ideas for QDS, QRNG, blind quantum computation and others.
- **2010s** - Satellite QKD; QKD at long distances; experiments for device-independent protocols

Many many theoretical advances in security proofs

References and resources

Quantum computing since Democritus

http://www.scottaaronson.com/democritus/

https://www.amazon.co.uk/Quantum-Computing-since-Democritus-Aaronson/dp/0521199565/ref=sr_1_1?ie=UTF8&qid=1534772690&sr=8-1&keywords=quantum+computing+since+democritus

Quantum computation and quantum information

https://www.amazon.co.uk/Quantum-Computation-Information-10th-Anniversary/dp/1107002176/ref=sr_1_1?s=books&ie=UTF8&qid=1534772728&sr=1-1&keywords=nielsen+and+chuang

References and resources

Quantum computing courses

https://www.edx.org/course/quantum-information-science-i
https://www.edx.org/course/quantum-mechanics-quantum-computation-uc-berkeleyx-cs-191x
https://cs.uwaterloo.ca/~watrous/LectureNotes.html
http://www.theory.caltech.edu/people/preskill/ph229/

An awesome quantum physics course

https://www.youtube.com/watch?list=PLUl4u3cNGP61-9PEhRognw5vryrSEVLPr&v=lZ3bPUKo5zc

References and resources

Quantum crypto courses

https://www.edx.org/course/quantum-cryptography-caltechx-delftx-qucryptox-0
https://www.edx.org/course/quantum-internet-quantum-computers-how-delftx-qtm1x
https://courses.cs.ut.ee/all/MTAT.07.024/2015_fall/uploads/

Simulating physics with computers - R. Feynman

https://www.cs.berkeley.edu/~christos/classics/Feynman.pdf

Quantum simulation

https://www.sciencemag.org/content/273/5278/1073.abstract

References and resources

Quantum supremacy

https://www.technologyreview.com/s/610274/google-thinks-its-close-to-quantum-supremacy-heres-what-that-really-means/

https://www.nature.com/articles/nature23458

QKD stuff

https://www.idquantique.com/

https://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information/Quantum-Key-Distribution/Toshiba-QKD-system/

https://www.nature.com/articles/nature23655