Long-term Security
through
Quantum Cryptography

Dominique Unruh

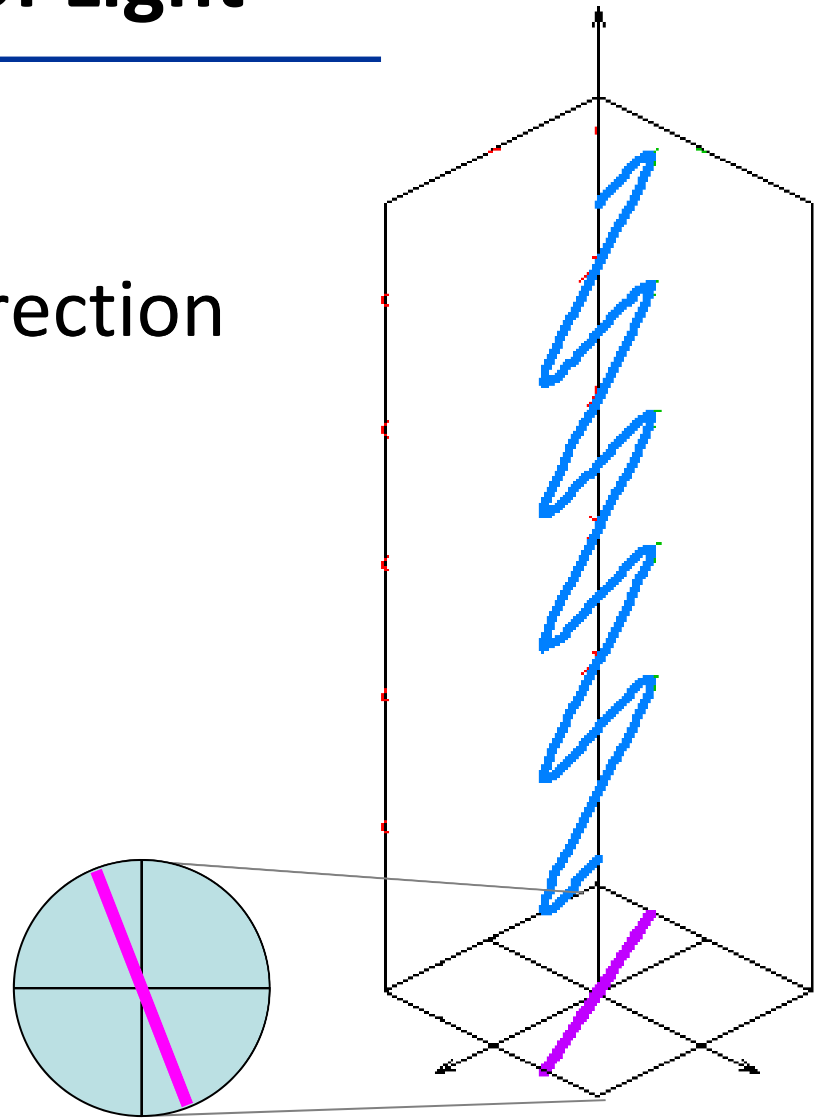
University of Tartu

Mathematics of QC:

The Qubit

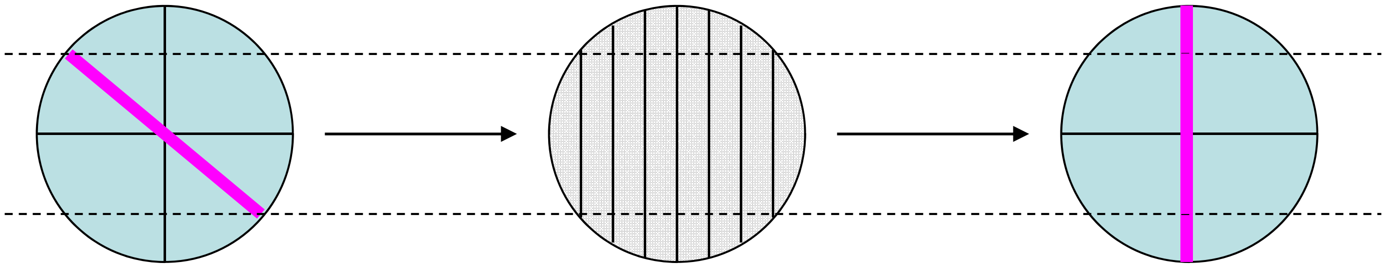
Polarisation of Light

- Light consists of waves
- Waves swing in a given direction (extreme simplification!)
- Direction = Polarisation



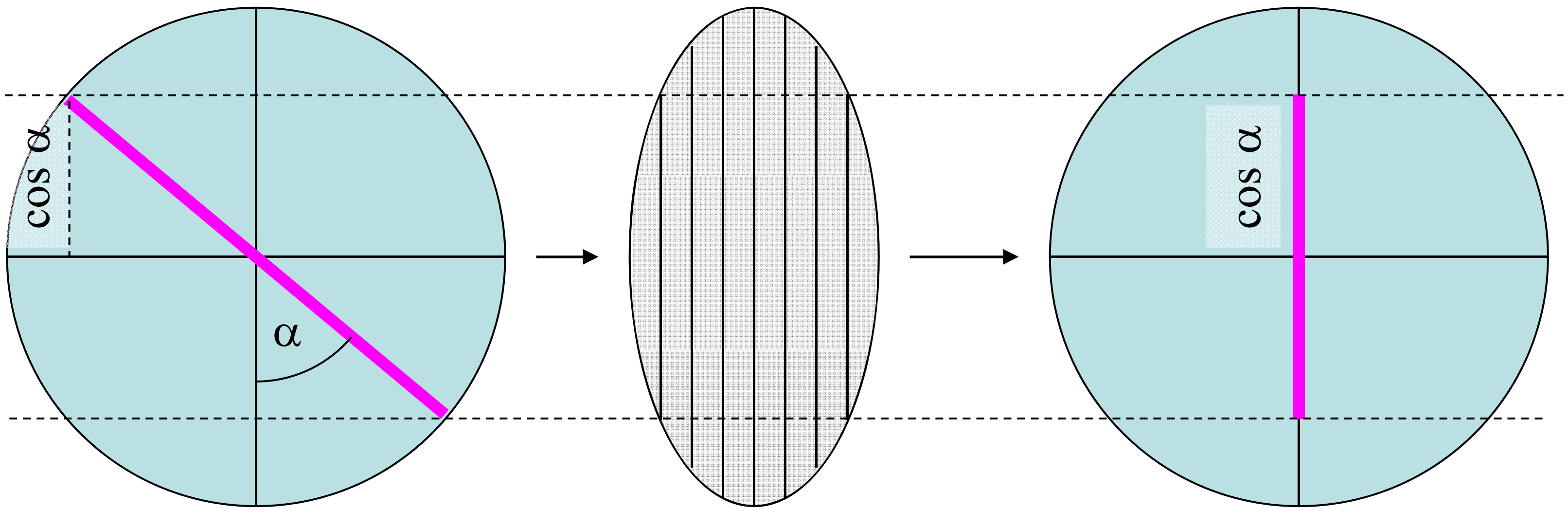
Polarising Filters

- **Polarisation filters** only let one polarisation through



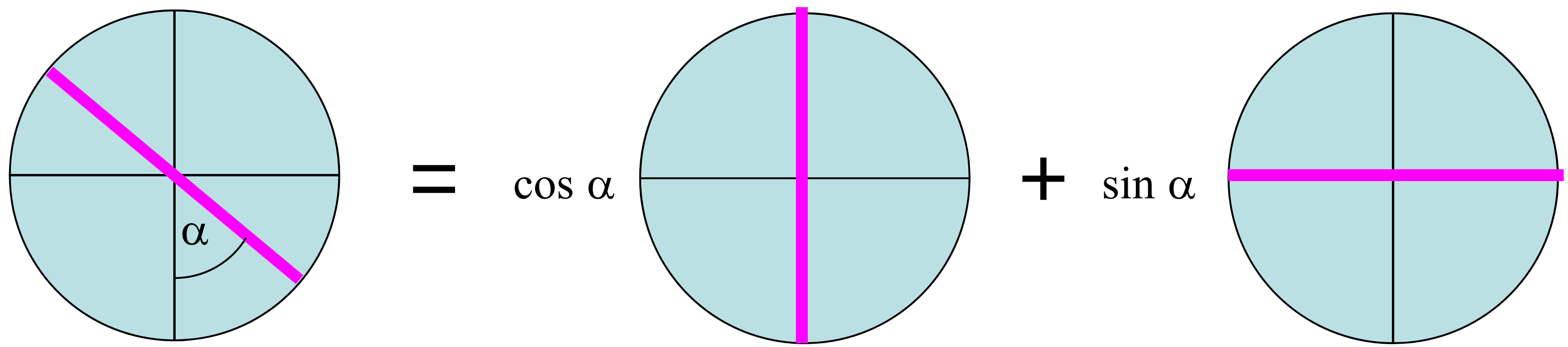
- Intensity of light is reduced
  - Only the part of the light parallel to the filter passes

Polarising Filters



- Amplitude of light multiplied with $\cos \alpha$
- α = Angle between polarization & filter
- Intensity = Amplitude^2
- Intensity of light multiplied with $(\cos \alpha)^2$

Polarising Filters



$$= \cos\alpha\,|\updownarrow\rangle + \sin\alpha\,|\leftrightarrow\rangle$$

- Polarising filter is linear transformation Φ:

$$\Phi|\leftrightarrow\rangle = 0$$

$$\Phi|\updownarrow\rangle = |\updownarrow\rangle$$

Polarising Single Photons

- Single photon has no amplitude/intensity
- It's there or not
- Intensity = Number of photons
- What happens in a polarising filter?

$$\beta\left|\updownarrow\right\rangle + \gamma\left|\leftrightarrow\right\rangle \quad\mapsto\quad \begin{cases} \left|\updownarrow\right\rangle & \text{with probability } \beta^2 \\ \text{nothing} & \text{with probability } \gamma^2 \end{cases}$$

Polarising Single Photons

- General rule :
  - Compute angle and amplitude of result
  - Probability of surviving photon
    = Amplitude^2 = Intensity
  - Renormalize amplitude to 1

$$\beta\left|\updownarrow\right\rangle+\gamma\left|\leftrightarrow\right\rangle$$

$$\mapsto \quad \beta\left|\updownarrow\right\rangle$$

$$\mapsto \quad \begin{cases} \left|\updownarrow\right\rangle & \text{with probability } \beta^2 \\ \text{nothing} & \text{with probability } 1\text{-}\beta^2=\gamma^2 \end{cases}$$

The Qubit

- Polarisation is example of qubit
- Other examples:
  - Atom is in excited state or not
  - Which way information in beam splitter
  - Any superposition of two possibilities (cats?)

Mathematics of QC:

Larger Systems

~~Recap: One Qubit~~ n Qubits

- State: Complex linear combination (length 1) of basis vectors ~~$|0\rangle$ and $|1\rangle$~~
  $|x\rangle$ for each bitstring x

  (Dimension: 2^n)

- Operations: Linear, length-preserving ops on the state (= unitary ops) ✓

Recap: Measurements on ~~One Qubit~~ n Qubits

- Describing the measurement (of $|\Phi\rangle$):
  ~~Two orthogonal vectors $|\Psi_0\rangle$ and $|\Psi_1\rangle$~~
  (polarization directions) **Many orthogonal subspaces V_i**

- Probability of outcome i:
  - Project $|\Phi\rangle$ ~~onto $|\Psi_i\rangle$~~ **onto V_i** $\rightarrow$ $|\Phi\rangle$
  - Prob = Square of length of $|\Phi\rangle$ ✓

- Post-measurement-state: $|\Phi\rangle$ (normalized) ✓

Quantum Mechanics are “simple”

- The last two slides capture the essence of quantum mechanics
- Mathematically simple model → Nice
- But: Many strange consequences and deep results

Example: Bell pairs

- Consider the state $|\Phi\rangle := (|00\rangle + |11\rangle) / \sqrt{2}$ (superpos. between two 0-bits and two 1-bits)
- We measure whether the first bit is 0.
- $V_{yes} = [|00\rangle, |01\rangle], \quad V_{no} = [|10\rangle, |11\rangle]$
- Project $|\Phi\rangle$ onto V_{yes}: $\quad |00\rangle / \sqrt{2}$
- Length: $1/\sqrt{2} \quad \Rightarrow$ Probability(yes) = $1/2$
- Post-measurement-state: $|00\rangle$

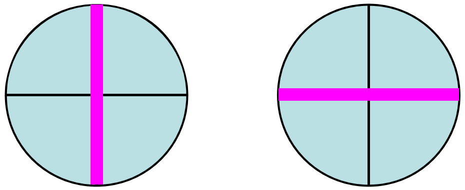
Example: Bell pairs (II)

- Post-measurement-state: $|00\rangle$
- Measuring second bit: yields 0 with prob. 1

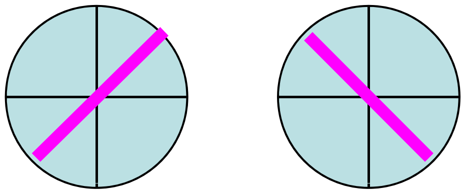
- When measuring the two bits in a Bell pair: Result is random, but the same!
- Even if the bits are in different places
  → Non-local behavior
- The bits are "entangled"

Example: Bell pairs (III)

- Remember: A single qubit can be measured in different "directions"
- $|0\rangle, |1\rangle$ is the so-called "computational basis"



- $|+\rangle, |-\rangle$ is the so-called "diagonal basis"
- $|+\rangle = (|0\rangle + |1\rangle) / \sqrt{2}$
- $|-\rangle = (|0\rangle - |1\rangle) / \sqrt{2}$



Bell pairs (IV)

- Measuring Bell pair in diagonal basis also leads to same result on both bits

- Either $++$ or $--$

- Both qubits give the same answer when asked the same question