

# Quantum Computing & Cryptography

Steve Vickers

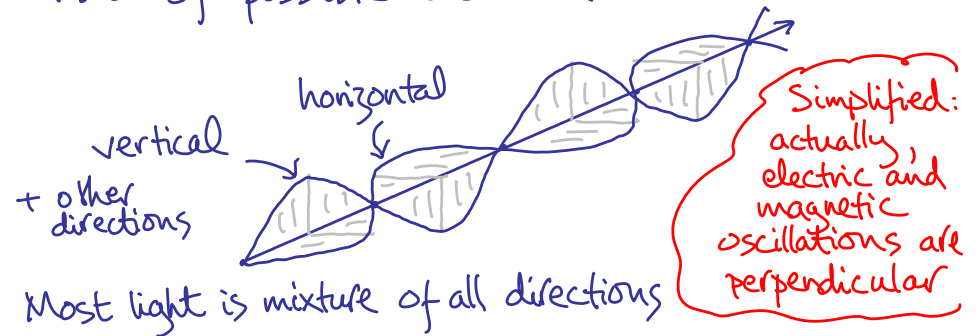
2011

## Non-examinable introduction

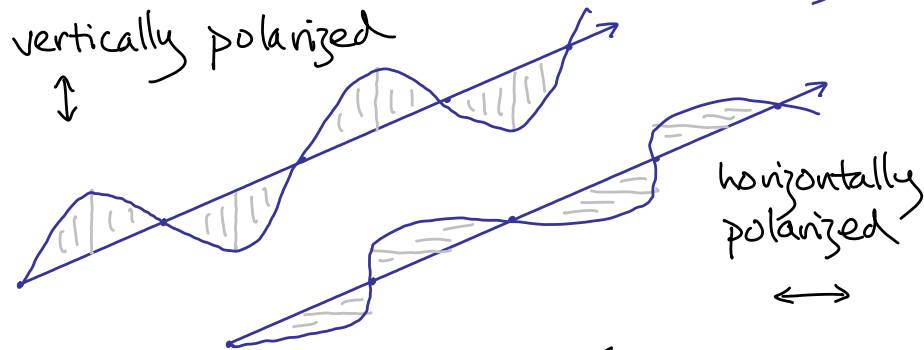
- Quantum key distribution
  - already in use, with polarized photons
  - quantum physics  $\Rightarrow$  no passive eavesdropping
- Quantum computers
  - no practical ones yet
  - quantum physics  $\Rightarrow$  clever probabilistic algorithms
  - no efficient classical simulation
  - Shor's factorization algorithm would break RSA

## Light as waves

= vibrations in electromagnetic field  
transverse to direction of travel  
180° of possible vibration directions



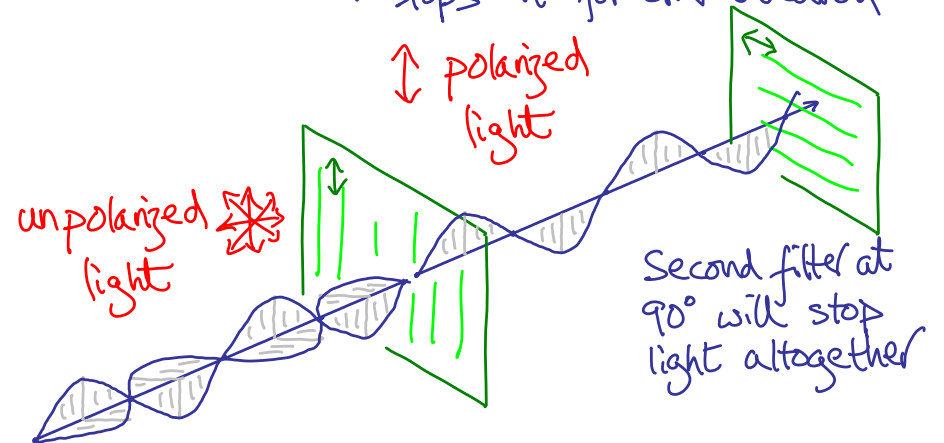
## Polarized light - only oscillates in some directions



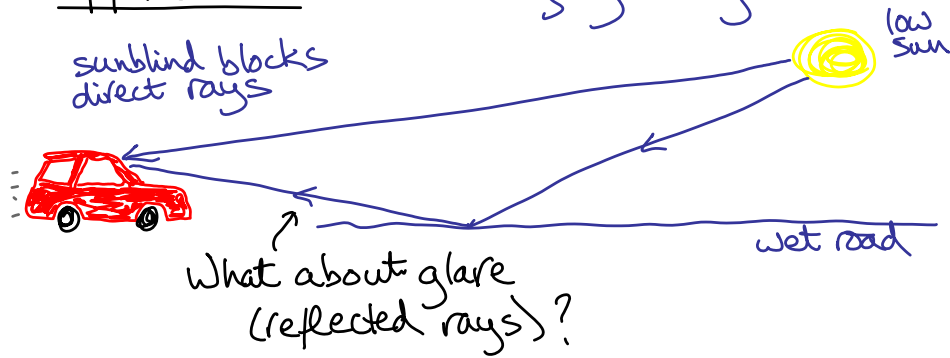
Also: diagonally polarized ↗ ↘ etc.  
Also: circularly polarized - direction rotates ↻ ↺

## Polarizing filter

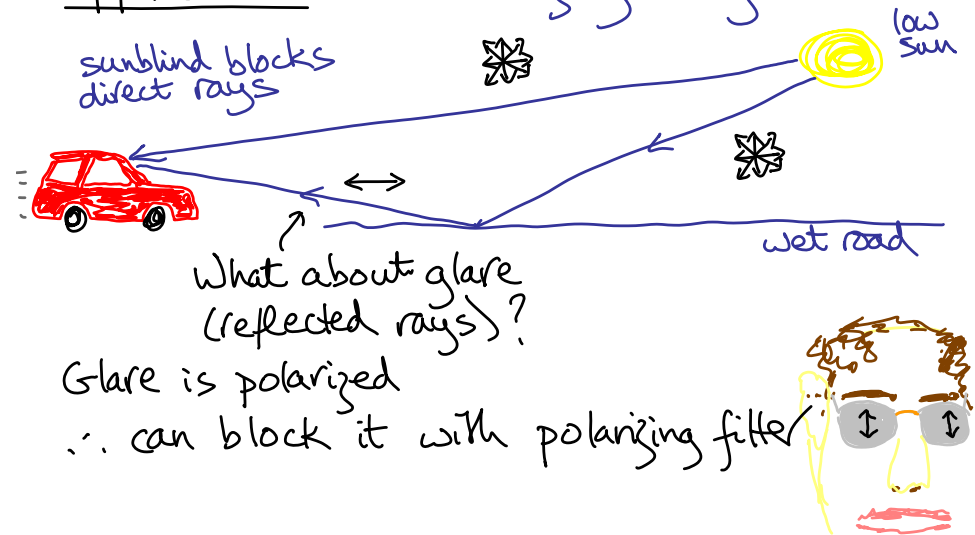
- passes light vibrating one direction
- stops it for other direction



## Application Polarizing sunglasses



## Application Polarizing sunglasses



## Another application 3D cinema

Want left & right eyes to see slightly different pictures  $\Rightarrow$  illusion of depth

- Two pictures mixed together, with opposite circular polarizations  $\odot$   $\ominus$
- Wear glasses with circular polarizing filters

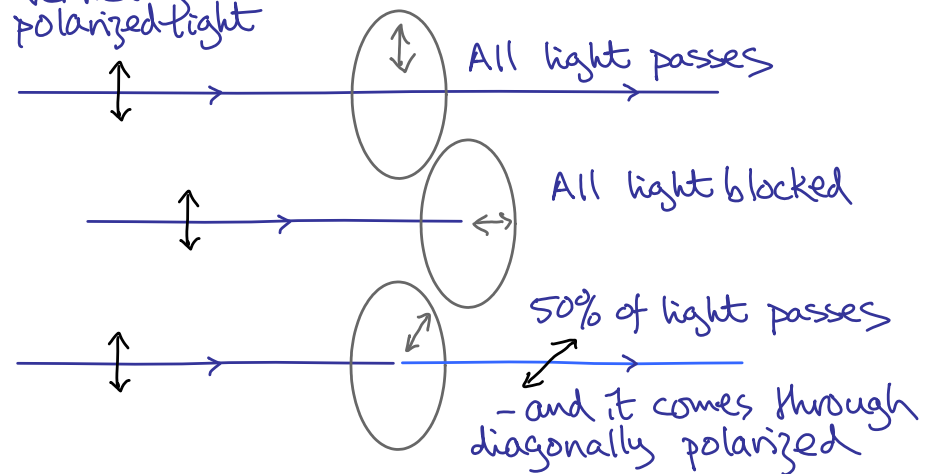
Why circular?



## Interesting phenomenon

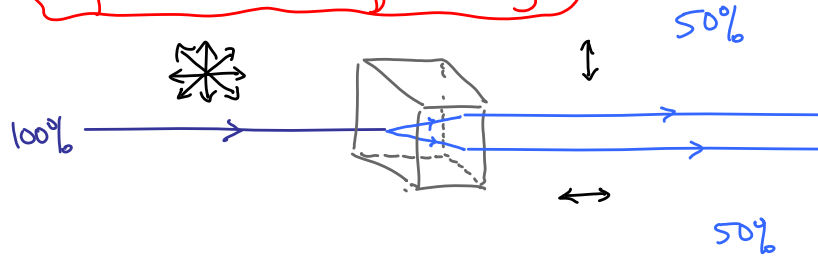
Vertically polarized light

Filter in various orientations



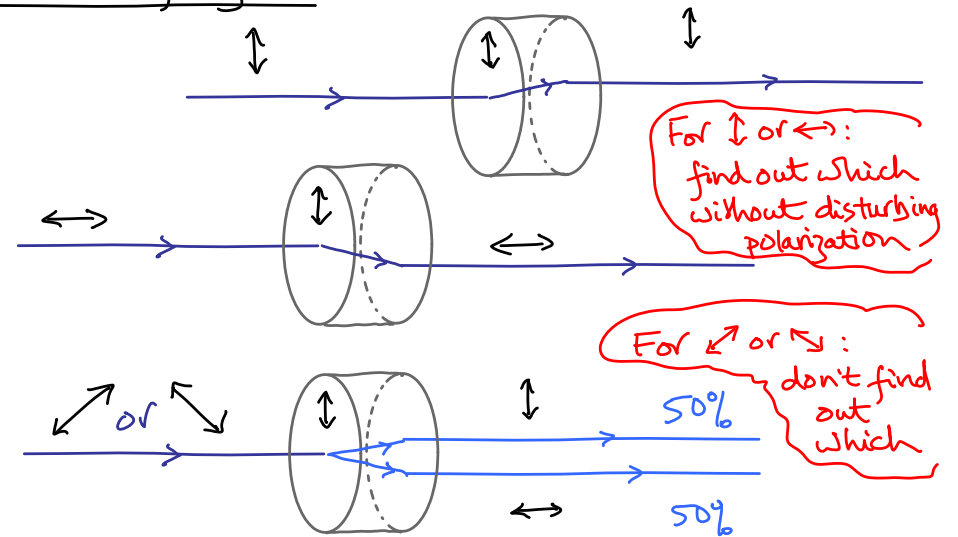
## Birefringent crystals

refract in two different ways



input splits into two polarized beams

## For birefringence:



## Photons Light comes in particles (quanta)

How do we know?

e.g. photo cells



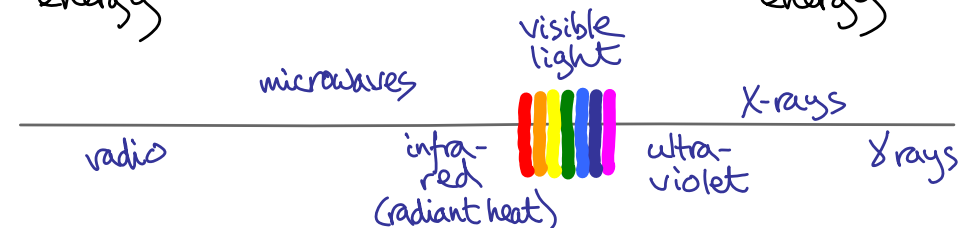
Input light must be at least a certain frequency - or no electricity out (no matter how bright light is)

## Explanation (Einstein)

- Light comes in particles (photons)
- Energy of each photon depends on frequency
- Need photons of at least a certain energy to dislodge electrons & make electricity

Low frequency, energy

High frequency, energy



## Weird

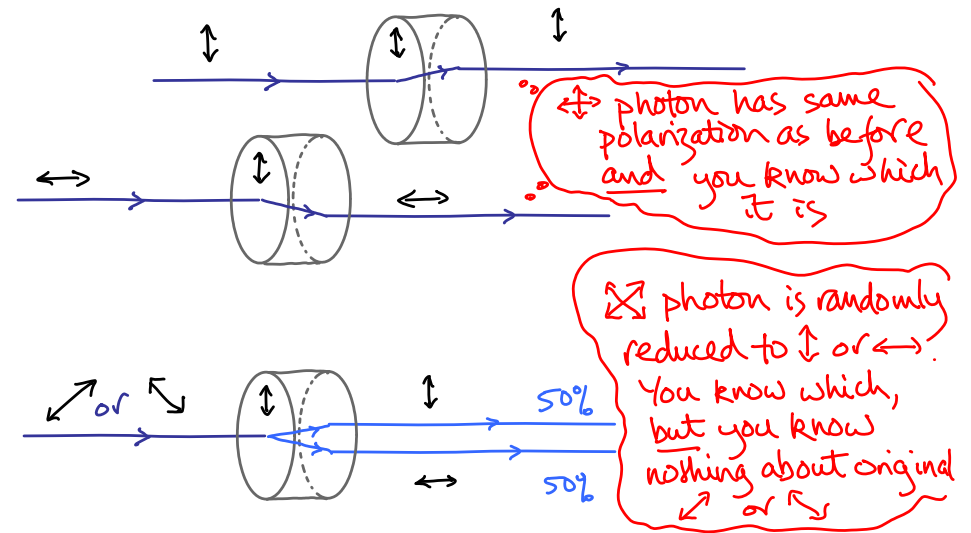
Photons still behave like waves  
 e.g. polarization  
 each photon has its own polarization state

Also e.g. diffraction

Waves can form interference patterns  
 A photon can interfere with itself  
 - probabilistic behaviour

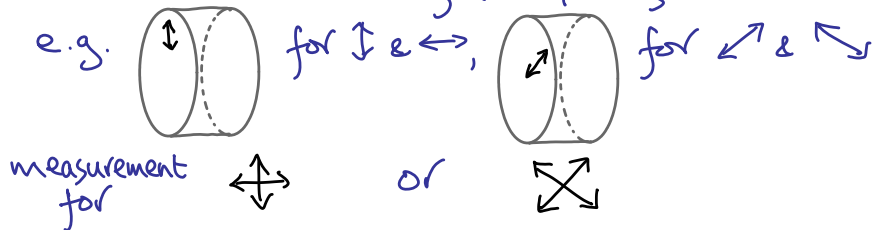
constructive } interference = { high } probability  
 destructive } { low }

## Single polarized photon & birefringent crystal

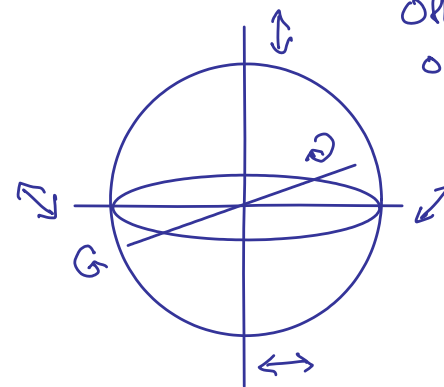


## Measurement

To find a photon's polarization state you measure it  
 - e.g. pass it through birefringent crystal, see where it comes out  
 BUT each orientation of crystal measures only two polarization states



## Range of polarization states - lie on sphere



Other points correspond to other polarization orientations

Infinitely many possible states, but ...

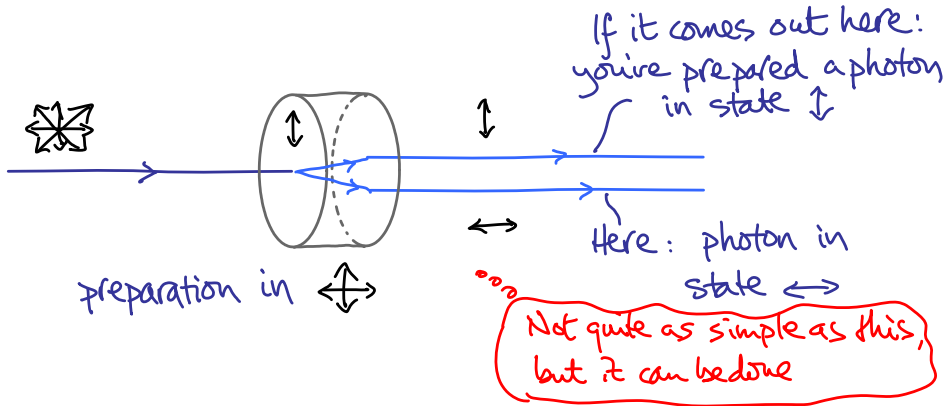
to measure you must choose an axis & accept one of only two possible results

∴ like a bit

Polarized photon is a quantum bit = qbit

## Preparation

Also to prepare a photon in a known state: measure it!  
Result says what its state is now.



## Quantum key distribution

BB84 =  
Bennett & Brassard  
1984

- Use polarized photons to share a private key
- Any eavesdropping disturbs polarization in way that can be detected no passive eavesdropping
- Technology already exists
  - generate single photons sometimes 0 or 2 - allow for that
  - manipulate their polarizations
  - transmit - fibre optics or open air

## Protocol

$\updownarrow, \nearrow$  encode 0  
 $\leftrightarrow, \nwarrow$  encode 1

- Alice prepares a string of photons
  - chooses  $\leftrightarrow$  or  $\nwarrow$  at random to prepare each one
  - sends them all to Bob
- Bob measures each for (at random)  $\updownarrow$  or  $\nwarrow$
- They tell each other what preparation / measurement types they used for each photon
- Where types disagree, photon is wasted
- Where they agree, a bit has been communicated securely

e.g.

Alice prepares		Bob measures		bit
state	type	type	state	
$\updownarrow$	$\leftrightarrow$	$\leftrightarrow$	$\updownarrow$	0
$\updownarrow$	$\leftrightarrow$	$\times$	random	X
$\nwarrow$	$\times$	$\times$	$\nwarrow$	0
$\nwarrow$	$\times$	$\times$	$\nwarrow$	1
$\nwarrow$	$\times$	$\leftrightarrow$	random	X

shared insecurely      Good bits = secure key = 001

## Eavesdroppers

- Eve cannot measure photons and send them on to Bob unchanged
  - To measure them she must guess whether Alice used  $\leftrightarrow$  or  $\nwarrow$
  - Wrong guess  $\Rightarrow$  messes up the polarization state
  - Alice and Bob can detect this statistically if they tell each other the states of some test photons as well as the types
- those photons won't be available for the key

Test photons Alice, Bob tell each other types and results.

e.g. Alice prepares  $\downarrow$ , Bob measures type  $\leftrightarrow$   
- Bob should always get same result  $\downarrow$

Eve guesses type:

- 50%  $\leftrightarrow$  - she always gets result  $\downarrow$ , retransmits  $\downarrow$  to Bob, no detectable difference
  - 50%  $\nwarrow$  - she gets result  $\leftarrow$  or  $\rightarrow$  at random, retransmits  $\leftarrow$  or  $\rightarrow$  to Bob
- Bob measures result  $\downarrow$  or  $\leftrightarrow$  at random  
25% of time Bob measures  $\leftrightarrow$  Alice & Bob see there's a problem

## Quantum computer/science

- Use techniques of quantum theory to analyse protocols like BB84 (polarized photons implement qubits, "quantum bits")
  - Exploit "entanglement" between qubits (e.g. Ekert E91 protocol)
  - Quantum computers
    - still only theoretical
    - important algorithms already designed
- These have been implemented
- Not implemented yet

## Quantum computer qbits

Uses quantum bits instead of ordinary bits

- Each has continuous range of states
  - like polarization of photon
  - various ways to measure (read) it
  - but only two possible results (like ordinary bit)

Computation: various operations, then measure  
- essentially probabilistic, but can still get tight results

Hard to build! e.g. photons won't stay still.

## Shor's algorithm

- Efficient quantum algorithm to factorize large numbers
- Works by clever use of number theory and Fourier transform
- Probably get answer quickly - & then can check it.
- Existing quantum computer to factorize 15
- We're nowhere close to scaling it up yet
- If we do, it will break RSA

## Quantum computing & cryptography

- Basic principles of quantum mechanics
- A selection of quantum algorithms & protocols
- Principles & consequences of quantum cryptography
- Prospects for future progress

### Main text book

Quantum Computer Science: An Introduction  
David Mermin  
Cambridge University Press 2007