

Using Physics to create an Unbreakable Code

Prof. Miles Padgett FRSE
Dept. Physics and Astronomy
University *of* Glasgow
m.padgett@physics.gla.ac.uk

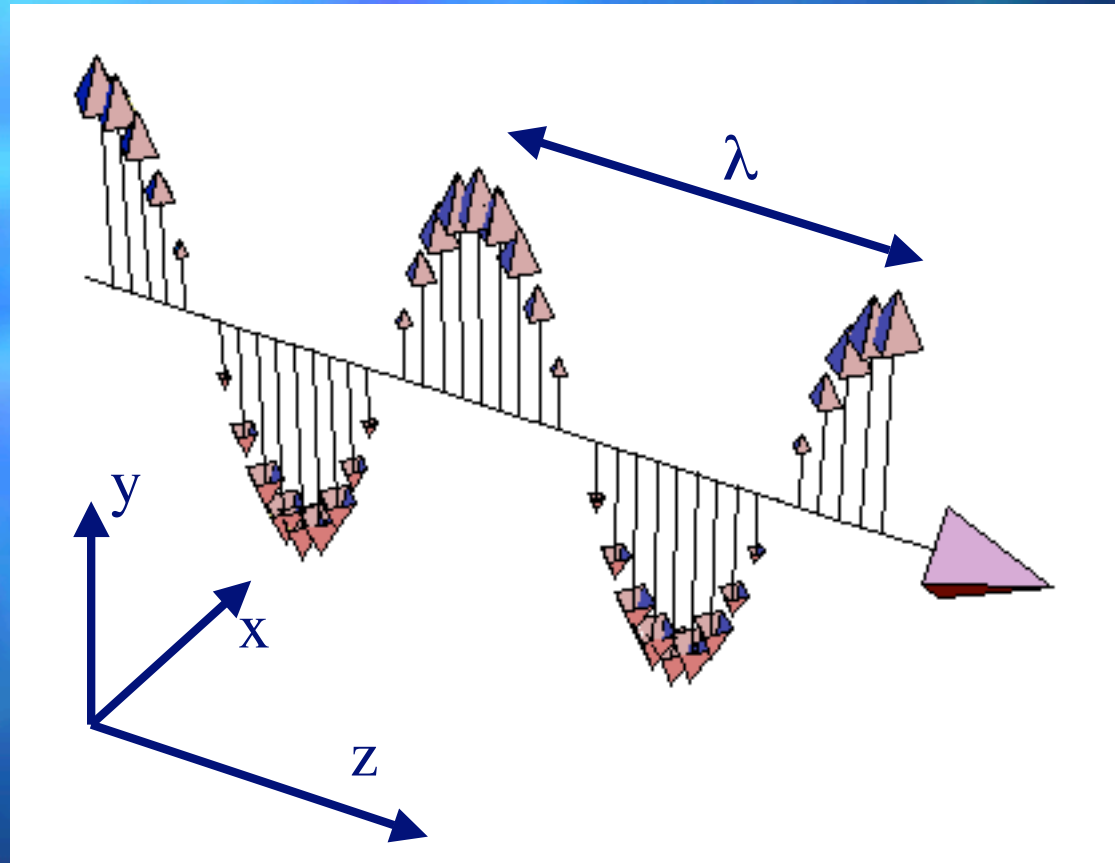
.....otherwise known as

- Quantum cryptography
- Quantum encryption

What is Light?

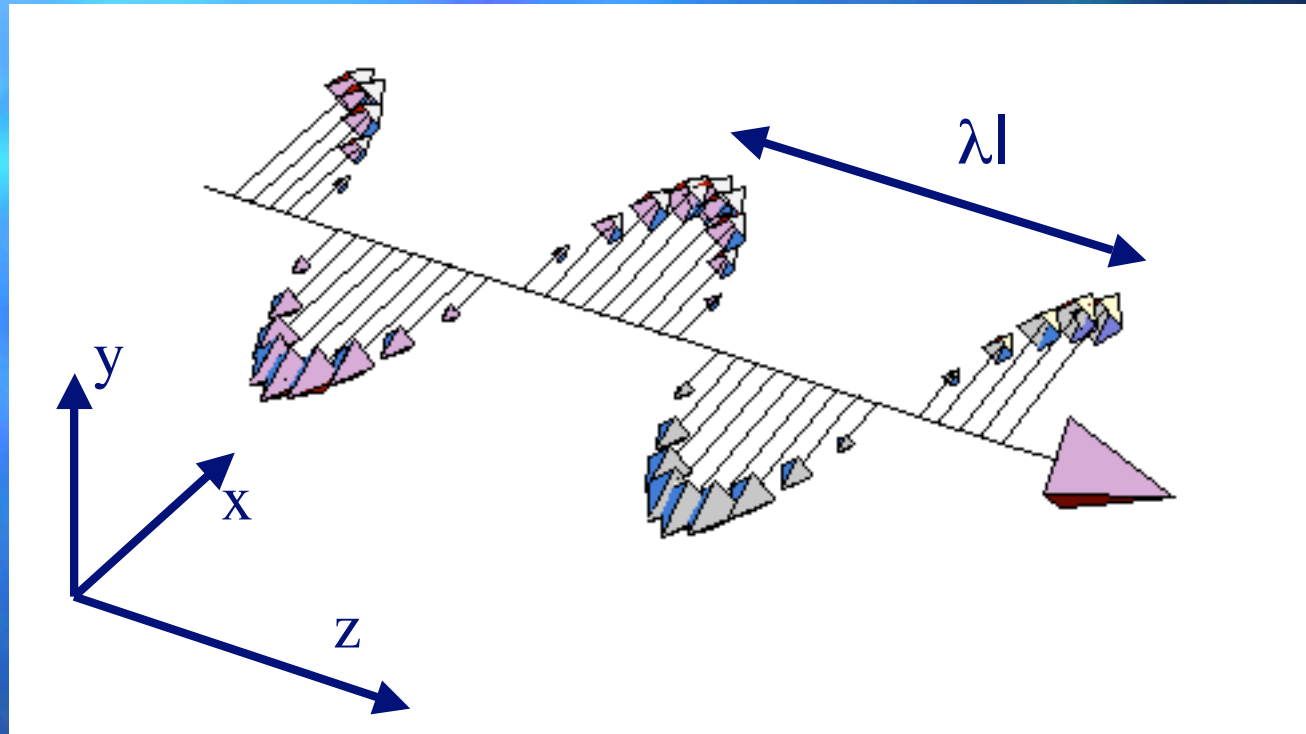
- Light is a “transverse wave” of the electromagnetic field
- Light is also a stream of photons
- For green light
 - wavelength, $\lambda \approx 0.0005\text{mm}$
 - frequency, $f \approx 6 \times 10^{14}\text{Hz}$
 - A one watt laser beam is 3×10^{18} photons per second

y-linear polarisation



■ $E_y = E_0 \cos(\omega t - kz),$ $(\omega = 2\pi f, k = 2\pi/\lambda)$

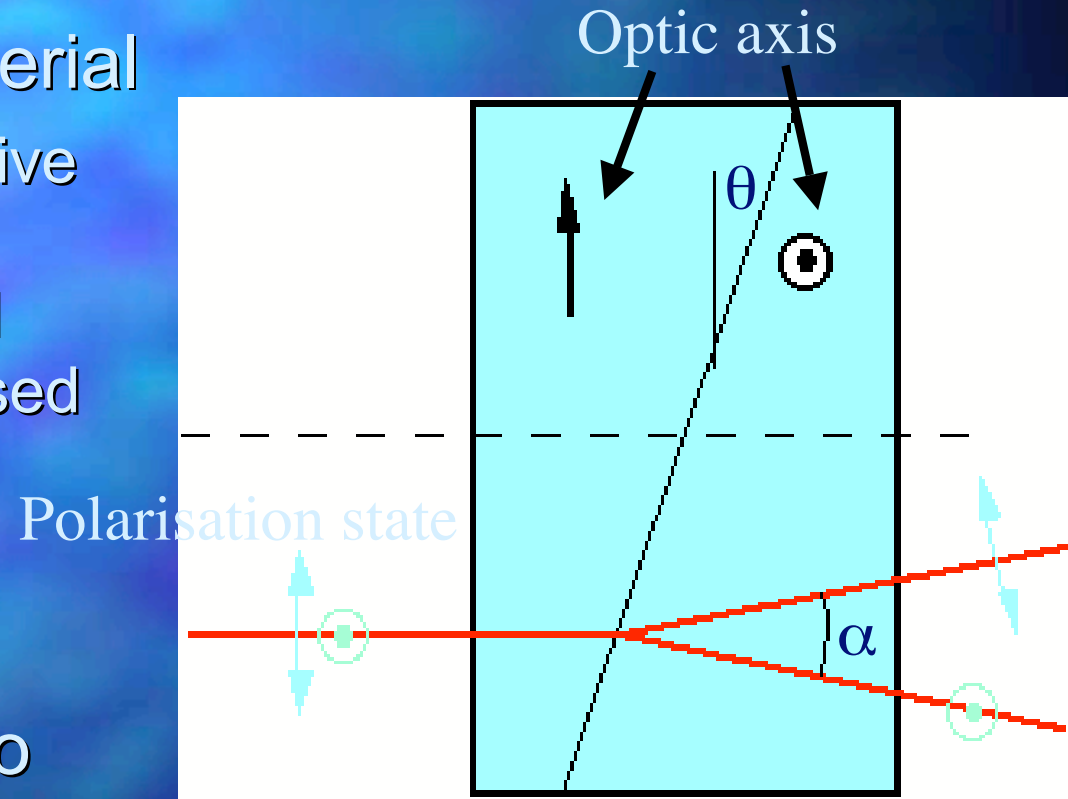
x-linear polarisation



■ $E_x = E_0 \cos(\omega t - kz),$ $(\omega = 2\pi f, k = 2\pi/\lambda)$

Measuring polarisation

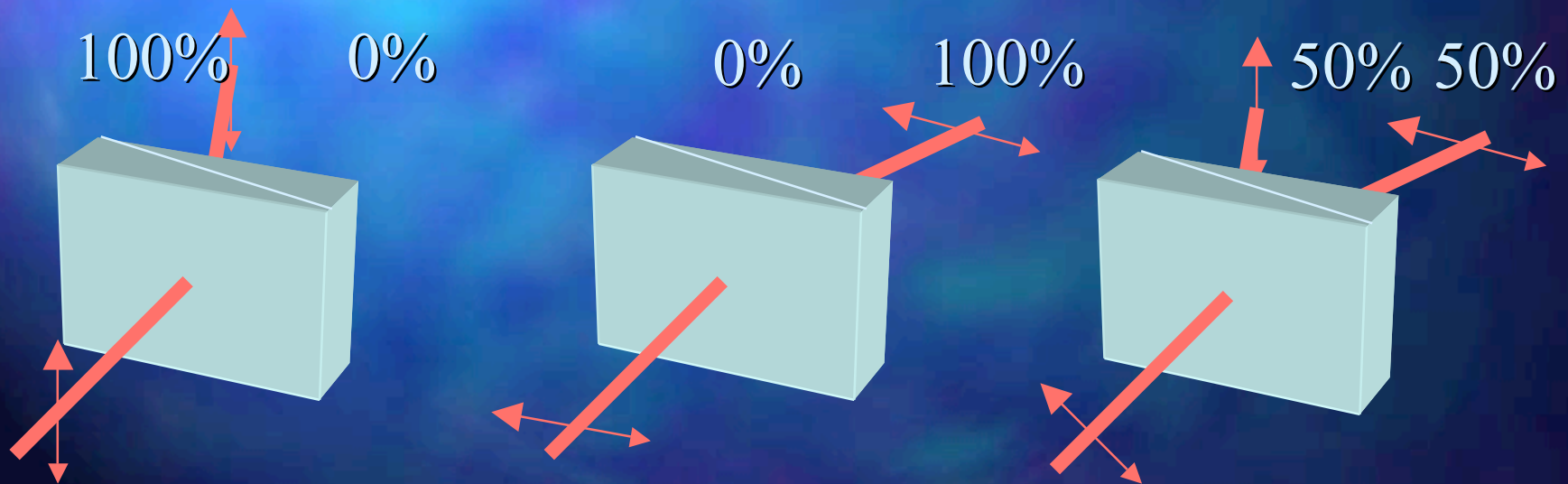
- Birefringent material
 - Different refractive indices for horizontally and vertically polarised light
- Wollaston splits orthogonal polarisations into separate paths



$$\alpha = 2 (n_{\text{high}} - n_{\text{low}}) \tan\theta$$

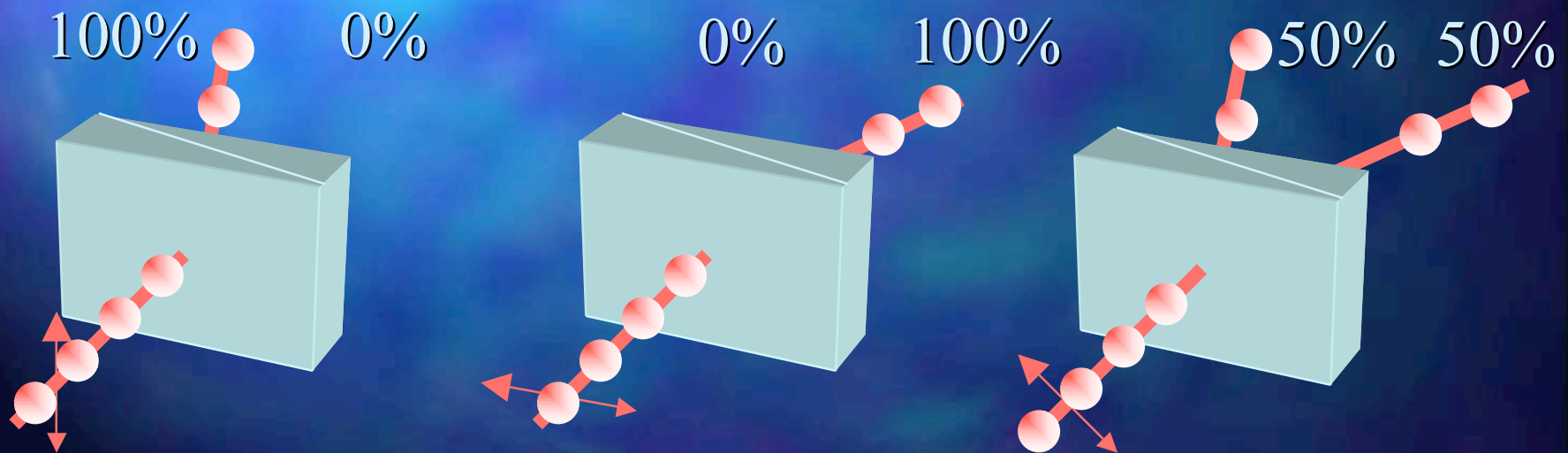
Measuring polarisation (demo)

- A polarising beam splitter separates horizontally from vertically polarised light
- Light polarised at 45° is split 50/50



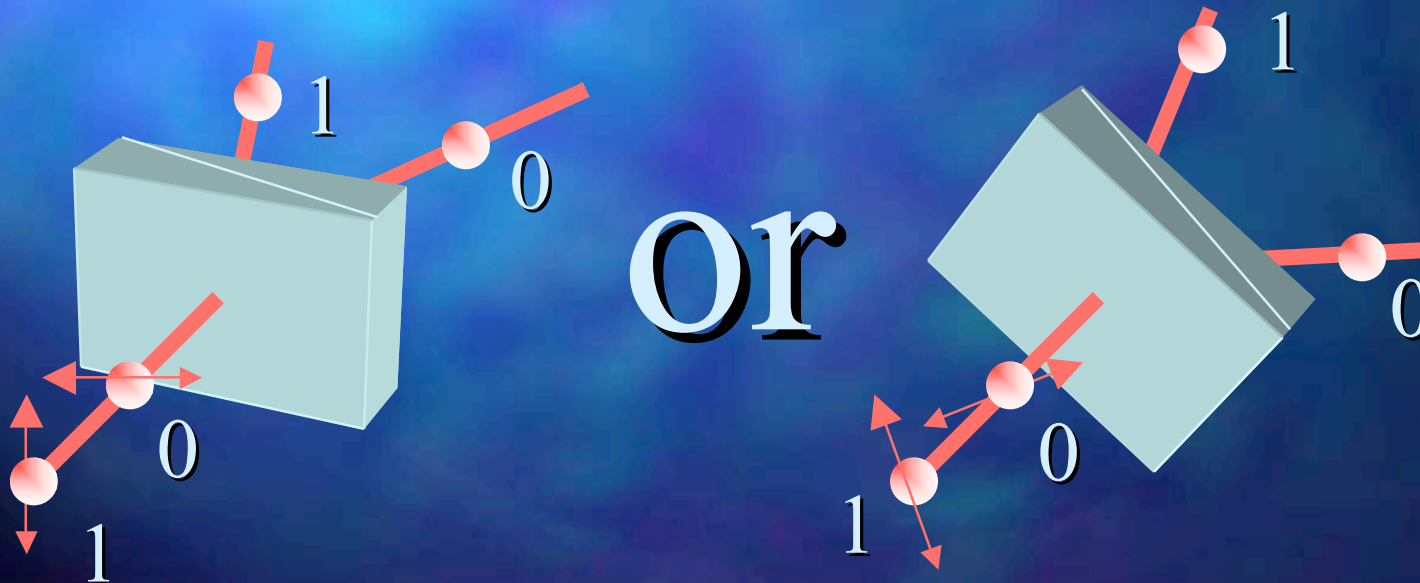
Polarisation of single photons

- Single photons are also polarised
 - one photon per second $\approx 1 \times 10^{-18}$ watts!
- Beam splitter still separates photons
- If polarised at 45° then 50/50 chance which way the photon goes





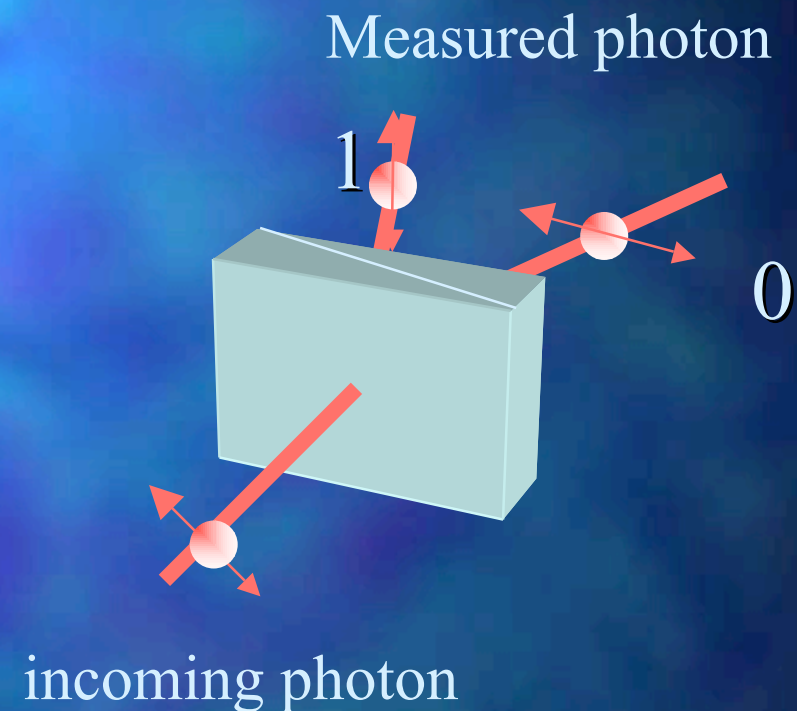
Sending data using photons

- Two polarisation states allows 0's and 1's to be transmitted
- But must decide on which direction to call horizontal



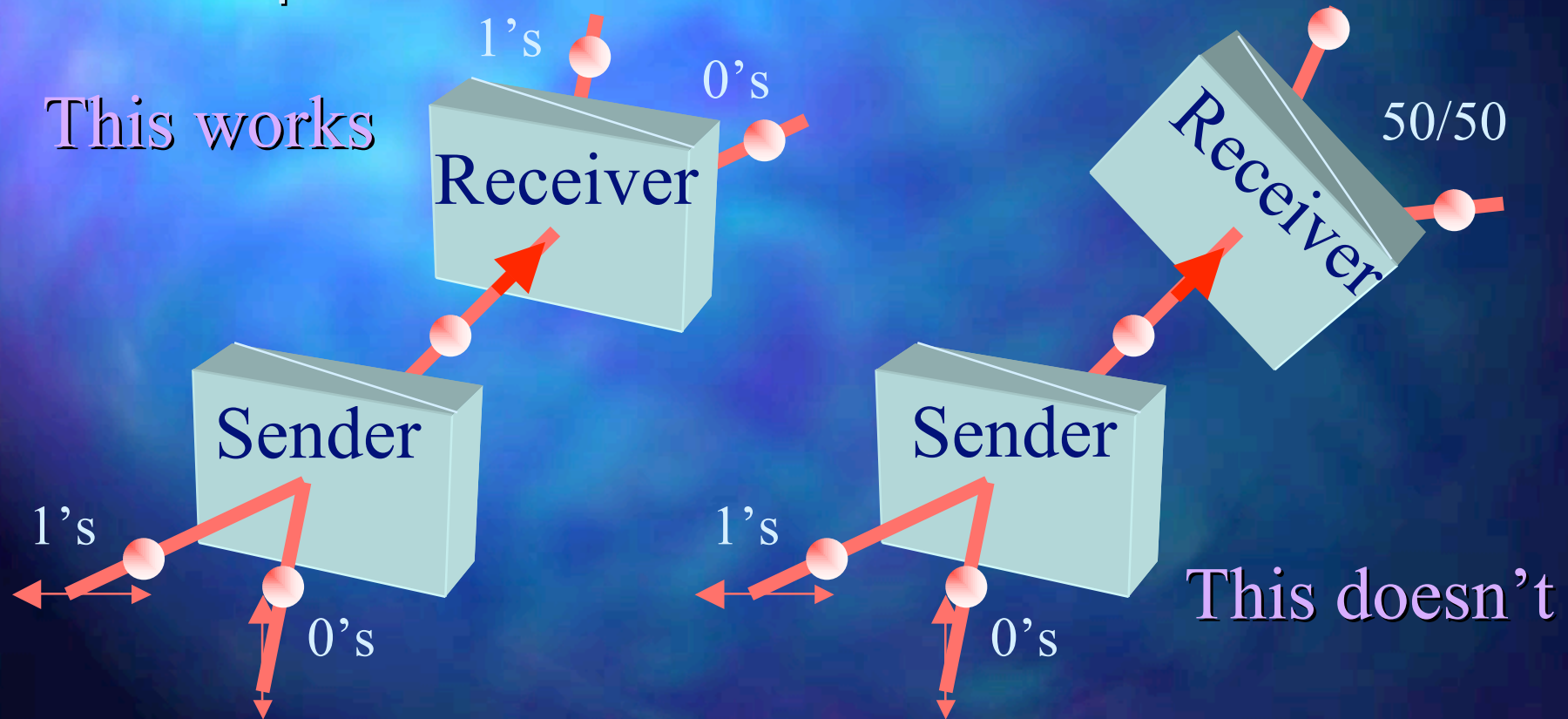
The polarisation of single photons is defined by measurement

- Measuring the photon sets its polarisation state
 - If 1 then 
 - If 0 then 
- Once measured all info about the “real” initial state is lost



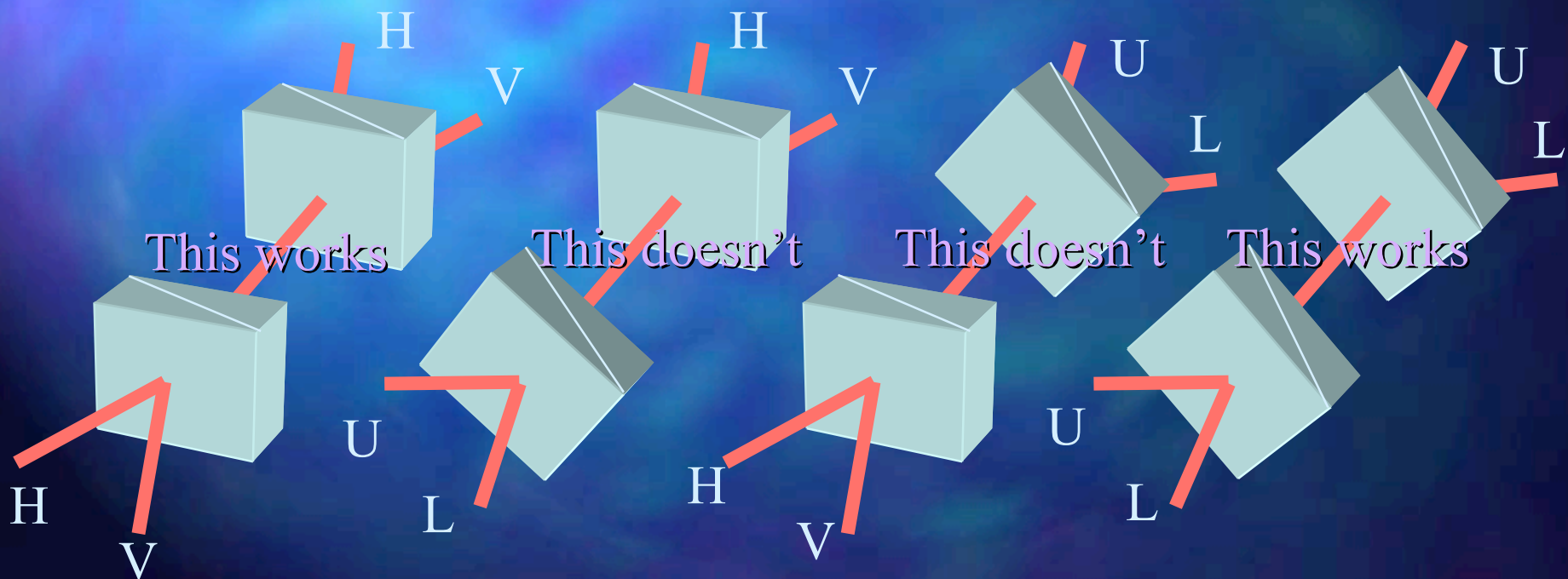
Reaching Agreement

- Sender and receiver must agree which way is up!



Mix and match at both ends

- Sender and receiver randomly decide to use horizontal & vertical or the diagonals (U, L)
- 50% of the time the 1's and 0's get mixed up



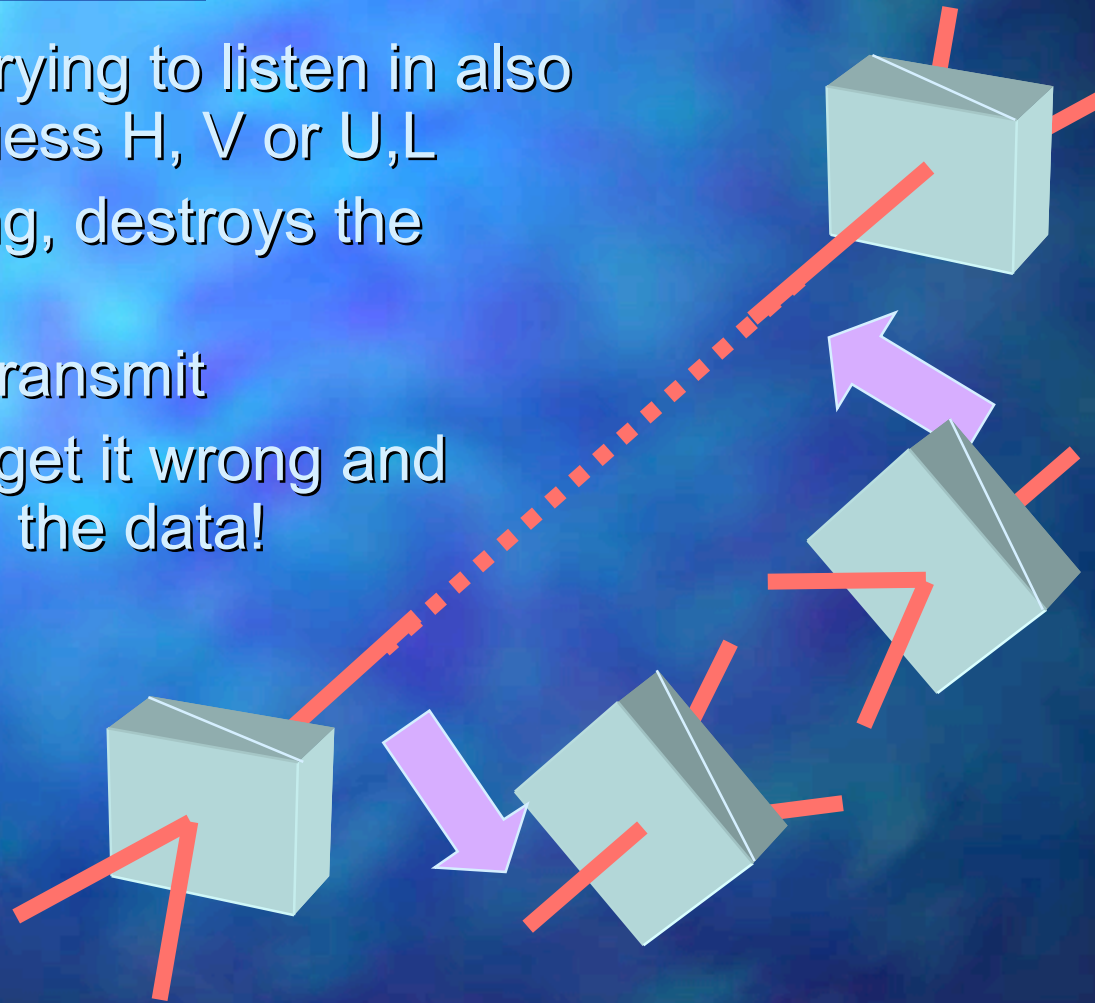
At the single photon level

- Sender and receiver randomly change between H, V and U, L
 - with single photons they can only do one or the other
 - 50% of the time they get it wrong - data get scrambled
- After transmission sender and receiver agree which data should have been good and which not

	sender				receiver			
	H	V	U	L	H	V	U	L
Good data			1	0			1	0
	0	1					1	0
Good data	1	0			1	0		
			0	1	0	1		
	1	0					1	0
Good data	1	0			1	0		

Trying to listen in

- Anyone trying to listen in also has to guess H, V or U,L
- Measuring, destroys the photon
- They re-transmit
- But may get it wrong and scramble the data!



Knowing you've been bugged

- Send a long message with random H, V or U, L then chat openly
- When sender and receiver both use H, V or U, L but still don't agree

They've been bugged

	sender				receiver			
	H	V	U	L	H	V	U	L
Good data			1	0			1	0
	0	1					1	0
Strange!	1	0			0	1		
			0	1	0	1		
	1	0					1	0
Good data	1	0			1	0		

How does this help?

- Send a long message
- Chat openly about it afterwards
 - compare a selection of data to check for bugging
- If not bugged then sender tells receiver which bits of the message contained the real data

They've exchanged a
secret!

For example

		sender				receiver			
		H	V	U	L	H	V	U	L
1	check data			1	0			1	0
2		0	1					1	0
3	data	1	0			1	0		
4				0	1	0	1		
5		1	0					1	0
6	dummy data	0	1			0	1		
7		0	1					1	0
8				1	0	1	0		
9	data			0	1			0	1
10	check data	0	1			0	1		

Use 1 and 10 to check security and 3 and 9 for message 10, 01