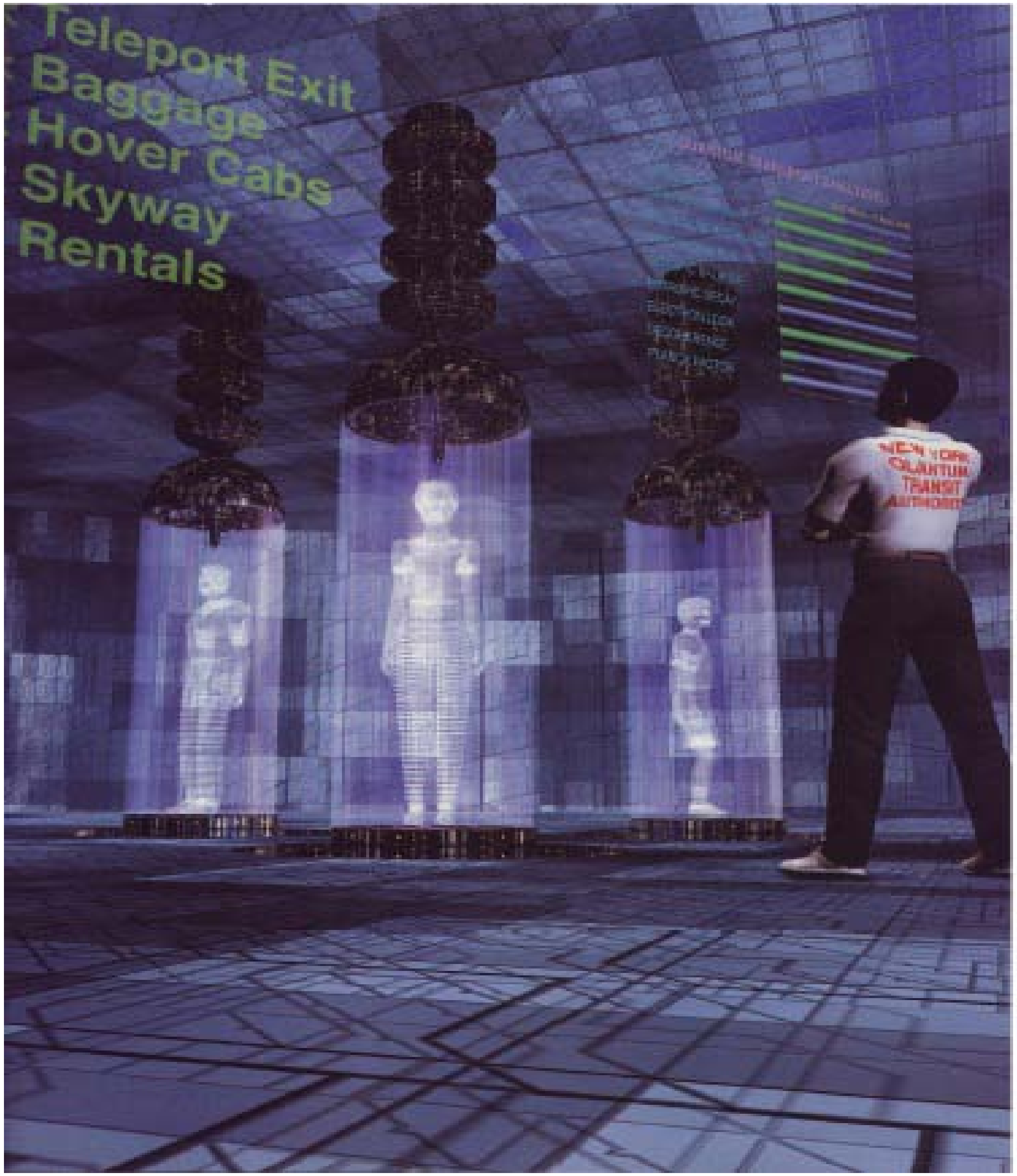


Image: Zeilinger 2000

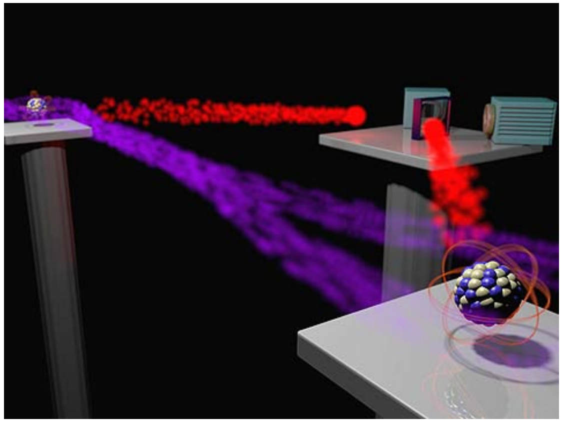
Quantum Communications Tutorial for Engineers

Globecom Washington DC 2016

Rob Malaney
UNSW

Quantum Communications
Tutorial

Image: Rosenfeld, MPQ, Garching.



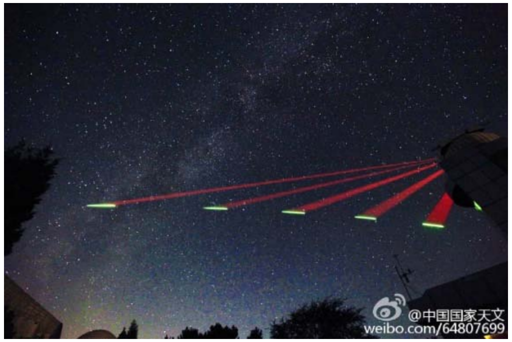
1) **Introduction -**
   Why Quantum Communications?

2) **Technical Background - Single Photon States (DV States)**
   (i) The Photon & The Qubit
   (ii) Quantum Key Distribution (QKD) -The "Killer App"
   (iii) Quantum Entanglement
   (iv) Quantum Teleportation
   (v) Quantum Error Correction

3) **Technical Background – Multi-Photon States (CV States)**
   (i) The Quantized Electromagnetic Field
   (ii) Coherent and Squeezed States
   (iii) The Entangled Two-mode Squeezed State

4) **Some Emerging Quantum-Communication Applications**
   (i) QKD (revisited)
   (ii) Satellite Communications
   (iii) The Quantum Internet
   (iv) Orbital Angular Momentum
   (v) Wireless (6G) Communications
   (vi) Links to Quantum Computers

5) **Conclusions**



First Test of Chinese Quantum Satellite.

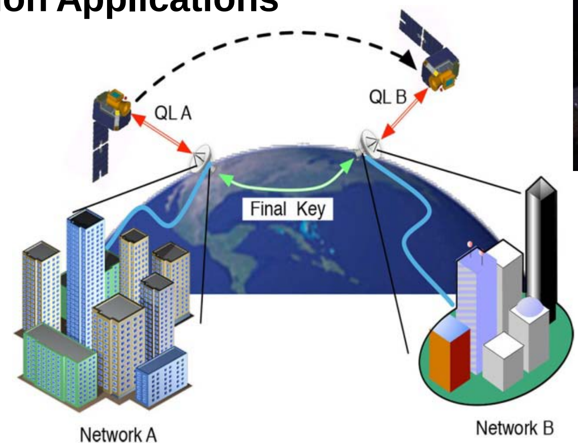
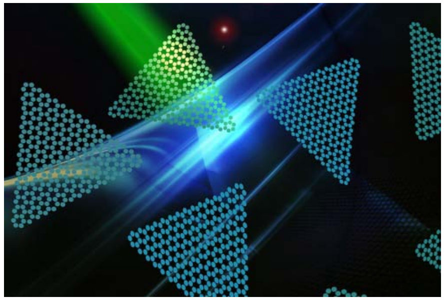


Image:SPIE

Introduction

Why Quantum Communications?

Interesting engineering challenges !



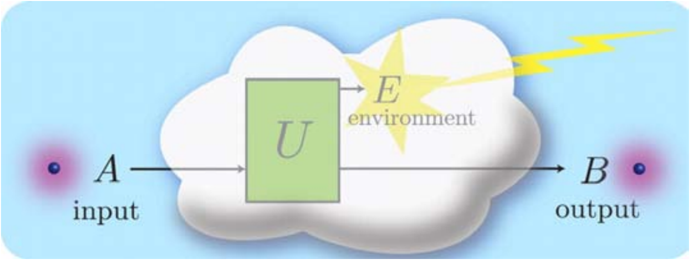
Creation of Deterministic Single Photons on Demand.

Image: University of Technology Sydney

Everyone seems to be doing it !

China Lunches World's First Quantum Satellite Sept '16. CCTV News.

The ultimate Cyber -Security solutions !



Representation of a quantum channel
Smith & Yard 2008

Now Truly Making its Way Into Real World Engineering Solutions →

Toward Large Scale Quantum Communications

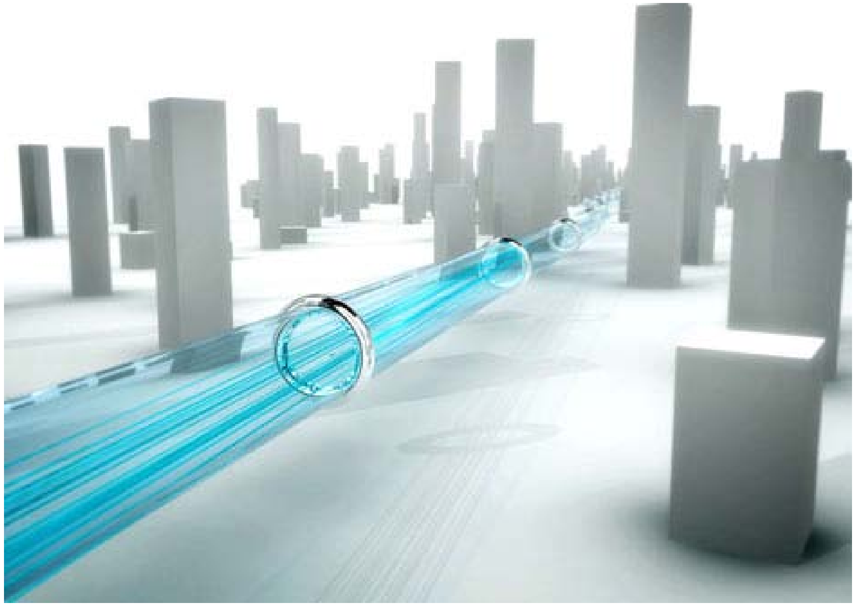
ieee spectrum online
For Tech Insiders

Quantum Communications is emerging as the breakthrough communications technology of the 21st Century

- **Major research thrusts globally are underway**
- **Practical fundamental limits are being explored via extensive deployments**
- **Research papers are appearing in Major IEEE Conferences (e.g. Globecom !)**
- **Commercial deployments in quantum cryptography are already being rolled out (e.g. MagiQ**: http://www.magiqtech.com**)**

Quantum Solutions for the Real World™

MagiQ



EU-sponsored quantum-cryptography network unparalleled in size and complexity.

Image: Austrian Research Centers

Quantum Communications over any Distance is Entirely Feasible

Quantum Communications Over 150km Now **Established (**many times !)

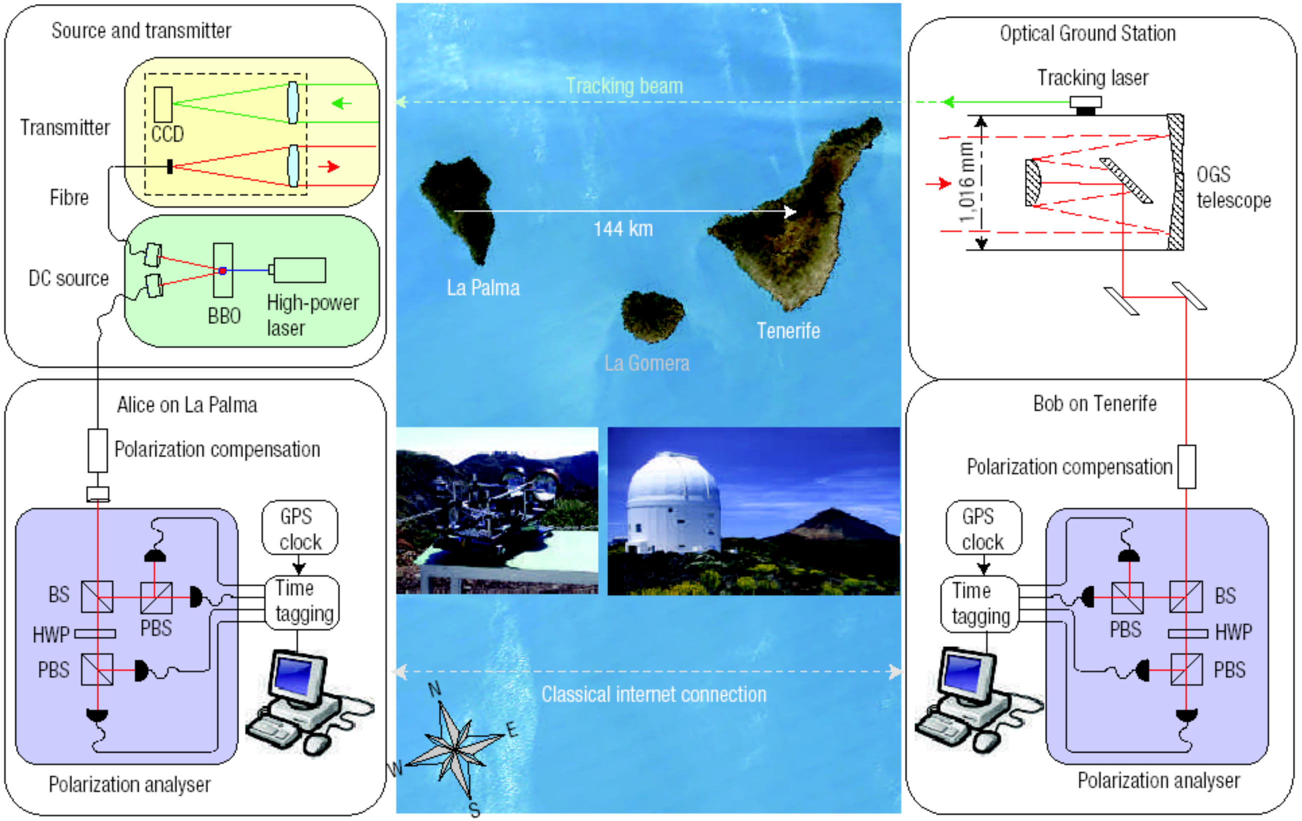


Image: Ursin et al. 2007.

Space Based Quantum Communications?

The Tenerife experiment was first test of a satellite based quantum communication network

Photo: Aug 2016 –

The Chinese quantum satellite blasts off from the Jiuquan Satellite Launch Centre. (AFP)

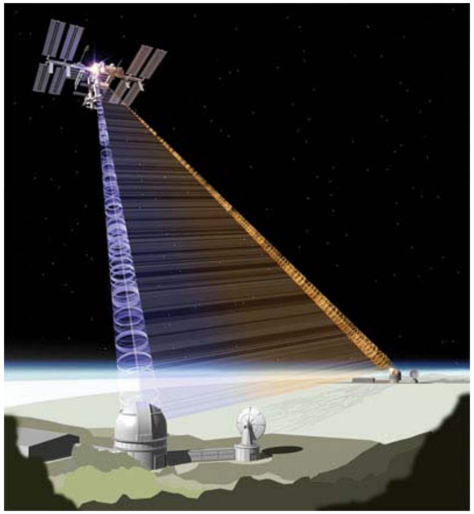
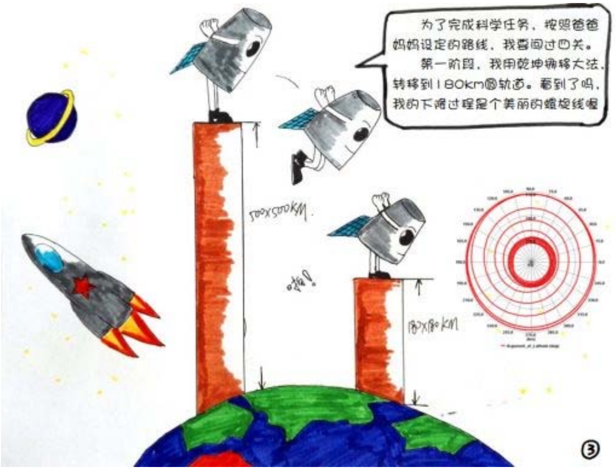


Image: ESA



Quantum Communications is now truly international !

Quantum Communications is Interesting!

Concepts you need to know (as we move along)

What is a Photon?
It is likely more than you thought (prior to 1992)

The Qubit
The Itsybitsy basic resource source of all quantum communications

The No Cloning Theorem
Copying classical information is easy, but try copying quantum information.

Quantum Entanglement
Why Einstein was wrong and right at same time.

Quantum Teleportation
Communication of quantum state information (magically)

The Infinite Qudit
Just when you thought this was all too easy

UNSW ENGINEERING
THE UNIVERSITY OF NEW SOUTH WALES

Quantum Mechanics is True!

(Postulates of Quantum Mechanics) *

1. Associated with any particle moving in a conservative field of force is a wave function which determines everything that can be known about the system.

2. With every physical observable q there is associated an operator **Q**, which when operating upon the wavefunction associated with a definite value of that observable will yield that value times the wavefunction.

3. Any operator **Q** associated with a physically measurable property ***q*** will be Hermitian.

4. The set of eigenfunctions of operator **Q** will form a complete set of linearly independent functions.

5. For a system described by a given wavefunction, the expectation value of any property ***q*** can be found by performing the expectation value integral with respect to that wavefunction.

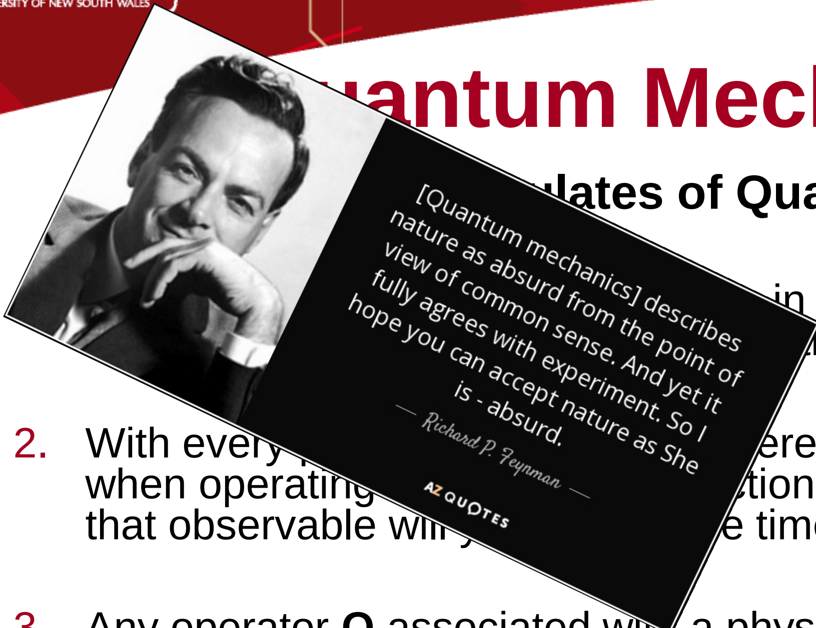
6. The time evolution of the wavefunction is given by the time dependent Schrodinger equation.

*Actually true – but "formally" unproven statements

Postulates 2 and 3 are building blocks of Quantum Communications !

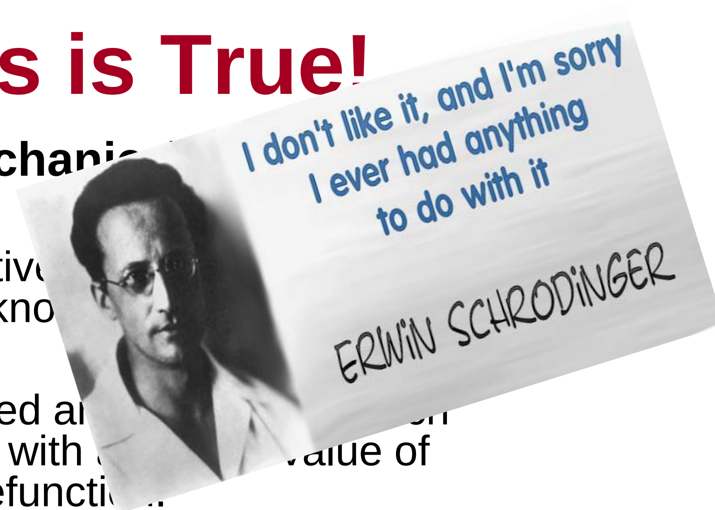
Hyperphysics.phy-ast.gsu.edu

UNSW ENGINEERING
THE UNIVERSITY OF NEW SOUTH WALES



...uantum Mechanics is True!

...lates of Quantum Mechani...



... in a conservative ...
... hat can be kno...

2. With every ... ere is associated a... when operating ... tion associated with ... value of that observable wi... e times the wavefuncti...

3. Any operator **Q** associated wi... a physically measurable property ***q*** will be Hermitian.

4. The set o... t of linearly independ...

5. For a sys... n value of any prope... e integral with respe...

6. The time e... dependent Schrodinger equation.

For me, the important thing about quantum mechanics is the equations, the mathematics. If you want to understand quantum mechanics, just do the math.
All the words that are spun around it don't mean very much. It's like playing the violin. If violinists were judged on how they spoke, it wouldn't make much sense. Freeman Dyson

*Actually true – but "formally" unproven statements

Postulates 2 and 3 are building blocks of Quantum Communications !

Quantum Communications –
Concepts you need to know (as we move along)

What is a Photon?
It is likely more than you thought (prior to 1992)

The Qubit
The Itsybitsy basic resource source of all quantum communications

The No Cloning Theorem
Copying classical information is easy, but try copying quantum information.

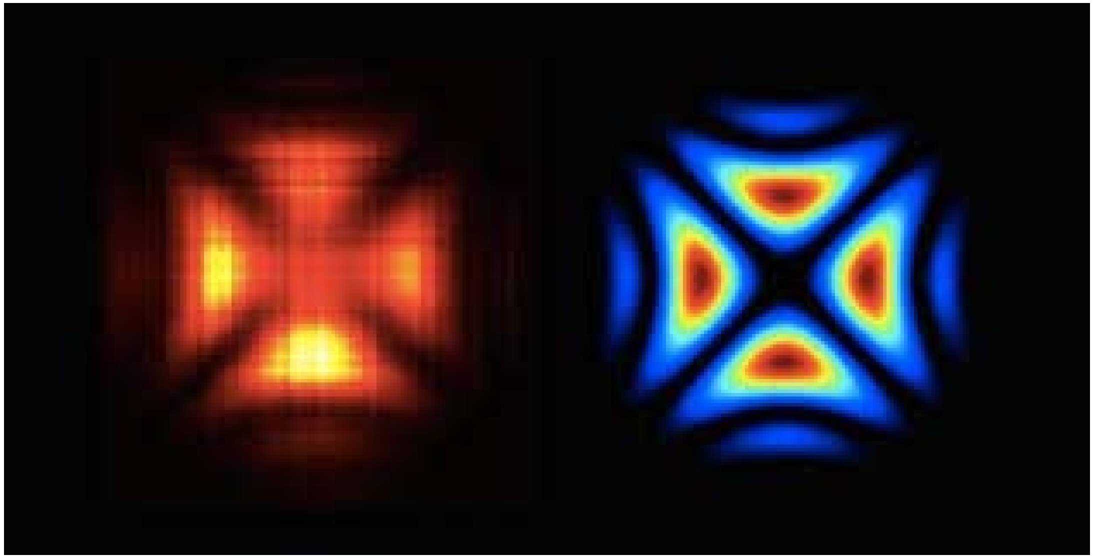
Quantum Entanglement
Why Einstein was wrong and right at same time.

Quantum Teleportation
Communication of quantum state information (magically)

The Infinite Qudit
Just when you thought this was all too easy

Technical Background

Single Photons (DV States) & The Qubit



Hologram of a single photon reconstructed from raw measurements (left) and theoretically predicted (right).
Chrapkiewicz et al.2016

What is a Photon?

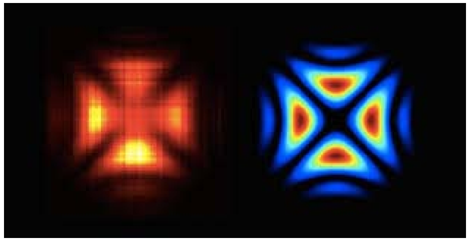
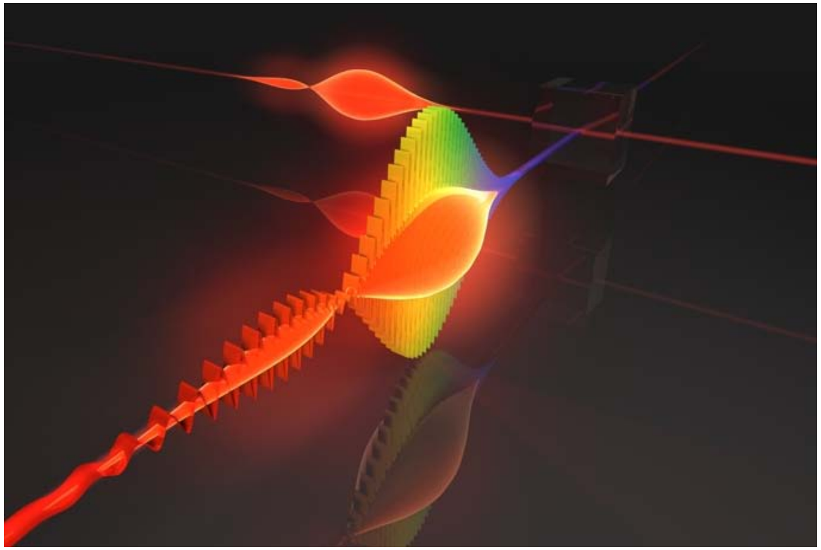


Image: M. Bellini/National Inst. of Optics



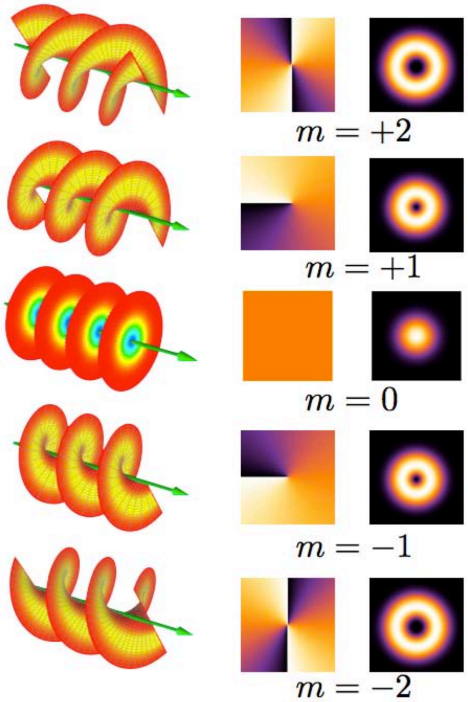
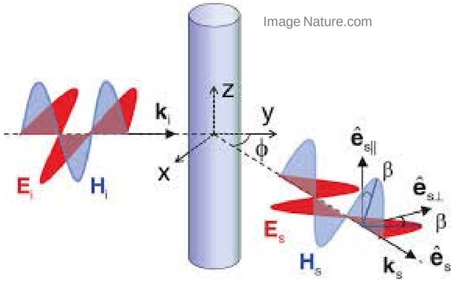


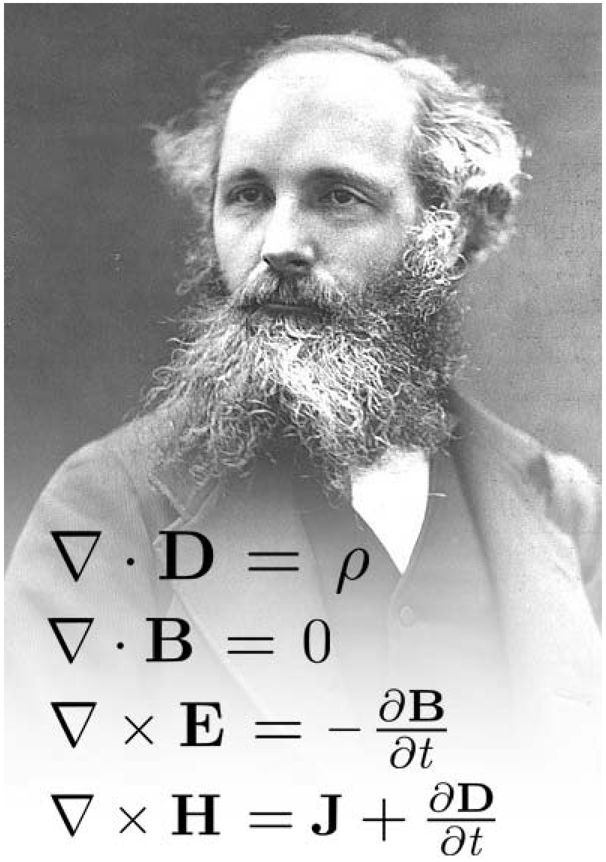
Image Wikipedia

A solution of the Quantised Electromagnetic Field -

Four Degrees of Freedom
(helicity and a three dimensional momentum vector)

What is a Photon?





$$\nabla \cdot \mathbf{D} = \rho$$
$$\nabla \cdot \mathbf{B} = 0$$
$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}$$
$$\nabla \times \mathbf{H} = \mathbf{J} + \frac{\partial \mathbf{D}}{\partial t}$$

Image :University of Michigan

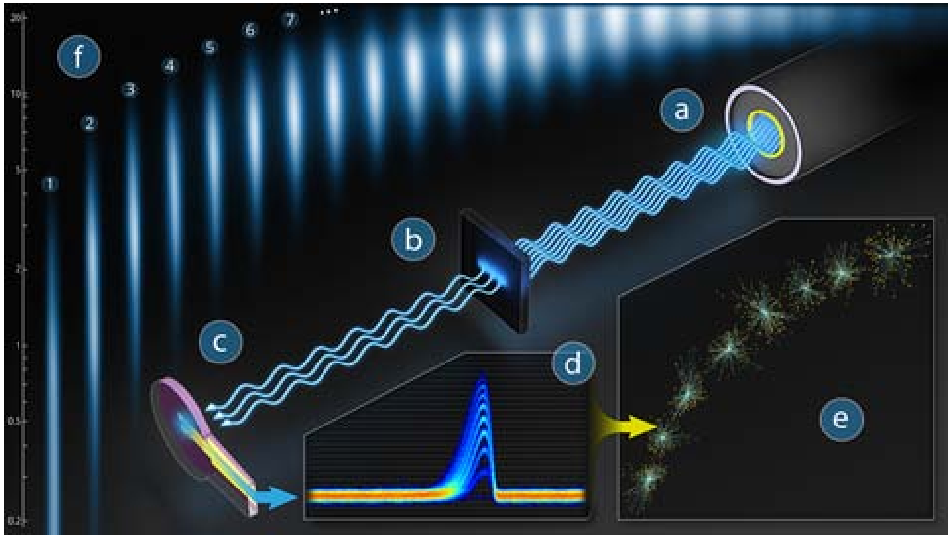
Altering the field quantities in Maxwell's Equations to operators that satisfy quantum commutation relations leads to the Quantized Electromagnetic Field (see later).

A particularly interesting quantum state derived from such machinery is one coherent to all orders - the so-called Coherent State (aka laser output)

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle = e^{-\frac{|\alpha|^2}{2}} e^{\alpha \hat{a}^\dagger} |0\rangle ,$$

A quantum state containing *n* photons (Fock State)

Very Attenuated Laser Pulses Approximate Single Photons



Credit: Sean Kelley/NIST PML

$$|\alpha\rangle \rightarrow |0\rangle + \gamma|1\rangle + \gamma^2|2\rangle + ...$$

$$\gamma << 1$$

Heavily attenuated weak laser pulses approximate Single Photon sources.

Can use polarization states of such single photons as **QUBITS**

Experimental deterministic “on demand” single photons is an open research area.

Quantum Communications –

Concepts you need to know (as we move along)

What is a Photon?

It is likely more than you thought (prior to 1992)

The Qubit

The Itsybitsy basic resource source of all quantum communications

The No Cloning Theorem

Copying classical information is easy, but try copying quantum information.

Quantum Entanglement

Why Einstein was wrong and right at same time.

Quantum Teleportation

Communication of quantum state information (magically)

The Infinite Qudit

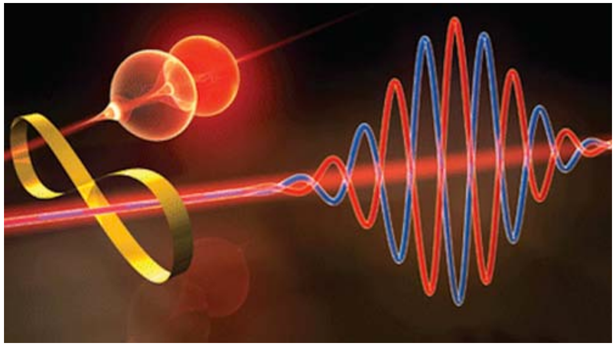
Just when you thought this was all too easy

The Qubit

The Schrodinger "Cat State"

(Wikipedia)

"Miniaturize" - e.g. take the "cat" to be a photon. And swap "dead or alive" states with any alternate orthogonal states of the photon |0> & |1>



Nature Photonics

Discrete-Variable Quantum System

Discrete Variable (DV) systems

A quantum system having a finite-dimensional Hilbert space

Qubits $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$

A quantum system having a two-dimensional Hilbert space

Spin, polarisation, etc.

Qudits

$$|\psi\rangle = \sum_{n=0}^{D-1} \alpha_n |n\rangle, \qquad \sum_{n=0}^{D-1} |\alpha_n|^2 = 1$$

A qudit is a generalization of the qubit to a D-dimensional Hilbert space

Later - Continuous variable systems $D \to \infty$ and $D_{i+1} - D_i \to 0$

The Qubit

(Bloch Sphere)

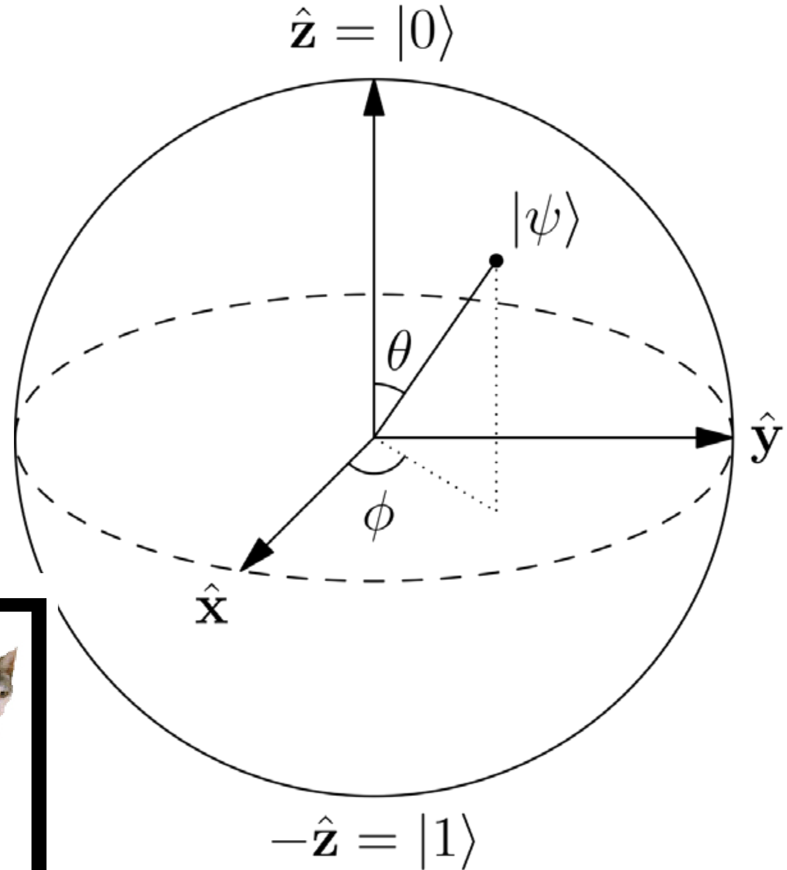
Bloch Sphere representation of a qubit.

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

$$\alpha = \cos\left(\frac{\theta}{2}\right)$$

$$\beta = e^{i\phi}\sin\left(\frac{\theta}{2}\right)$$

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



(Images - Wikipedia)

Quantum Communications –
Concepts you need to know (as we move along)

What is a Photon?
It is likely more than you thought (prior to 1992)

The Qubit
The Itsybitsy basic resource source of all quantum communications

The No Cloning Theorem
Copying classical information is easy, but try copying quantum information.

Quantum Entanglement
Why Einstein was wrong and right at same time.

Quantum Teleportation
Communication of quantum state information (magically)

The Infinite Qudit
Just when you thought this was all too easy

Quantum Key Distribution (QKD)

The No Cloning Theorem

A arbitrary unknown qubit cannot be copied or amplified without disturbing its original state.

This is the statement of the
No-Cloning Theorem
Wootters & Zurek (1982)

Quantum Key Distribution

The No Cloning Theorem

Imagine there existed a unitary transformation that could do this (unitary is applied to the product state)

$$U\left(|s_1\rangle|0\rangle\right) = |s_1\rangle|s_1\rangle$$

$$U\left(|s_2\rangle|0\rangle\right) = |s_2\rangle|s_2\rangle$$

$$U\left(|s\rangle|0\rangle\right) = |s\rangle|s\rangle$$

$$U\left(|s_\perp\rangle|0\rangle\right) = |s_\perp\rangle|s_\perp\rangle$$

Consider applying our device also to

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|s\rangle + |s_\perp\rangle\right)$$

$$U\left(|\Psi\rangle|0\rangle\right) = U\left\{\frac{1}{\sqrt{2}}\left(|s\rangle + |s_\perp\rangle\right)|0\rangle\right\}$$

$$= \frac{1}{\sqrt{2}}\left[\left(|s\rangle|s\rangle\right) + \left(|s_\perp\rangle|s_\perp\rangle\right)\right] \neq |\Psi\rangle|\Psi\rangle$$

But we wanted

$$|\Psi\rangle|\Psi\rangle = \frac{1}{2}\left(|s\rangle + |s_\perp\rangle\right)\left(|s\rangle + |s_\perp\rangle\right)$$

so $|s\rangle, |s_\perp\rangle$ and $|\Psi\rangle$ cannot be copied simultaneously

Note shorthand notation

$$|s_1\rangle|s_1\rangle \equiv |s_1\rangle \otimes |s_1\rangle$$

$$\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

Quantum Mechanics is Linear

Quantum Key Distribution

The No Cloning Theorem

Alternate Proof: Lets take inner product of both first equation using 2nd equation (e.g. LHS of both equations form an inner product)

$$\left(U^{\dagger}\langle s_2|\langle 0|\right)\left(U|s_1\rangle|0\rangle\right)=\left(\langle s_2|\langle s_2|\right)\left(|s_1\rangle|s_1\rangle\right)$$

$$U^{\dagger}U\langle s_2|s_1\rangle\langle 0|0\rangle=\langle s_2|s_1\rangle\langle s_2|s_1\rangle$$

Quantum Key Distribution

The No Cloning Theorem

But $$U^{\dagger}U = I \qquad \langle 0|0\rangle = 1$$

Thus $$\langle s_2|s_1\rangle = \langle s_2|s_1\rangle\langle s_2|s_1\rangle$$

Thus $$\langle s_2|s_1\rangle = \langle s_2|s_1\rangle^2$$

Thus, only possible if

$$\langle s_2|s_1\rangle = 0 \qquad \langle s_2|s_1\rangle = 1$$

Quantum Key Distribution

The No Cloning Theorem

$$\langle s_2 | s_1 \rangle = \langle s_2 | s_1 \rangle^2$$

This means that you can copy a state if you know already that it is *identical* to all the other states available to you

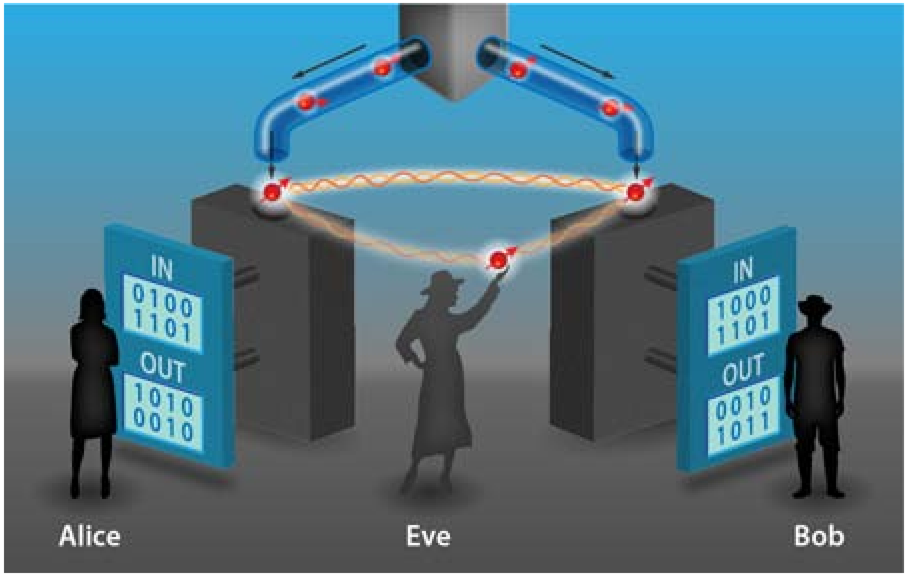
This means the *distinct* states available to you can be copied **only** if they are mutually orthogonal

Q) What is the difference between above and classical information?
A) None.

Quantum Key Distribution

The BB84 Protocol

- The BB84 protocol (Bennett and Brassard 1984) was the first quantum cryptography protocol introduced – let us discuss this now

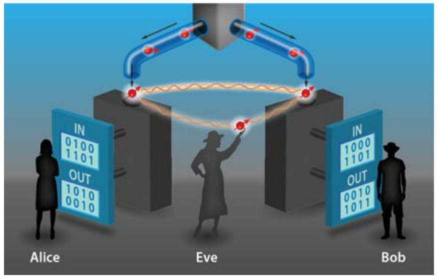


APS.org

- As you will see it is a good use of our knowledge of polarization states, and implicitly uses the No Cloning Theorem to avoid attacks

Quantum Key Distribution

The BB84 Protocol



- Let us use **two** basis as a means of doing a measurement. Use

$$M = \left(\left| m_\theta^{(1)} \right\rangle, \left| m_\theta^{(2)} \right\rangle \right) = \left(\begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}, \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix} \right)$$

1) The rectilinear basis (our horizontal-vertical basis)
Refer to this basis as "+"

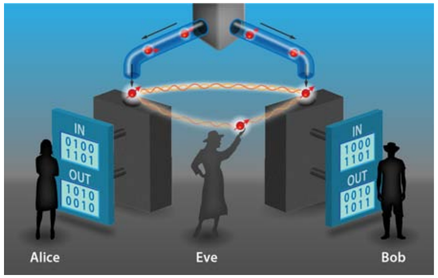
$$\theta = 0^o$$

$$M = \left(\left| m_\theta^{(1)} \right\rangle, \left| m_\theta^{(2)} \right\rangle \right) = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$$

UNSW ENGINEERING
THE UNIVERSITY OF NEW SOUTH WALES

Quantum Key Distribution

The BB84 Protocol



Let us use **two** basis as a means of doing a measurement. Use again

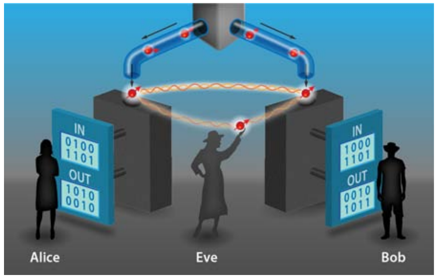
$$M=\left(\left|m_\theta{}^{(1)}\right\rangle,\left|m_\theta{}^{(2)}\right\rangle\right)=\left(\begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix},\begin{pmatrix}-\sin\theta\\ \cos\theta\end{pmatrix}\right)$$

2) The diagonal basis (rotate horizontal-vertical basis) $\theta = 45^o$
Refer to this basis as “x”.

$$M=\left(\left|m_\theta{}^{(1)}\right\rangle,\left|m_\theta{}^{(2)}\right\rangle\right)=\left(\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix},\begin{pmatrix}-\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}\right)$$

Quantum Key Distribution

The BB84 Protocol



We can prepare states referenced to a state in a particular basis e.g.

$$|0\rangle_+$$

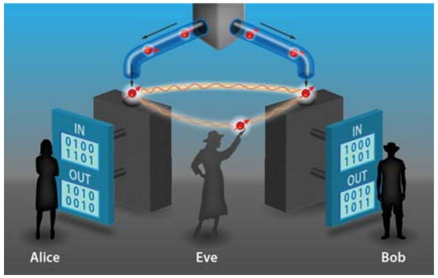
means the zero state referenced to the "+" basis

We have four possible states referenced this way

$$|0\rangle_+ , |0\rangle_x \, |1\rangle_+ , |1\rangle_x$$

Quantum Key Distribution

The BB84 Protocol



This table summarizes the BB4 protocol

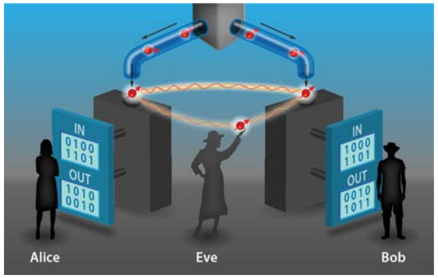
Table I. The BB84 Key Distribution Protocol. Here, "Y" and "N" stand for "yes" and "no," respectively, and "R" means that Bob obtains a random result

Alice's string	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Alice's basis	+	+	+	×	×	+	×	×	×	×	+	+	+	+
Bob's basis	+	×	+	+	×	+	×	+	×	×	+	+	+	+
Bob's string	1	R	0	R	0	0	1	R	1	1	1	1	0	0
Same basis?	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits to keep	1		0		0	0	1		1	1	1	1	0	0
Test	Y		N		N	Y	N		N	N	N	Y	Y	N
Key			0		0		1		1	1	1			0

Image: Bruss et al 2007

Quantum Key Distribution

The BB84 Protocol



Step 1: Alice prepares a series of qubits in each of the four possible states

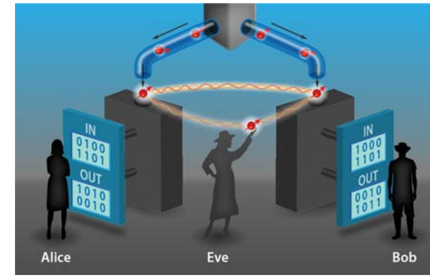
$$|0\rangle_+ ,|0\rangle_x |1\rangle_+ ,|1\rangle_x$$

Table I. The BB84 Key Distribution Protocol. Here, "Y" and "N" stand for "yes" and "no," respectively, and "R" means that Bob obtains a random result

Alice's string	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Alice's basis	+	+	+	×	×	+	×	×	×	×	+	+	+	+
Bob's basis	+	×	+	+	×	+	×	+	×	×	+	+	+	+
Bob's string	1	R	0	R	0	0	1	R	1	1	1	1	0	0
Same basis?	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits to keep	1		0		0	0	1		1	1	1	1	0	0
Test	Y		N		N	Y	N		N	N	N	Y	Y	N
Key			0		0		1		1	1	1			0

Quantum Key Distribution

The BB84 Protocol



Step 2: Bob measures the qubit in a randomly chosen “x” or “+” basis

In noiseless channel – If Bob chooses same basis as Alice the result is same

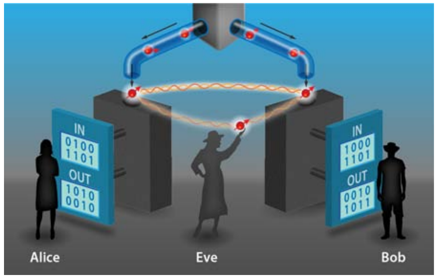
If Bob chooses different basis from Alice the result is random

Table I. The BB84 Key Distribution Protocol. Here, "Y" and "N" stand for "yes" and "no," respectively, and "R" means that Bob obtains a random result

Alice's string	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Alice's basis	+	+	+	×	×	+	×	×	×	×	+	+	+	+
Bob's basis	+	×	+	+	×	+	×	+	×	×	+	+	+	+
Bob's string	1	R	0	R	0	0	1	R	1	1	1	1	0	0
Same basis?	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits to keep	1		0		0	0	1		1	1	1	1	0	0
Test	Y		N		N	Y	N		N	N	N	Y	Y	N
Key			0		0		1		1	1	1			0

Quantum Key Distribution

The BB84 Protocol



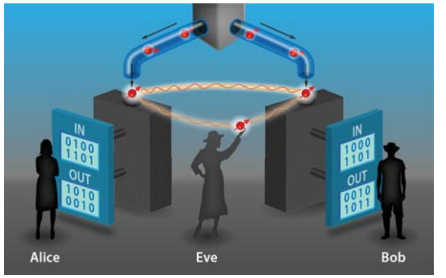
Step 3: Using a classical channel Bob tells Alice which basis he used for each measurement – Alice tells Bob which measurement to keep (i.e. what measurements correspond to same basis she used).
Using this they form the *sifted* key (the "bits to keep" in table below)

Table I. The BB84 Key Distribution Protocol. Here, "Y" and "N" stand for "yes" and "no," respectively, and "R" means that Bob obtains a random result

Alice's string	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Alice's basis	+	+	+	×	×	+	×	×	×	×	+	+	+	+
Bob's basis	+	×	+	+	×	+	×	+	×	×	+	+	+	+
Bob's string	1	R	0	R	0	0	1	R	1	1	1	1	0	0
Same basis?	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits to keep	1		0		0	0	1		1	1	1	1	0	0
Test	Y		N		N	Y	N		N	N	N	Y	Y	N
Key			0		0		1		1	1	1			0

Quantum Key Distribution

The BB84 Protocol



Step 4: Alice tells Bob via classical channel a small subset of the bits which she uses as a test.

If Bob agrees that he measured the same 0s and 1s in his measurements (some small error tolerance is allowed in practice)

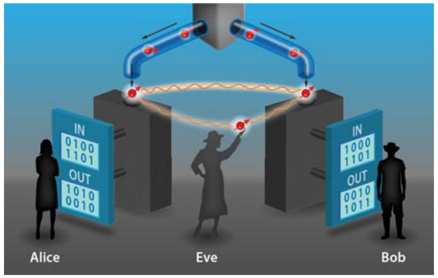
they assume all is well and use remaining unannounced bits as the initial key.

Table I. The BB84 Key Distribution Protocol. Here, "Y" and "N" stand for "yes" and "no," respectively, and "R" means that Bob obtains a random result

Alice's string	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Alice's basis	+	+	+	×	×	+	×	×	×	×	+	+	+	+
Bob's basis	+	×	+	+	×	+	×	+	×	×	+	+	+	+
Bob's string	1	R	0	R	0	0	1	R	1	1	1	1	0	0
Same basis?	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits to keep	1		0		0	0	1		1	1	1	1	0	0
Test	Y		N		N	Y	N		N	N	N	Y	Y	N
Key			0		0		1		1	1	1			0

Quantum Key Distribution

The BB84 Protocol (summary)



Step 1: Alice creates string 0's and 1's

1	0	0	1	0	1	0	0	0	0	1	0	0	0	1	1	0	0
x	+	x	+	+	x	+	x	x	+	+	x	+	x	x	x	x	+

Step 2: Alice polarizes photons with different basis and mapping

0 -> first element of basis
1-> second element of basis

Step 3: Bob chooses a random basis from x and + and measures and strores result

x	+	+	x	x	x	+	x	+	x	+	+	x	+	x	+	x	+

Step 4:Alice calls Bob on classical channel and discusses basis each used to find where basis agreed (the blue boxes)

1	0				1	0	0			1				1		0	0
x	+				x	+	x			+				x		x	+

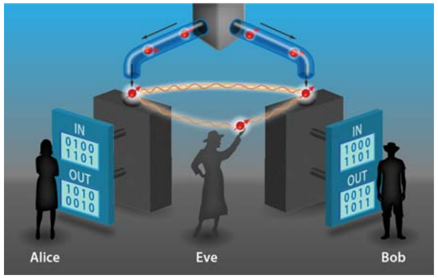
1 0 1 0 0 1 1 0 0 becomes the secret key.

Step 5: Alice and Bob use this initial key to generate a new key using error correction

Step 6: Based on number of errors they estimate how much information an eavesdropper ‘Eve’ ***may*** have obtained – they then create a shorter string of which the are sure Eve has no knowledge of (privacy amplification)

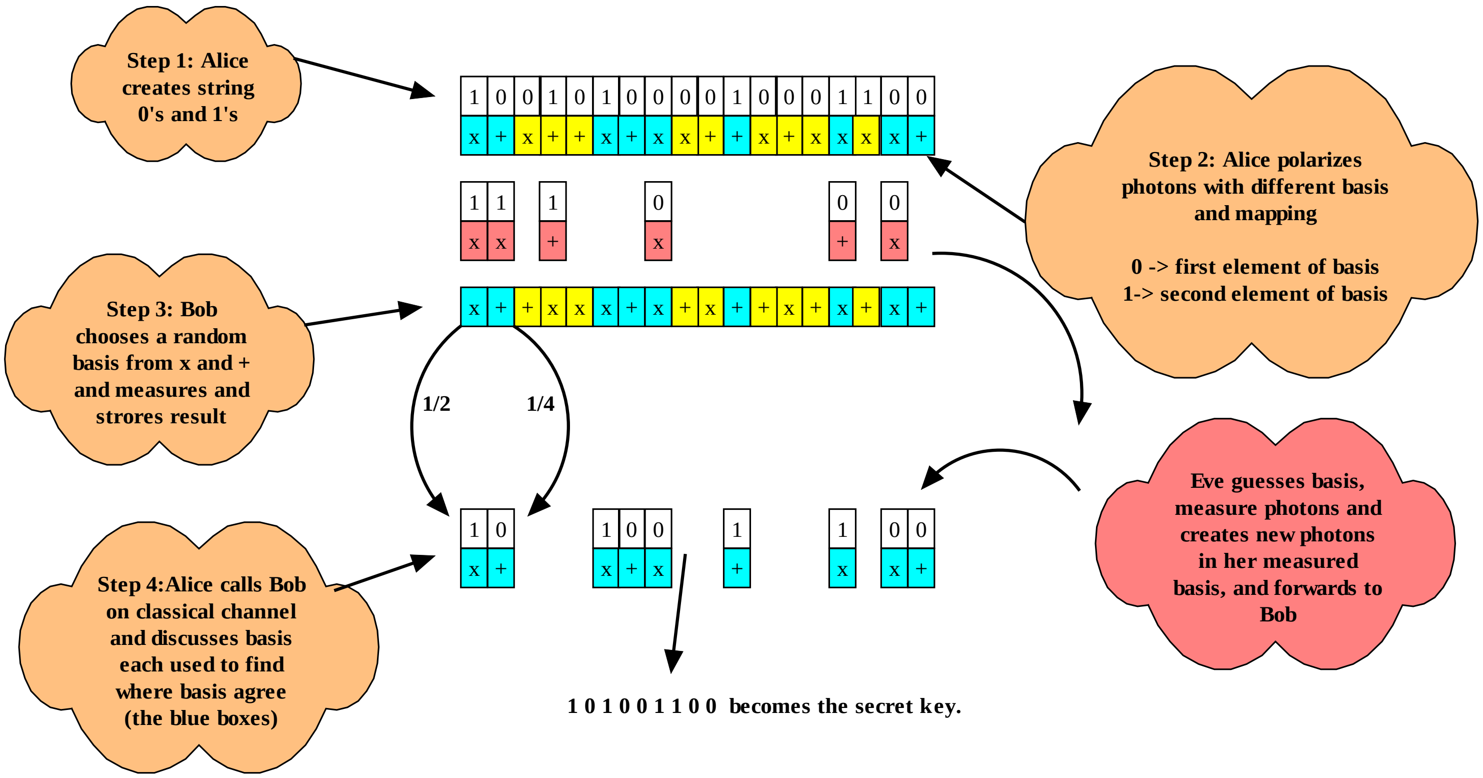
Quantum Key Distribution

The BB84 Protocol



But Eve can guess-estimate?

“Formal” Proof of Security for QKD took 12 years !



Quantum Communications

Concepts you need to know (as we move along)

What is a Photon?
It is likely more than you thought (prior to 1992)

The Qubit
The Itsybitsy basic resource source of all quantum communications

The No Cloning Theorem
Copying classical information is easy, but try copying quantum information.

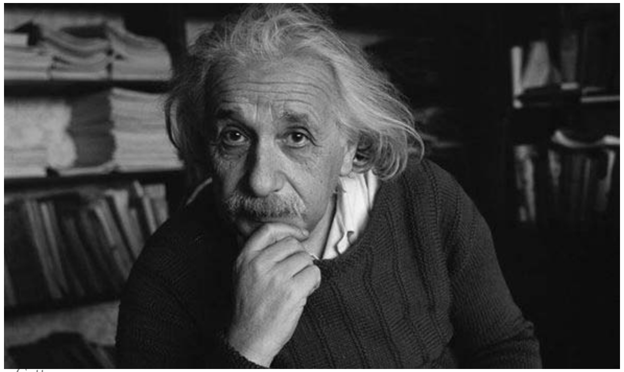
Quantum Entanglement
Why Einstein was wrong and right at same time.

Quantum Teleportation
Communication of quantum state information (magically)

The Infinite Qudit
Just when you thought this was all too easy

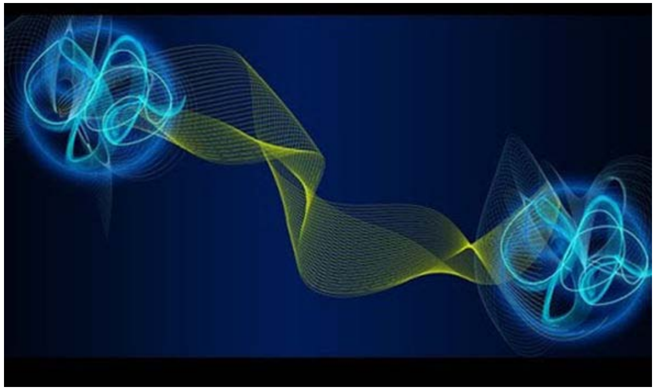
Quantum Communications

Quantum Entanglement

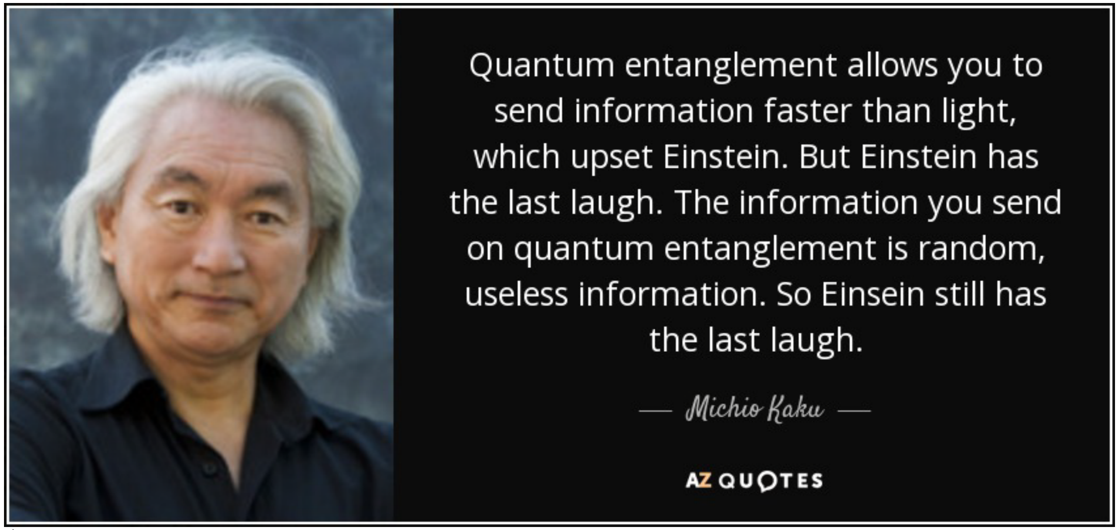


Getty

"Bizarre science: Particles TALK to each other over huge distances breaking laws of physics"
UK Daily Express Oct. 2015



YouTube



Azquotes.com

Quantum Communications

Quantum Entanglement

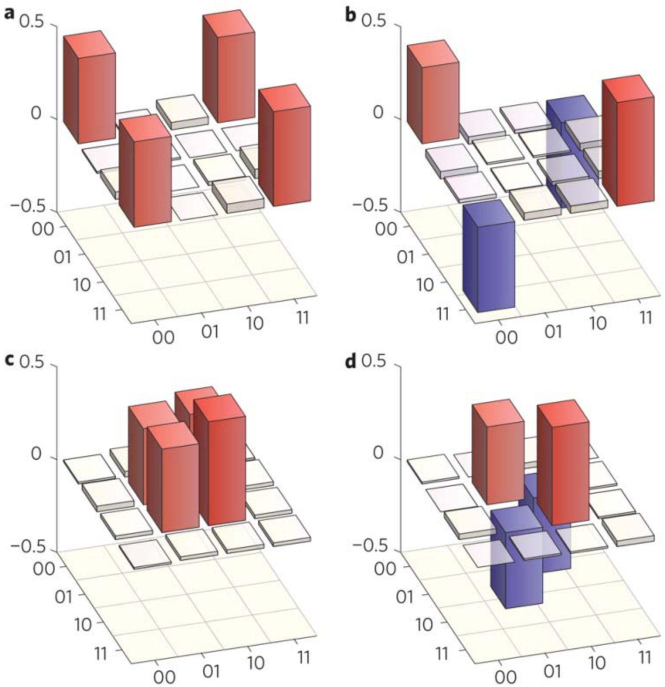


Image: Shadbolt et al 2001.

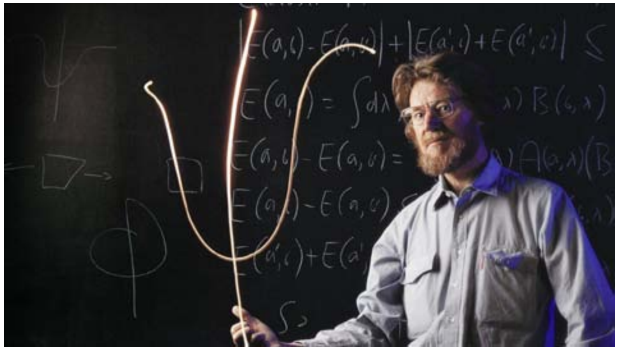


Image: BBC.

$$|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle),$$
$$|0\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle),$$
$$|1\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle),$$

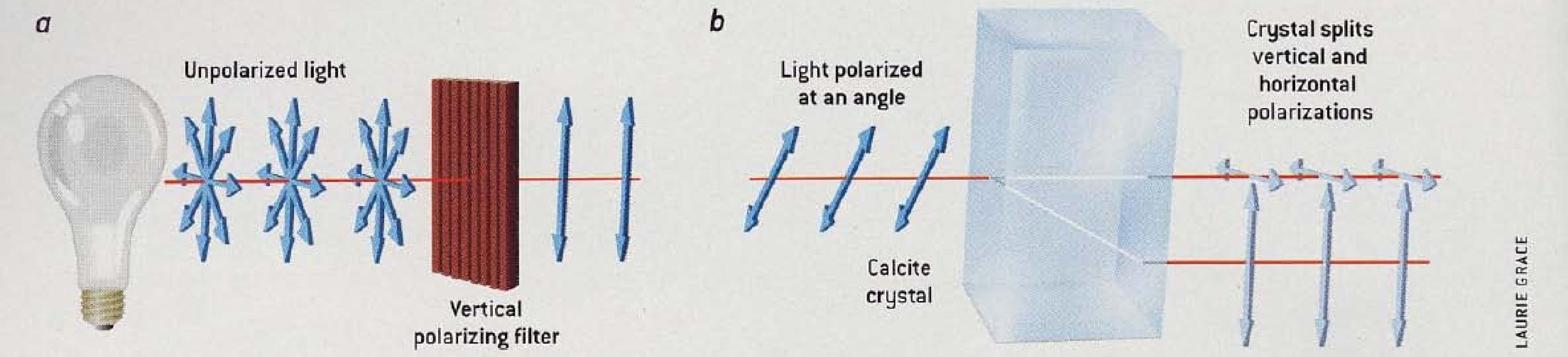
and

$$|1\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle).$$

The Bell States

Quantum Communications

Creating Quantum Entanglement



UNPOLARIZED LIGHT consists of photons polarized in all directions (*a*). In polarized light the photons' electric-field oscillations (*arrows*) are all aligned. A calcite crystal (*b*) splits a light beam, sending photons that are polarized parallel with its axis into one beam and those that are perpendicular into the other. Intermediate angles go into a quantum superposition of both beams. Each such photon can be detected in one beam or the other, with probability depending on the angle. Because probabilities are involved, we cannot measure the polarization of a single photon with certainty.

Image. Zeilinger, 2000

Quantum Communications

Creating Quantum Entanglement

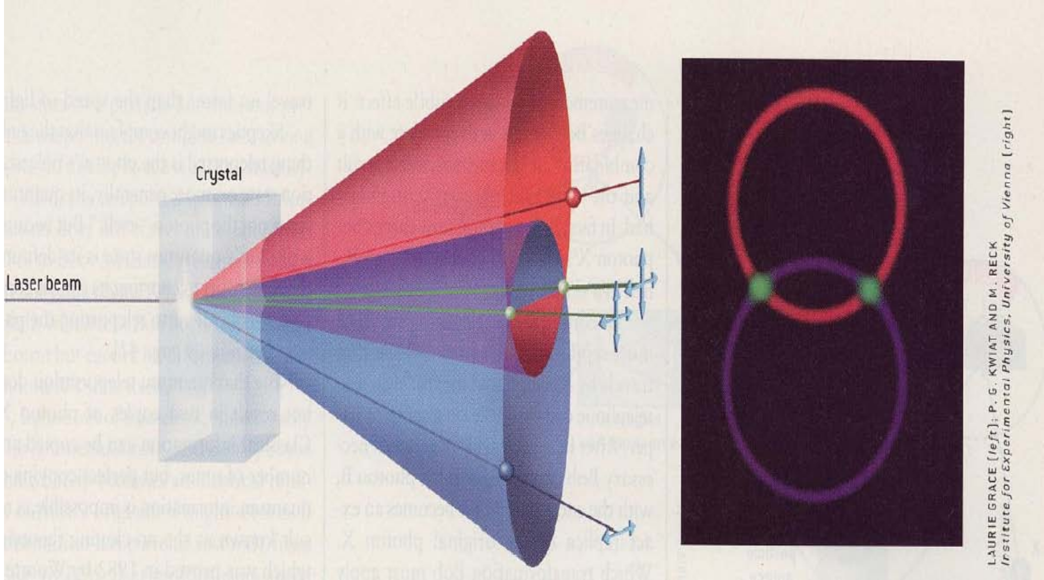


Image. Zeilinger, 2000

Entanglement leads to many strange outcomes!

Quantum blindsight. "You appear to be blind in your left eye and blind in your right eye. Why you can see with both eyes is beyond me..."

Smith & Yard 2008

Quantum Communications –
Concepts you need to know (as we move along)

What is a Photon?
It is likely more than you thought (prior to 1992)

The Qubit
The Itsybitsy basic resource source of all quantum communications

The No Cloning Theorem
Copying classical information is easy, but try copying quantum information.

Quantum Entanglement
Why Einstein was wrong and right at same time.

Quantum Teleportation
Communication of quantum state information (magically)

The Infinite Qudit
Just when you thought this was all too easy

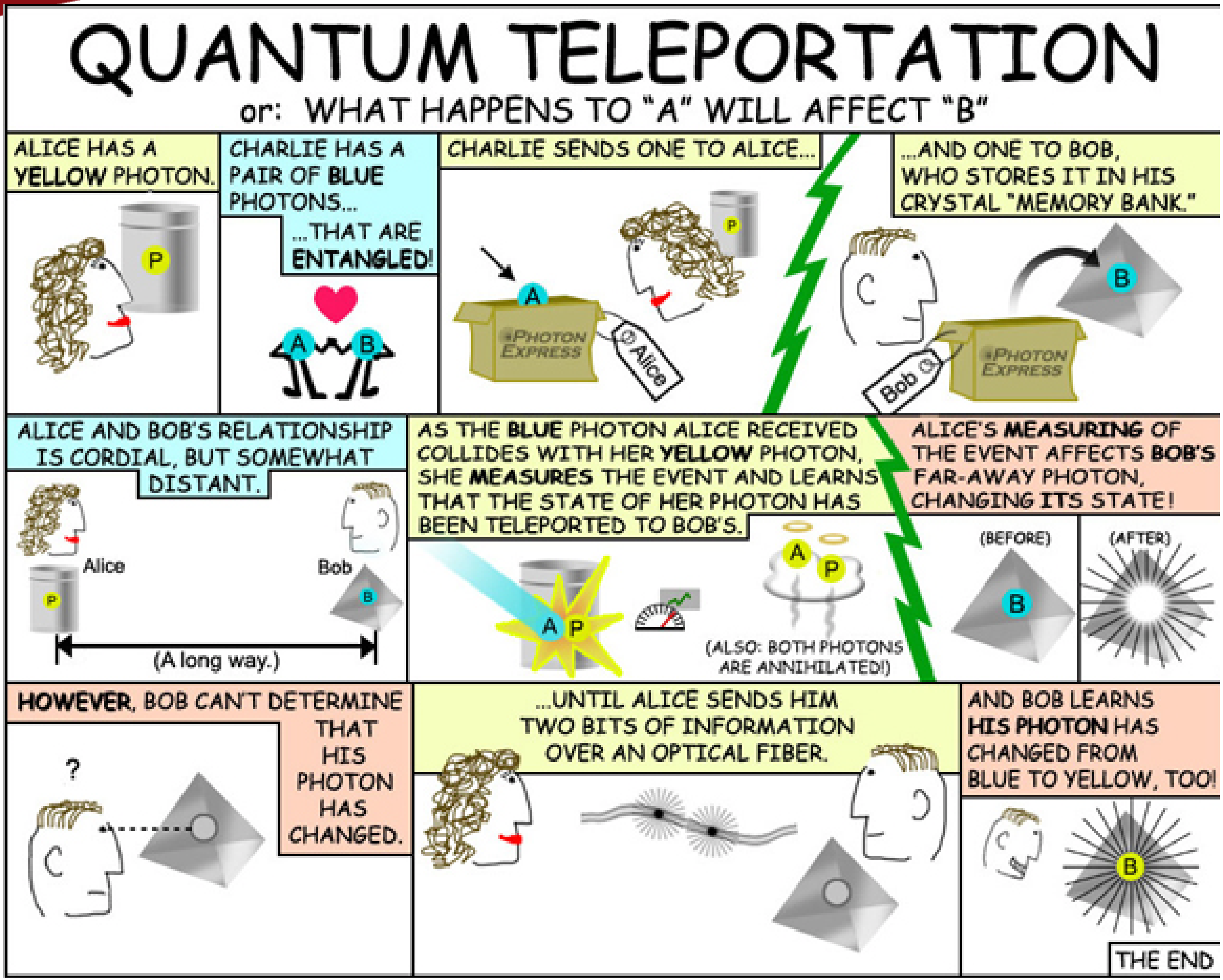

QUANTUM TELEPORTATION
or: WHAT HAPPENS TO "A" WILL AFFECT "B"
ALICE HAS A YELLOW PHOTON.
P
CHARLIE HAS A PAIR OF BLUE PHOTONS...
...THAT ARE ENTANGLED!
A
B
CHARLIE SENDS ONE TO ALICE...
PHOTON EXPRESS
Alice
...AND ONE TO BOB, WHO STORES IT IN HIS CRYSTAL "MEMORY BANK."
Bob
ALICE AND BOB'S RELATIONSHIP IS CORDIAL, BUT SOMEWHAT DISTANT.
Alice
Bob
(A long way.)
AS THE BLUE PHOTON ALICE RECEIVED COLLIDES WITH HER YELLOW PHOTON, SHE MEASURES THE EVENT AND LEARNS THAT THE STATE OF HER PHOTON HAS BEEN TELEPORTED TO BOB'S.
(ALSO: BOTH PHOTONS ARE ANNIHILATED!)
ALICE'S MEASURING OF THE EVENT AFFECTS BOB'S FAR-AWAY PHOTON, CHANGING ITS STATE!
(BEFORE)
(AFTER)
HOWEVER, BOB CAN'T DETERMINE THAT HIS PHOTON HAS CHANGED.
?
...UNTIL ALICE SENDS HIM TWO BITS OF INFORMATION OVER AN OPTICAL FIBER.
AND BOB LEARNS HIS PHOTON HAS CHANGED FROM BLUE TO YELLOW, TOO!
THE END

Image: NASA

Quantum Communications –

Quantum Teleportation (Star Trek Version)

Image. Zeilinger, 2000

Quantum Communications –

Quantum Teleportation – has been done for real – many times !

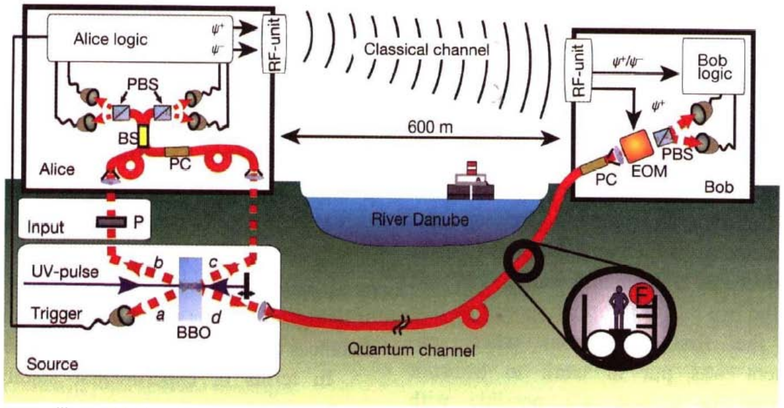
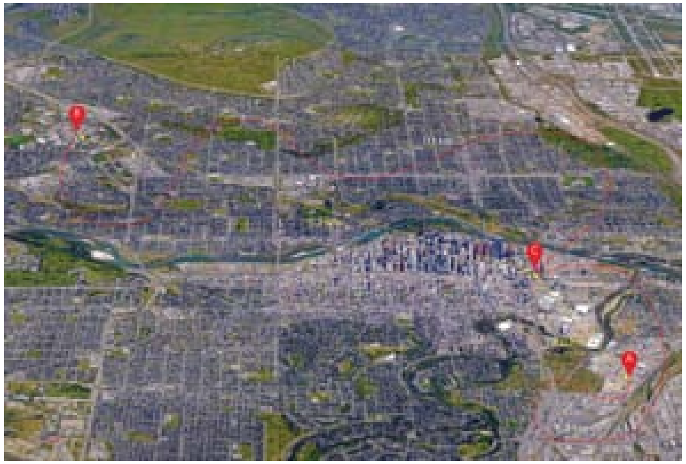
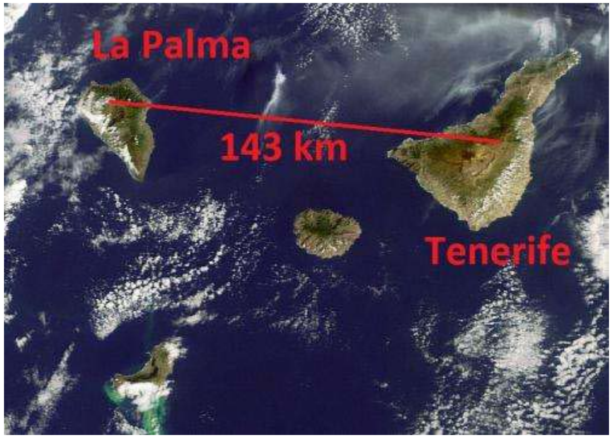


Image: Zeilinger,2006

University of Calgary





ESA

Quantum Teleportation
(Technically Speaking)

Step 1

Suppose Alice has a qubit that she wants to teleport to Bob. This qubit can be written generally as: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

We want to teleport this state C

Our quantum teleportation scheme requires Alice and Bob to share a maximally entangled state beforehand, for instance one of the four Bell states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B\right)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B\right)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B\right)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\right)$$

Tensor product used as in Postulate 2

2 particle entangled state – but 1 particle (A) held by Alice and another (B) held by Bob

Wikipedia

Quantum Teleportation

So, Alice has two particles (C, the one she wants to teleport, and A, one of the entangled pair), and Bob has one particle, B. In the total system, the state of these three particles is given by

$$|\psi\rangle \otimes |\Phi^+\rangle = (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$$

Tensor product used again ----to get 3 particle state

Step 2: Alice makes measurement in Bell basis of her two qubits (A and C)

$$|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle)$$

$$|0\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle)$$

$$|1\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle)$$

$$|1\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle)$$

Before looking at Alice's measurement result – note the following identities which simplify our algebra

Wikipedia

Quantum Teleportation

The three particle state shown above thus becomes the following four-term superposition:

$$\frac{1}{2}\left(\left|\Phi^{+}\right\rangle\otimes\left(\alpha|0\rangle+\beta|1\rangle\right)+\left|\Phi^{-}\right\rangle\otimes\left(\alpha|0\rangle-\beta|1\rangle\right)+\left|\Psi^{+}\right\rangle\otimes\left(\beta|0\rangle+\alpha|1\rangle\right)+\left|\Psi^{-}\right\rangle\otimes\left(\beta|0\rangle-\alpha|1\rangle\right)\right)$$

No operation yet performed – all 3 particles still in same state

$$\left|\Phi^{+}\right\rangle\otimes\left(\alpha|0\rangle+\beta|1\rangle\right)$$

$$\left|\Phi^{-}\right\rangle\otimes\left(\alpha|0\rangle-\beta|1\rangle\right)$$

$$\left|\Psi^{+}\right\rangle\otimes\left(\beta|0\rangle+\alpha|1\rangle\right)$$

$$\left|\Psi^{-}\right\rangle\otimes\left(\beta|0\rangle-\alpha|1\rangle\right)$$

Step 2: Alice makes a measurement on Her two qubits (A and C) – which forces the complete system into **one** of these states

Wikipedia

Quantum Teleportation

Three Consequences of Alice's measurement

1. Alice and Bobs original entanglement no longer exists

2. Alice' two qubits are now entangled in one of the Bell states

3. Bob's qubit B is now in 'form' of original C qubit

"teleportation of C almost complete"

$$|\Phi^+\rangle \otimes (\alpha|0\rangle + \beta|1\rangle)$$
$$|\Phi^-\rangle \otimes (\alpha|0\rangle - \beta|1\rangle)$$
$$|\Psi^+\rangle \otimes (\beta|0\rangle + \alpha|1\rangle)$$
$$|\Psi^-\rangle \otimes (\beta|0\rangle - \alpha|1\rangle)$$

Wikipedia

Quantum Teleportation

Step 3: Alice informs Bob **Classically** (send 2 bits) what one of the 4 possible state her two particles are in

Step 4: Bob uses this information to transform via a unitarily (Postulate 3) his qubit into same form as original C particle

$$|\Phi^+\rangle \otimes (\alpha|0\rangle + \beta|1\rangle)$$
$$|\Phi^-\rangle \otimes (\alpha|0\rangle - \beta|1\rangle)$$
$$|\Psi^+\rangle \otimes (\beta|0\rangle + \alpha|1\rangle)$$
$$|\Psi^-\rangle \otimes (\beta|0\rangle - \alpha|1\rangle)$$

Eg. if first state needed use the Identity matrix!

or

e.g if 2nd state chosen use Pauli matrix

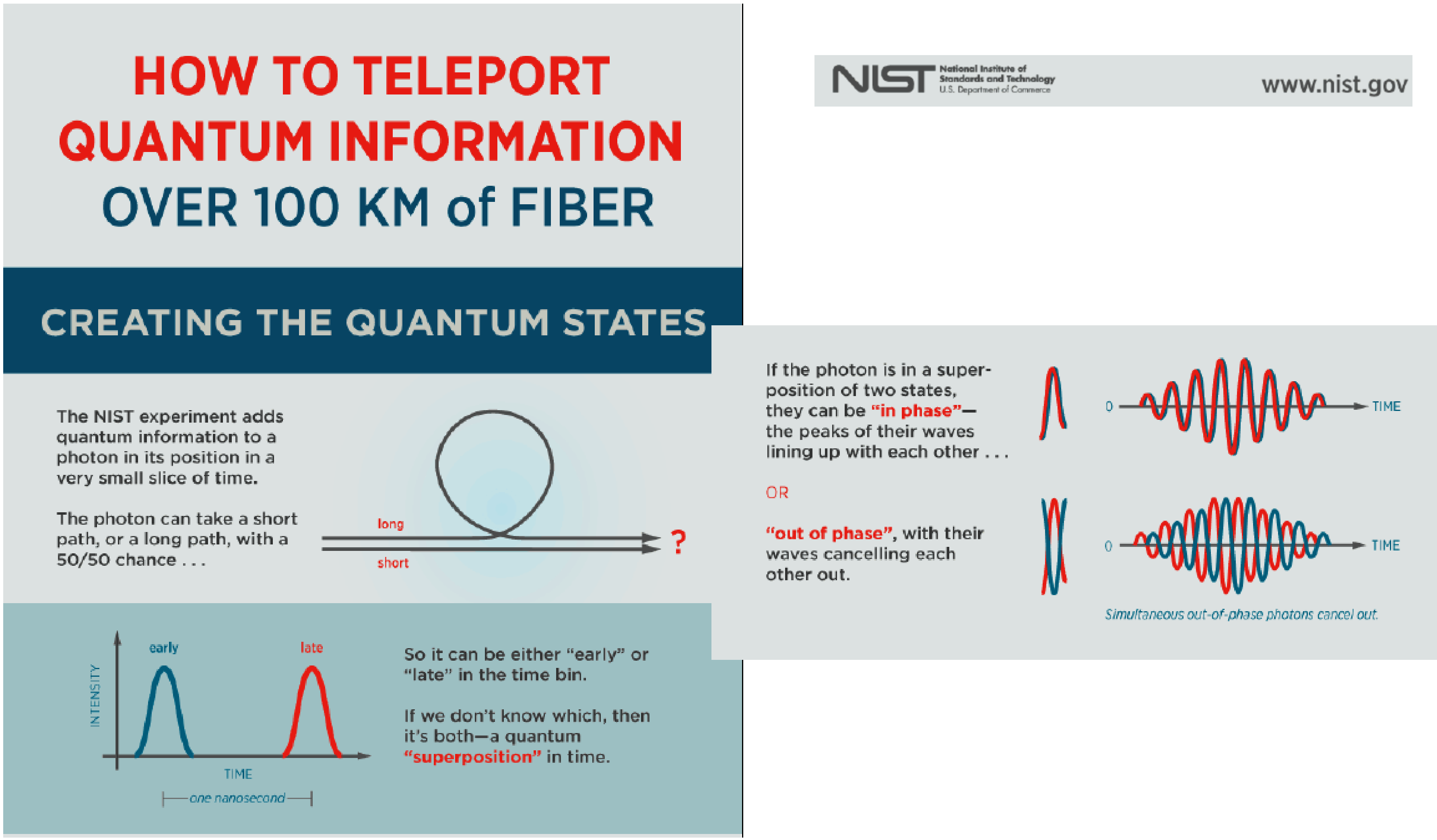
to transform into required state C

$$\sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Teleportation of C Completed!

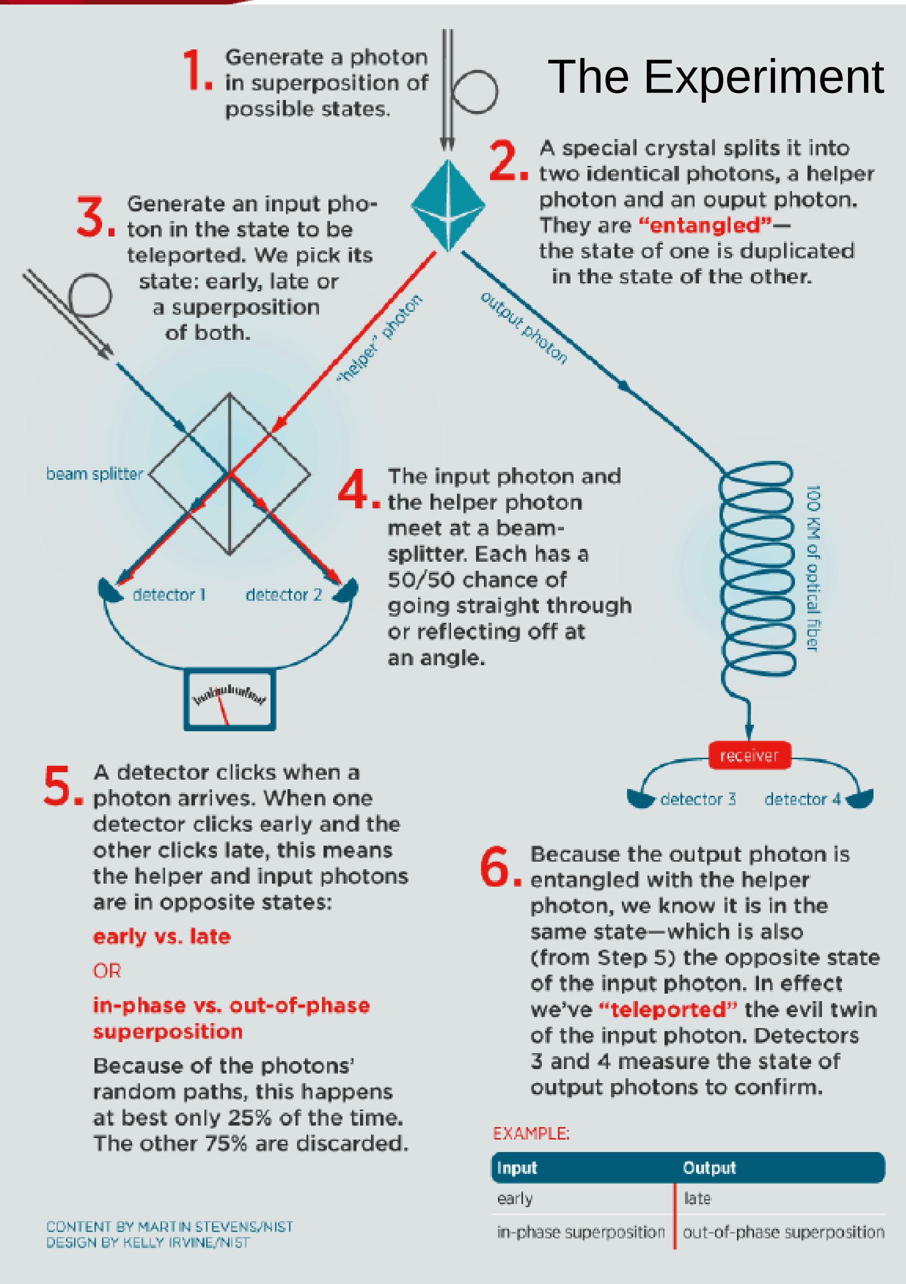
Wikipedia

Quantum Teleportation
(Experimentally Speaking)



Quantum Teleportation
(Experimentally Speaking)

NIST National Institute of Standards and Technology U.S. Department of Commerce www.nist.gov



Quantum Error Correction

Already a well-developed field even though study just commenced mid-90's

We focus on ideas of protecting the quantum state using the machinery of projection operators

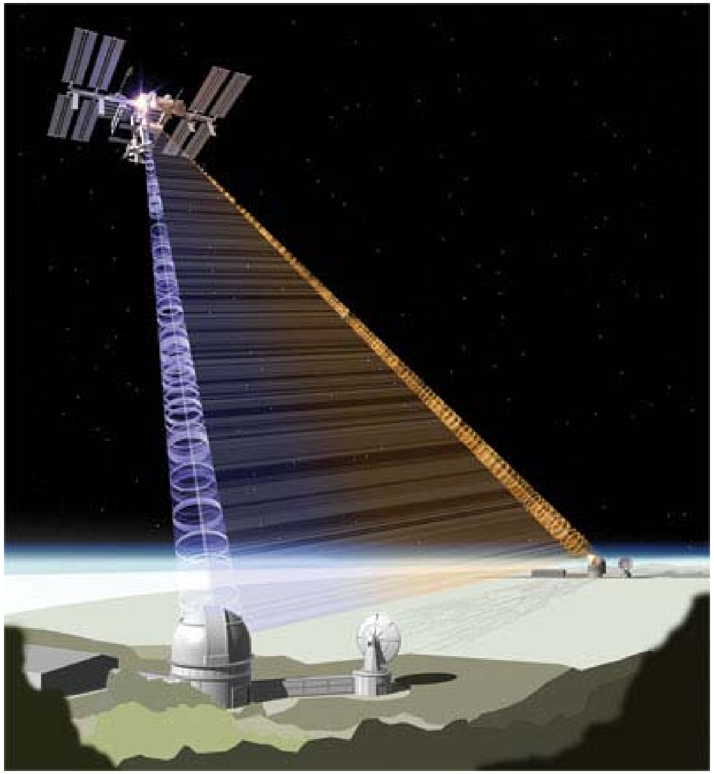


Illustration: European Space Agency (ESA)

Where do Quantum Errors Arise?

Our unitary transforms (or quantum gates) are not just matrices on a board – they need to be *physically* implemented (using laser pulses, field rotations etc) –

- if not perfectly implemented an error in the quantum state can occur.

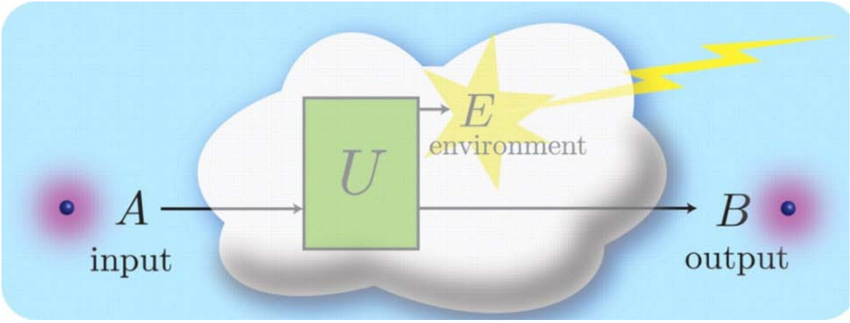
$|\Phi^+\rangle$ 00 $I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$

$|\Phi^-\rangle$ 01 $Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$

$|\Psi^+\rangle$ 10 $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$

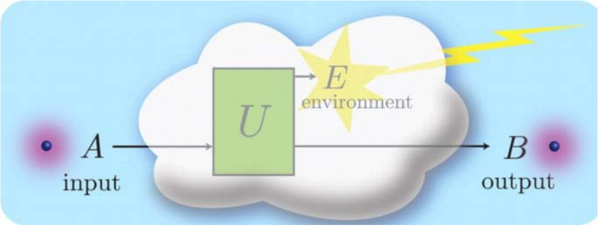
$|\Psi^-\rangle$ 11 $XZ=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&0\\0&-1\end{pmatrix}=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$

Traversal through a medium e.g. Fiber or Air causes a quantum error.



Smith & Yard 2008

(Quantum) Error Correction is easy – right (wrong)?



Basic Problem.

We are given a state |s> which we want to protect – i.e. identify any error and correct for it.

All we need to do is a repetition code such as

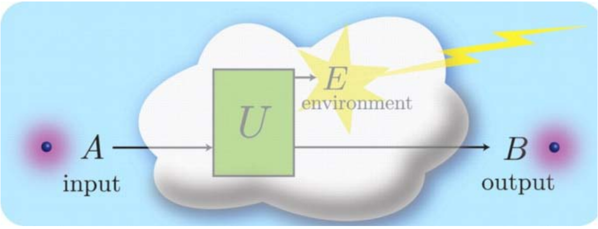
$$|s\rangle \rightarrow |s\rangle|s\rangle|s\rangle$$

Too easy? Yes - for classical error correction

But in quantum world - No. Our old friend the "No cloning theorem" says "no way".

This is what makes quantum communications a lot more *interesting* than classical communications!

Quantum Error Correction



Basic Problem.

We are given a state |s> which we want to protect – i.e. identify any error and correct for it.

$$|s\rangle = a|0\rangle + b|1\rangle$$

We can *add* other *qubits* to the state |s>,

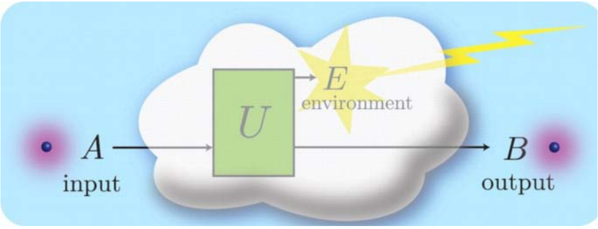
such as two qubits in state |0>

$$|s,00\rangle = a|000\rangle + b|100\rangle$$

We then can find a unitary transform that operates on this three particle composite system with mapping

$$|000\rangle \rightarrow |000\rangle$$
$$|100\rangle \rightarrow |111\rangle$$

Quantum Error Correction



Our initial state

$$|s\rangle = a|0\rangle + b|1\rangle$$

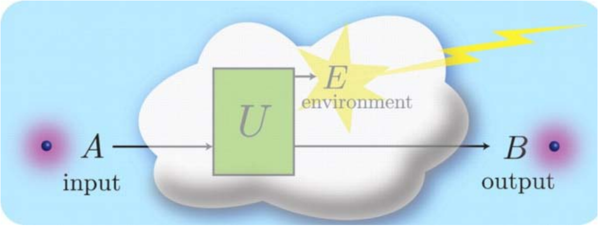
Is now *encoded* as

$$|s\rangle_C = a|000\rangle + b|111\rangle$$

We have encoded a single qubit into three qubits

Seem like a good idea?

Quantum Error Correction
X Correcting Codes



Lets us assume

1) noise affects at most one of our three qubits
2) Error flips a |0> to a |1> and vice versa

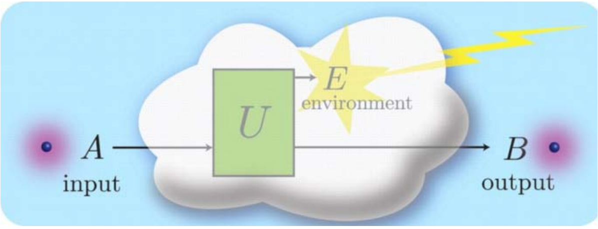
3) That is we assume that *possibly* the noise changes one of the qubits via the action of the *X* matrix

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

[Yes, there are other errors!]

Quantum Error Correction

X Correcting Codes



Let's first do a special form of

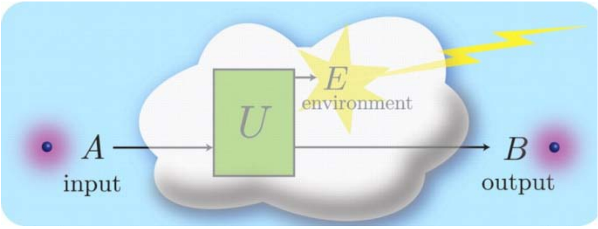
incomplete measurement. Which will

1) **Have four outcomes**
2) **Which is *not* associated with a specific vector in the state space**
3) **But rather with a 2 dimensional subspace of the state space**
4) **And where the subspaces are mutually orthogonal**

NB. state space for 3 qubits has four mutually orthogonal 2D subspaces

Quantum Error Correction

X Correcting Codes



Consider the four projection operators

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

$$P_4 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

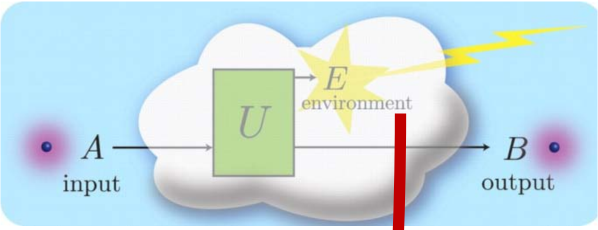
Acting on

$$|s\rangle_C = a|000\rangle + b|111\rangle$$

If measurement leads to subspace P_4 – what/where is the error?

If measurement leads to subspace P_1 – what/where is the error?

Quantum Error Correction
X Correcting Codes



How do we correct an X error at a qubit?

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Tells us – Apply the inverse of *X* to the qubit identified.

What is inverse of *X*? (Hint – it looks awfully like *X*)

We have completed your first quantum error correction.
Real quantum error correction is just as simple as this (well……, kind-of, sort-of)

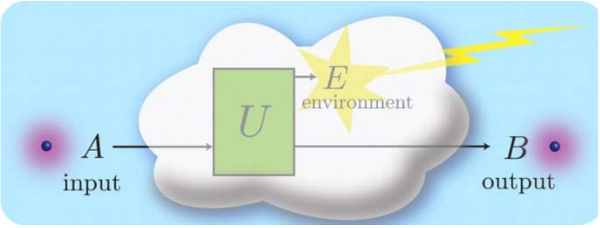
We have defeated Entanglement (with environment) using Entanglement (with an ancilla)

Quantum Error Correction
X Correcting Codes

Other Correcting Codes using same technique?

Assume again noise affects only one qubit but affect is

$$U = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}$$



Aside

$$U|0\rangle = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}|0\rangle = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} \cos\theta \\ i\sin\theta \end{pmatrix} = \cos\theta\begin{pmatrix} 1 \\ 0 \end{pmatrix} + i\sin\theta\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \cos\theta|0\rangle + i\sin\theta|1\rangle$$

For focus assume *second* qubit is only affected – then

$$|s\rangle_C = a|000\rangle + b|111\rangle$$

becomes

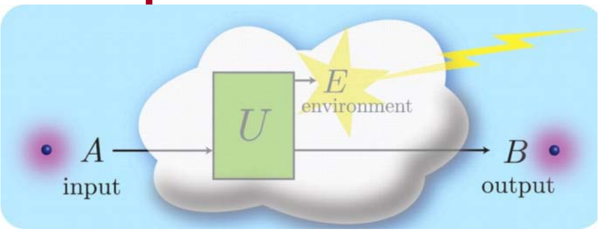
$$|s\rangle_C^{\#} = U_2|s\rangle_C = a\left(\cos\theta|000\rangle + i\sin\theta|010\rangle\right) + b\left(i\sin\theta|101\rangle + \cos\theta|111\rangle\right)$$

Note subscript 2 means apply only to 2nd qubit

Quantum Error Correction

X Correcting Codes

Other Correcting Codes using same technique?



Aside. Checking previous result

$$|s\rangle_C = a|000\rangle + b|111\rangle$$

$$\begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = \begin{pmatrix} \cos\theta|0\rangle + i\sin\theta|1\rangle \\ i\sin\theta|0\rangle + \cos\theta|1\rangle \end{pmatrix}$$

Note these arrows are conceptual only - formally we would need to do the matrix form of the states properly

Exercise for reader –confirm the result below

$$|s\rangle_C^{\#} = U_2|s\rangle_C = a\left(\cos\theta|000\rangle + i\sin\theta|010\rangle\right) + b\left(i\sin\theta|101\rangle + \cos\theta|111\rangle\right)$$

e.g. the second |0> in first term of $|s>_C$ transforms to

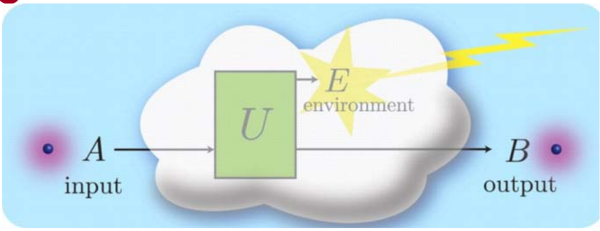
$$\cos\theta|0\rangle + i\sin\theta|1\rangle$$

UNSW ENGINEERING
THE UNIVERSITY OF NEW SOUTH WALES

Quantum Error Correction

X Correcting Codes

Measuring the encoded state



But when we do a measure

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

$$P_4 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

on

$$|s\rangle_C^{\#} = U_2 |s\rangle_C = a\left(\cos\theta|000\rangle + i\sin\theta|010\rangle\right) + b\left(i\sin\theta|101\rangle + \cos\theta|111\rangle\right)$$

Only two outcomes have a non-zero probability!

$$p_2 = \langle s|_C^{\#} P_2 |s\rangle_C^{\#} = \sin^2\theta$$

$$p_4 = \langle s|_C^{\#} P_4 |s\rangle_C^{\#} = \cos^2\theta$$

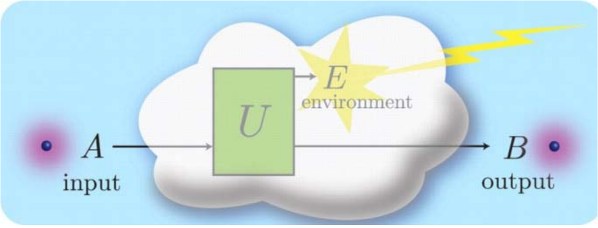
$$\frac{P_2|s\rangle_C^{\#}}{\sqrt{\langle s|_C^{\#} P_2 |s\rangle_C^{\#}}} = a|010\rangle + b|101\rangle$$

Final States

$$\frac{P_4|s\rangle_C^{\#}}{\sqrt{\langle s|_C^{\#} P_4 |s\rangle_C^{\#}}} = a|000\rangle + b|111\rangle$$

Quantum Error Correction

X Correcting Codes



Error Correction?

Note that the projection onto this final state

$$\frac{P_4 |s\rangle_C^{\#}}{\sqrt{\langle s|_C^{\#} P_4 |s\rangle_C^{\#}}} = a|000\rangle + b|111\rangle$$

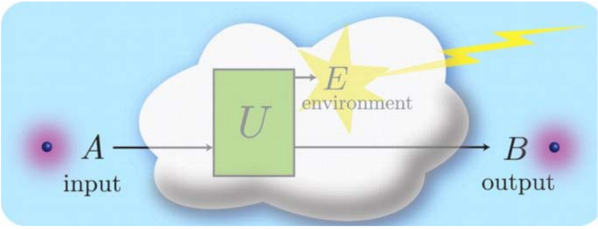
Has automatically corrected the error (caused by *U* on the 2nd qubit) –

Therefore no need to do anything further if we get this outcome -

The measurement has corrected the error !

Quantum Error Correction

X Correcting Codes



Error Correction?

Note that the projection onto other final state

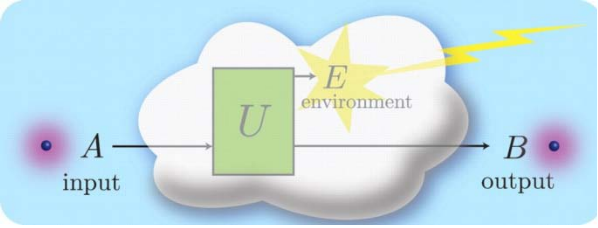
$$\frac{P_2\left|s\right\rangle_C^{\#}}{\sqrt{\left\langle s\right|_C^{\#} P_2\left|s\right\rangle_C^{\#}}} = a\left|010\right\rangle + b\left|101\right\rangle$$

Has *not* automatically corrected the error (caused by *U* on the 2nd qubit) –

Therefore as this projection outcome this is mapped to a flip error in the second qubit – we need to correct this by applying the *X* operator

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Quantum Error Correction
Z Correcting Codes



Are we there yet?

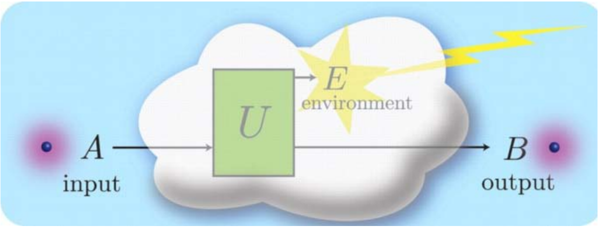
Almost:
As real quantum engineers – we have a feeling we need to do just one more type of error correction.

Alright then - how about a *Z* correcting error code?

A combination of *X* and *Z* correcting error codes leads to a very effective strategy!

Quantum Error Correction

Z Correcting Codes



Consider the operator

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

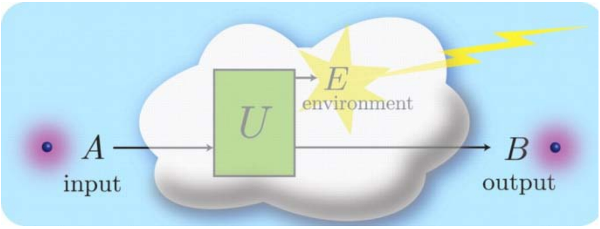
Acting on any of our three qubits from the state $\left|s\right\rangle_C = a\left|000\right\rangle + b\left|111\right\rangle$

Leads to

$$\left|s\right\rangle_C^{\#} = a\left|000\right\rangle - b\left|111\right\rangle$$

Quantum Error Correction

Z Correcting Codes



We need a scheme that corrects Z errors
but does not correct X errors.

To do this let us define →

$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$|-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

Now

$$Z|+\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = |-\rangle$$

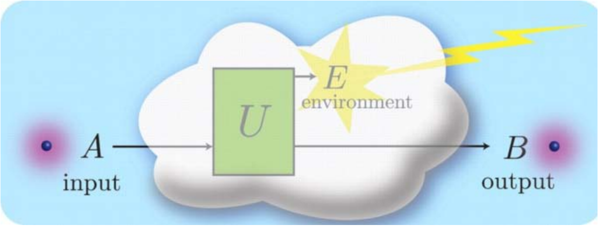
We see

$$Z|+\rangle = |-\rangle$$

$$Z|-\rangle = |+\rangle$$

Quantum Error Correction

Z Correcting Codes



We can protect any single qubit *Z*-type error by encoding |+> and |-> states as

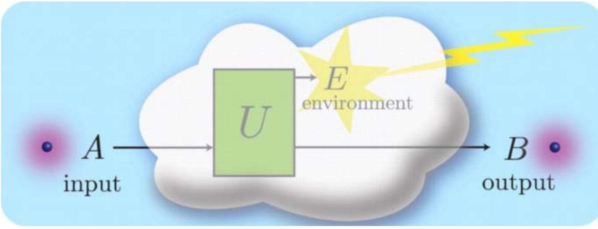
$$|+\rangle_c = |+++\rangle = \frac{1}{2\sqrt{2}}\Big(\big(|0\rangle+|1\rangle\big)\otimes\big(|0\rangle+|1\rangle\big)\otimes\big(|0\rangle+|1\rangle\big)\Big)$$

$$|-\rangle_c = |---\rangle = \frac{1}{2\sqrt{2}}\Big(\big(|0\rangle-|1\rangle\big)\otimes\big(|0\rangle-|1\rangle\big)\otimes\big(|0\rangle-|1\rangle\big)\Big)$$

Again we have appended two additional qubits, just as before

Quantum Error Correction

Z Correcting Codes



We can now correct any *Z*-type error by projecting into subspaces similar to the *X* case where we used

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$
$$P_4 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

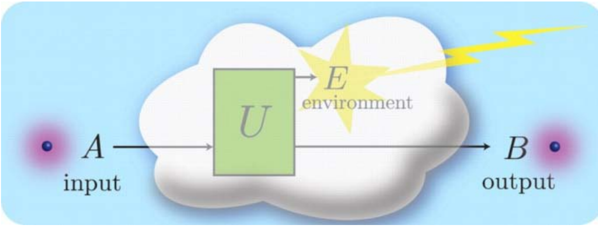
What are the new projection operators will be for *Z* errors?

(hint)

$$X|1\rangle = |0\rangle \qquad Z|+\rangle = |-\rangle$$
$$X|0\rangle = |1\rangle \qquad Z|-\rangle = |+\rangle$$

Quantum Error Correction

Z Correcting Codes



Yep, you got it

PS. This is the real addition symbol in the middle – not a state!

$$Q_1 = |-++\rangle\langle -++| + |+--\rangle\langle +--|$$

$$Q_2 = |+-+\rangle\langle +-+| + |-+-\rangle\langle -+-|$$

$$Q_3 = |++-\rangle\langle ++-| + |--+\rangle\langle --+|$$

$$Q_4 = |+++\rangle\langle +++| + |---\rangle\langle ---|$$

Just as before an error correction (Z-matrix) multiplies a qubit depending where the subspace measurement found (which Q found)

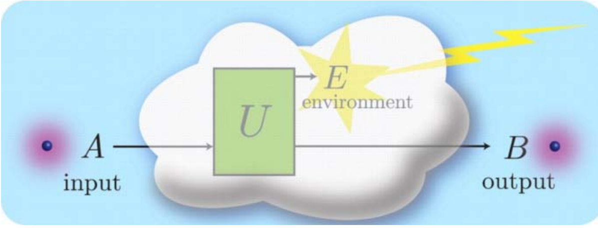
One can show that not only does this scheme protect against error of form

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

....but also of form $V = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$

Quantum Error Correction

The Shor Code



The Shor Code (1995) combines *X* and *Z* error correction techniques that protects against all single bit errors. We only briefly outline main points of this this code

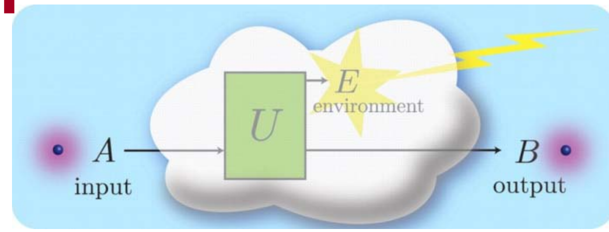
It appends ***eight*** additional qubits to a standard state

$$|s\rangle = a|0\rangle + b|1\rangle$$

A composite nine particle system results in a state vectors of length **2^9**

Quantum Error Correction

The Shor Code



In the Shor Code single qubit states end up being encoded as

$$|0\rangle_c = \frac{1}{2\sqrt{2}}\left(\left(|000\rangle + |111\rangle\right)\otimes\left(|000\rangle + |111\rangle\right)\otimes\left(|000\rangle + |111\rangle\right)\right)$$

$$|1\rangle_c = \frac{1}{2\sqrt{2}}\left(\left(|000\rangle - |111\rangle\right)\otimes\left(|000\rangle - |111\rangle\right)\otimes\left(|000\rangle - |111\rangle\right)\right)$$

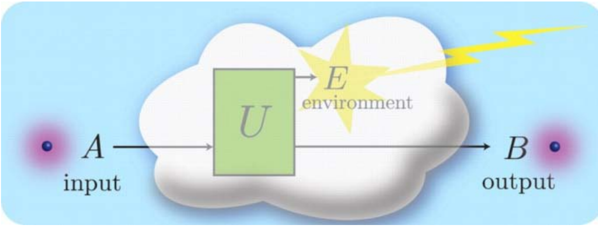
By looking back you can see that the form of the *Z*-error correcting scheme has been used here except that the *X*-error mapping below has been used

$$|0\rangle \rightarrow |000\rangle$$

$$|1\rangle \rightarrow |111\rangle$$

Quantum Error Correction

The Shor Code



Consider the 27 possible single qubit errors

$$X_1 \ldots X_9$$

$$Z_1 \ldots Z_9$$

$$X_1 Z_1 \ldots X_9 Z_9$$

It turns out that some of the Z error cannot be distinguished (only 3 independent0 (but have same error correction) –

We end up having have 22 (9X's, 9XZ's, 3Z's, one I) unique error corrections (including *I* matrix =no error)

Also every single qubit error can be written as some linear superposition of the 22 matrices

(most important is the need for an extra subspace than contains 2^9-44=468 dimensions associated with multiple qubit error errors)

(Shor 1995)

Quantum Communications –
Concepts you need to know (as we move along)

What is a Photon?
It is likely more than you thought (prior to 1992)

The Qubit
The Itsybitsy basic resource source of all quantum communications

The No Cloning Theorem
Copying classical information is easy, but try copying quantum information.

Quantum Entanglement
Why Einstein was wrong and right at same time.

Quantum Teleportation
Communication of quantum state information (magically)

The Infinite Qudit
Just when you thought this was all too easy…….

Discrete vs. Continuous Quantum Systems

- **Discrete**
  - The standard unit of information is the qubit
  - Qubits are typically associated with single photon states
  - Information coding by using properties, e.g. the polarization of the photon
  - **Drawback (?)** single photon production (on demand) and detection is somewhat difficult.
- **Continuous**
  - laser beams easy to produce
  - amplitude and phase properties of the light easy to measure
  - measurements: yields information about the field quadratures of a quantum state
  - All done using standard "off-the shelf" optical equipment
  - **Drawback (?)** Theoretical issues not as well developed e.g formal proofs of security for wide range of operating conditions.

CV Systems

- Continuous-variable (CV) quantum systems
- Quantized electromagnetic field
- Quantum harmonic oscillator
- Heisenberg uncertainty principle
- Fock states
- Coherent states
- Squeezed states
- Continuous variable quantum key distribution (CV QKD)

Alternate Quantum Systems

- **Discrete variable systems**
  - A quantum system having a finite-dimensional Hilbert space

- **Qubits** $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad |\alpha|^2 + |\beta|^2 = 1$
  - A quantum system having a two-dimensional Hilbert space
  - Spin, polarisation, etc.

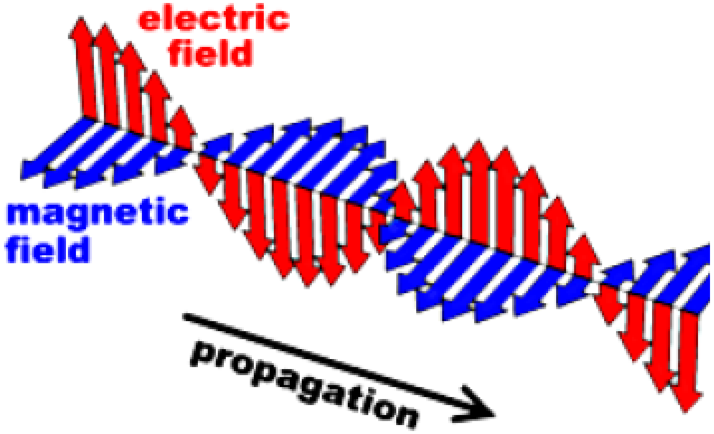
- **Qudits** $|\psi\rangle = \sum_{n=0}^{D-1} \alpha_n |n\rangle, \qquad \sum_{n=0}^{D-1} |\alpha_n|^2 = 1$
  - A qudit is a generalization of the qubit to a D-dimensional Hilbert space

Now, assume $D \to \infty$ ⟹ **Continuous variable systems**

Continuous Variable (CV) Quantum System

A quantum system is called a CV system when it has an infinite-dimensional Hilbert space described by observables with continuous eigenspectra.

- For instance amplitude & phase quadratures of light (polar)
- Or its quadratures $\hat{X}$ & $\hat{P}$ (Cartesian)
- $\hat{X}$ ~ electric field, $\hat{P}$ ~ magnetic field
- Or position $\hat{x}$ and momentum $\hat{p}$ of a free particle



Quantized Electromagnetic Field


Quantwiki.org

Source free

$$\nabla \times \mathbf{E} + \frac{\partial \mathbf{B}}{\partial t} = 0$$
$$\nabla . \mathbf{E} = 0$$
$$\nabla . \mathbf{B} = 0$$
$$\nabla \times \mathbf{B} - \varepsilon\mu \frac{\partial \mathbf{B}}{\partial t} = 0$$

$$\mathbf{E}(r,t) = \sum_{k,s} E_k \mathbf{e}_k^{(s)} \left[\alpha_{k,s} e^{i(kr-\omega_k t)} + \alpha_{k,s}^* e^{-i(kr-\omega_k t)} \right]$$

$$E_k = \left(\frac{h\omega_k}{4\pi\varepsilon_0} \right)^{1/2}$$

Promote Fourier components $\alpha_{k,s}$ to operators $\hat{a}_{k,s}$

The classical **E** field is the expectation value of the quantum operator $\hat{\mathbf{E}}$

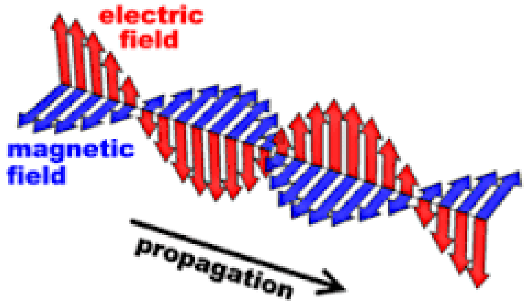

wattsupwiththat.com

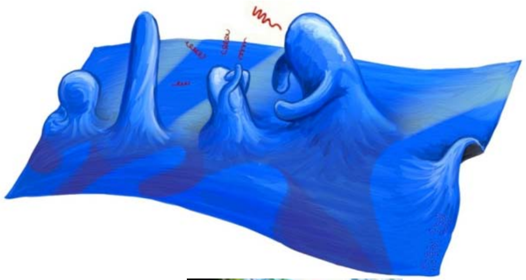
$$\left[\hat{a}_{k,s}, \hat{a}_{k',s'}^\dagger \right] = \delta_{kk'}\delta_{ss'},$$
$$\left[\hat{a}_{k,s}, \hat{a}_{k',s'} \right] = 0$$
$$\left[\hat{a}_{k,s}^\dagger, \hat{a}_{k',s'}^\dagger \right] = 0$$

$$\hat{\mathbf{E}}(r,t) = E_0 \mathbf{e} \left[\hat{X} \cos(kr - \omega t) + \hat{P} \sin(kr - \omega t) \right]$$
$$\hat{X} = \frac{1}{\sqrt{2}} \left(\hat{a} + \hat{a}^\dagger \right)$$
$$\hat{P} = \frac{1}{\sqrt{2}} \left(\hat{a} - \hat{a}^\dagger \right)$$

Quantized Electromagnetic Field

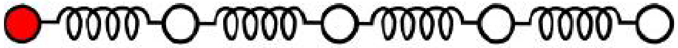
- The prototype of a CV system is represented by N modes, corresponding to N quantized modes of the electromagnetic field.
- A mode refers to a single degree of freedom of the electromagnetic field, e.g. polarization, frequency

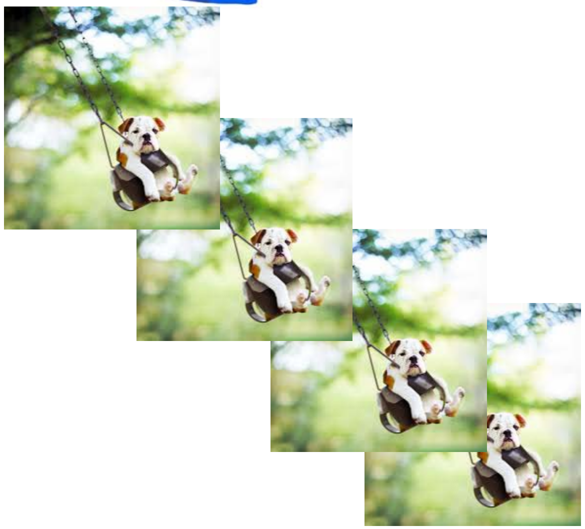




Dampt.cam.ac.uk

A system of N modes can be modeled as a collection of N quantum harmonic oscillators with different frequencies.





helentronica.com

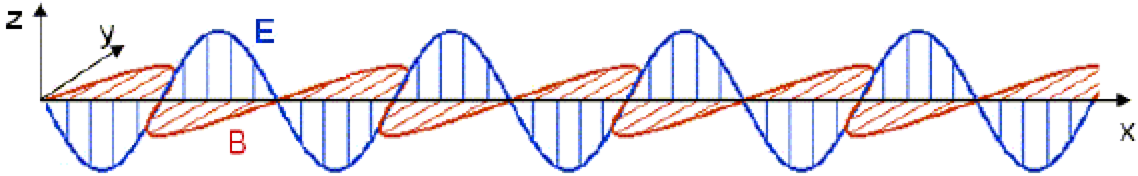
Quantized Electromagnetic Field

A single-mode field is equivalent to a harmonic oscillator

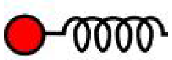
the electric and magnetic fields play the roles of position and momentum.

The quadrature field operators $\hat{X}$ and $\hat{P}$:

act similar to the position and momentum operators of the quantum harmonic oscillator.



UNSW ENGINEERING
THE UNIVERSITY OF NEW SOUTH WALES



Quantum Harmonic Oscillator

Quantum harmonic oscillator of unit mass, is described by the Hamiltonian (energy)

$$\hat{H} = \frac{\hbar}{2}\left(\omega^2 \hat{X}^2 + \hat{P}^2\right)$$

Canonical commutation relation ($\hbar = 1$)

$$\left[\hat{X}, \hat{P}\right] = i$$

The operators $\hat{X}$ and $\hat{P}$ are Hermitian and therefore correspond to observable quantities.

Quantum Harmonic Oscillator

It is convenient, to introduce the non-Hermitian (and therefore non-observable) annihilation ($\hat{a}$) and creation ($\hat{a}^{\dagger}$) operators (or Ladder operators)

- Annihilation (lowering) operator $$\hat{a} = \frac{1}{\sqrt{2}}\left(\hat{X} + i\hat{P}\right)$$
- Creation (raising) operator $$\hat{a}^{\dagger} = \frac{1}{\sqrt{2}}\left(\hat{X} - i\hat{P}\right)$$

$$\left[\hat{a}, \hat{a}^{\dagger}\right] = 1$$

$$H = \hbar\omega\left(\hat{a}^{\dagger}\hat{a} + \frac{1}{2}\right)$$

Fock States

Number operator $\hat{n} = \hat{a}^{\dagger}\hat{a}$

Fock states $\left\{|n\rangle\right\}_{n=0}^{\infty}$: eigenstates of the number operator

$$\hat{n}|n\rangle = n|n\rangle$$

or Fock states $\left\{|n\rangle\right\}_{n=0}^{\infty}$: energy eigenstate of the single mode field with the energy eigenvalue

$$\hat{H}|n\rangle = E_n|n\rangle, \qquad E_n = \hbar\omega\left(n + \frac{1}{2}\right)$$

Fock states are orthonormal, and form a basis for single-mode Hilbert space

$$\langle n|m\rangle = \delta_{nm}$$

Fock States

When the harmonic oscillator describes an electromagnetic (light) field, $|n\rangle$ represents a state of the field with exactly *n* photons.

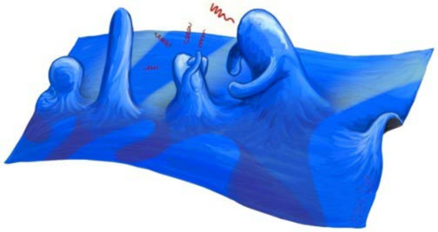
The creation and annihilation operators create and destroy photons, respectively

$$\hat{a}^{\dagger}|n\rangle = \sqrt{n+1}\,|n+1\rangle$$

$$\hat{a}|n\rangle = \sqrt{n}\,|n-1\rangle$$

Vacuum state $|0\rangle$ - State containing no photons

(State of minimal energy)



$$|n\rangle = \frac{1}{\sqrt{n!}}\left(\hat{a}^{\dagger}\right)^{n}|0\rangle$$

Heisenberg Uncertainty Principle

$$\sigma_X \sigma_P \geq \frac{\hbar}{2}$$

$$\sigma_X = \sqrt{\left\langle \hat{X}^2 \right\rangle - \left\langle \hat{X} \right\rangle^2} \ , \quad \sigma_P = \sqrt{\left\langle \hat{P}^2 \right\rangle - \left\langle \hat{P} \right\rangle^2}$$

$$\left\langle \hat{X} \right\rangle = \langle \psi | \hat{X} | \psi \rangle, \ \left\langle \hat{P} \right\rangle = \langle \psi | \hat{P} | \psi \rangle$$

In contrast to the classical case, a state of the quantum harmonic oscillator can never be a simple point in phase space. It always acquires some spread, to fulfil uncertainty principle

Heisenberg Uncertainty Principle

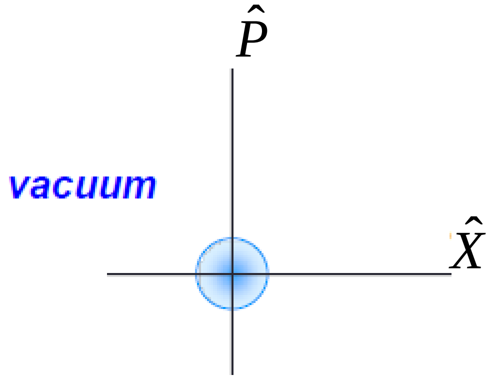
If we set $h = 1$

$$\sigma_X \sigma_P \geq \frac{1}{2}$$

For vacuum state $|0\rangle$

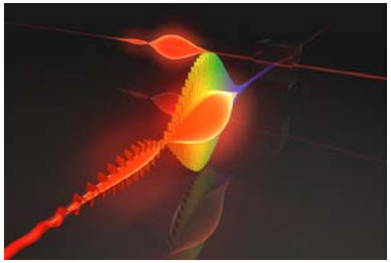
$$\sigma_X^2 = \frac{1}{2} = \sigma_P^2$$

$|0\rangle$: State of minimal uncertainty with equal uncertainties in position and momentum



Coherent States

Coherent state $|\alpha\rangle$: labelled by a complex number α and are the right eigenstates of the annihilation operator :



$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$$

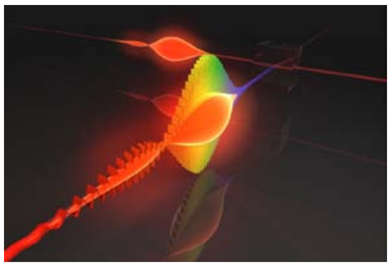
and can be expanded in the basis of Fock states as

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$$

Unlike the Fock states, the coherent states are not orthogonal

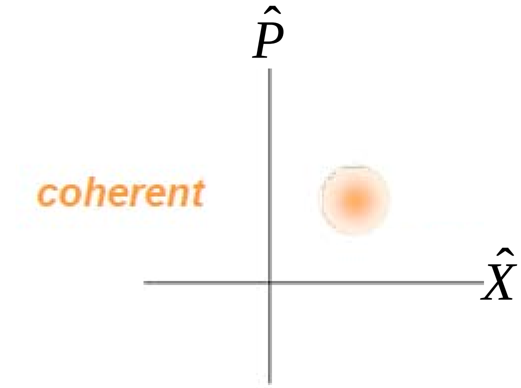
Coherent States

Coherent state $|\alpha\rangle$: can be described as vacuum states displaced from the origin of phase space



$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle$$

$$\hat{D}(\alpha) = \exp(-\alpha^* \hat{a} + \alpha \hat{a}^\dagger)$$



$|\alpha\rangle$: State of minimal uncertainty with equal uncertainties in position and momentum

$$\sigma_X^2 = \frac{1}{2} = \sigma_P^2$$

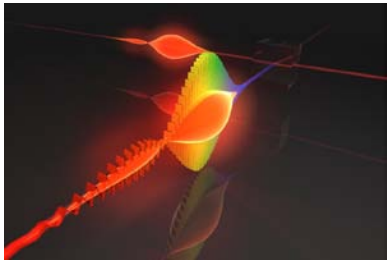
Coherent States

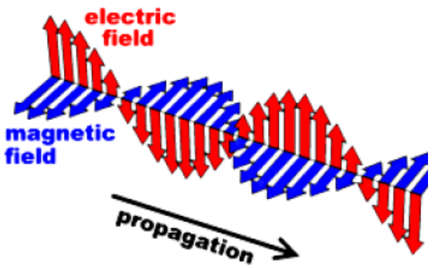
Expectation value of the number operator $\hat{n} = \hat{a}^\dagger \hat{a}$

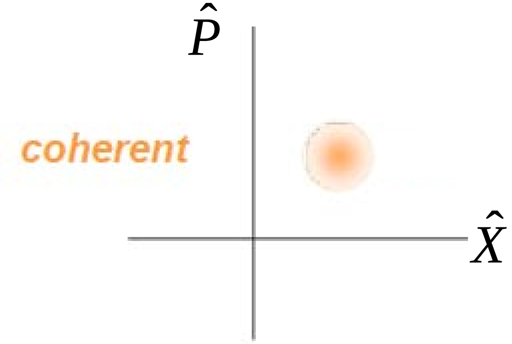
$$\langle \alpha | \hat{n} | \alpha \rangle = |\alpha|^2$$

For an electromagnetic field, $|\alpha|^2$ is the mean photon number in the coherent state. When the mean photon number becomes very large, the fixed uncertainties $\sigma_X^2 = 1/2 = \sigma_P^2$

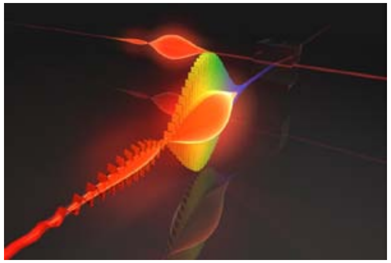
become negligible compared to the displacement from the origin of phase space, and the coherent state behaves like a classical phase space point.







Squeezed States



squeezed vacuum state $S(\xi)|0\rangle$

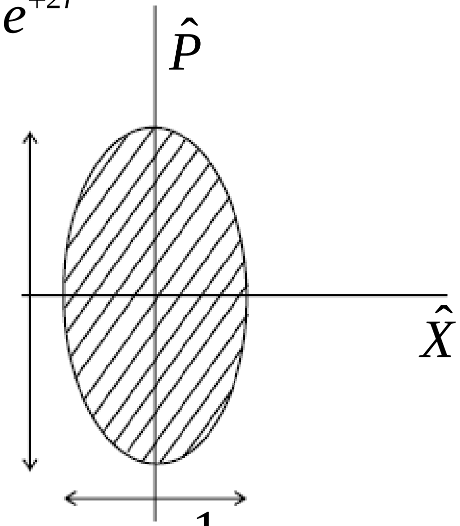
$$\hat{S}(\xi) = \exp\left(\frac{1}{2}\left(\xi^* \hat{a}^2 - \xi \hat{a}^{*^2}\right)\right)$$

Uncertainty in one of quadratures
is below that of the vacuum state

$$\sigma_X \neq \sigma_P$$

$$\sigma_X^2 < \frac{1}{2},\ \sigma_P^2 > \frac{1}{2},\quad \sigma_X \sigma_P \geq \frac{1}{2}$$

$$\sigma_P^2 = \frac{1}{2} e^{+2r}$$

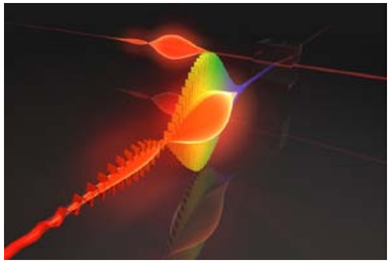


$$\sigma_X^2 = \frac{1}{2} e^{-2r}$$

Two-Mode Squeezed States

Two-mode squeezed vacuum state $\hat{S}_{12}(\xi)|0\rangle|0\rangle$:

$$\hat{S}_{12}(\xi) = \exp\left(\xi^* \hat{a}_1 \hat{a}_2 - \xi \hat{a}_1^* \hat{a}_2^*\right)$$



$S_{12}(r)$ does not factor as a product of two single-mode squeeze operators

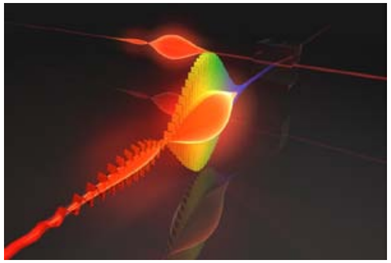
Two-mode squeezed vacuum state is not a product of two single-mode squeezed vacuum states

It is an entangled state containing strong correlations between the two modes.

Two-Mode Squeezed States

squeezed state ： $\hat{X}_+ = \frac{\hat{X}_1 + \hat{X}_2}{\sqrt{2}}, \hat{P}_- = \frac{\hat{P}_1 - \hat{P}_2}{\sqrt{2}}$

anti-squeezed $\hat{X}_- = \frac{\hat{X}_1 - \hat{X}_2}{\sqrt{2}}, \hat{P}_+ = \frac{\hat{P}_1 + \hat{P}_2}{\sqrt{2}}$



$$\sigma^2_{\hat{X}_+} = \sigma^2_{\hat{P}_-} = \frac{1}{2} e^{-2\xi}, \qquad \sigma^2_{\hat{X}_-} = \sigma^2_{\hat{P}_+} = \frac{1}{2} e^{+2\xi}$$

For $\xi = 0$, the state corresponds to two vacuum states

For $\xi > 0$, $\sigma^2_{\hat{X}_+} = \sigma^2_{\hat{P}_-} < \frac{1}{2}$

For $\xi \to \infty$, $\hat{P}_1 - \hat{P}_2 = p_0$, $\hat{X}_1 + \hat{X}_2 = x_0$ perfect (anti) correlation (maximal entanglement)

Achieving strong squeezing is experimentally challenging and an infinite level of squeezing is not physically possible

Creating
Two-Mode Squeezed States

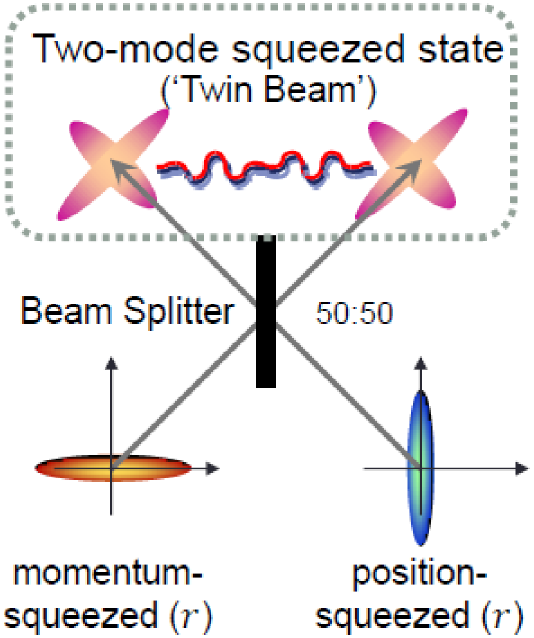


Image: Adesso, 2007

There are many ways two produce two-mode squeezed beams.

Now easy and standard work-horse of CV quantum communications.

Two-Mode Squeezed States

Two-mode squeezed vacuum state can also be expanded in the basis of Fock states as :

$$|\psi\rangle_{TMSV} = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}(-\lambda)^n |n\rangle_1 |n\rangle_2$$

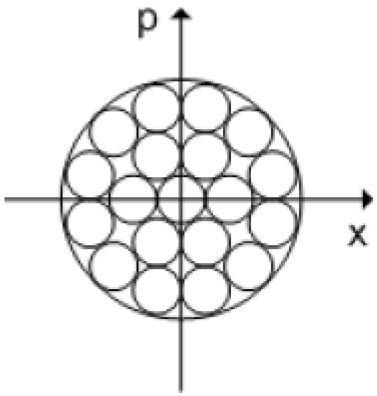
$$\lambda = \tanh(\xi)$$

This description represents the correlation between photon numbers (entanglement).

If I measure the photon numbers of beam 1, and obtain the eigenstate $|m\rangle$, which means there are m photons, I know for sure that there are m photons in beam 2. This works even if the two beams are far apart.

CV Quantum Key Distribution (CV QKD)

Sort of Similar to DV QKD !



CV Quantum Key Distribution (coherent state protocol)

The security is based on the fact that coherent states are non-orthogonal (no-cloning theorem applies)

(1) Alice generates two classical random variables each drawn from a Gaussian distribution a_x, a_p. Alice prepares a coherent state, displaced by (these variables are encoded onto a coherent state)

(2) For each incoming state, Bob draws a random bit u_0 and measures either the $\hat{X}$ or $\hat{P}$ quadrature based on u_0 , obtaining a_x or a_p

(3) Bob reveals his string of random bits u_0 and Alice keeping as the final string of data the values (a_x or a_p) matching Bob's quadrature.

(4) Alice informs Bob of which values she keeps

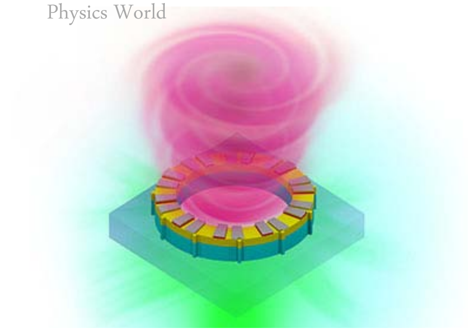
(5) Error correction and

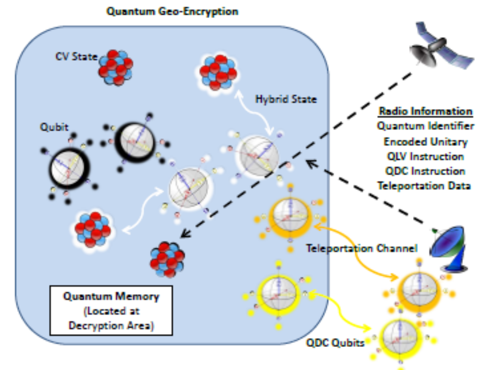
(6) Privacy amplification proceeds - both similar to DV protocol

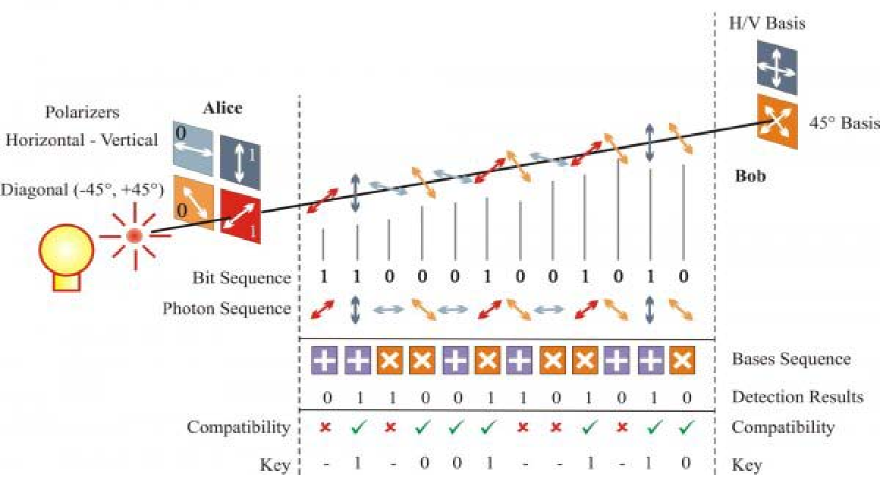
Emerging Quantum Applications
Quantum Communications

University of Vienna

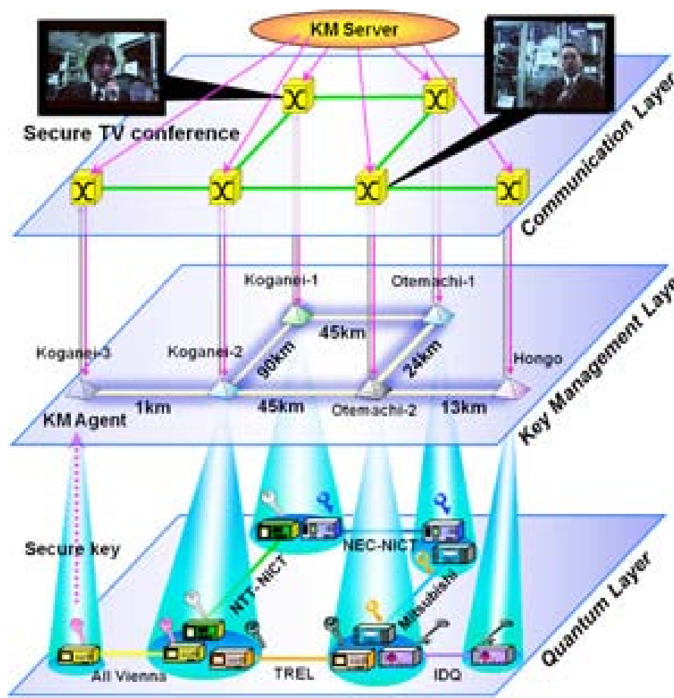
Physics World







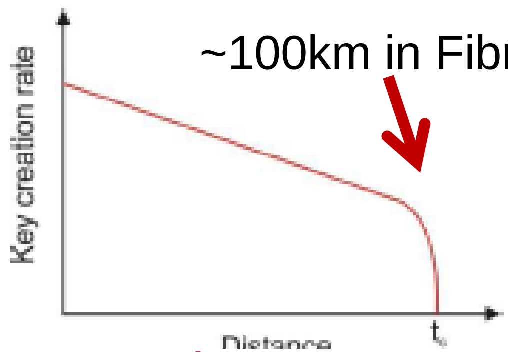
swissquantum.idquantique.com



UQCC-Tokyo

QKD (revisited) – Product Status

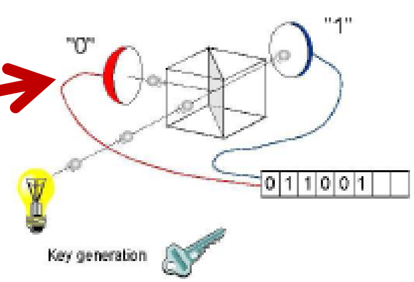
IDQuantique, Toshiba, MagiQ, SeQureNet, QinetiQ, Quintessence (CV states)

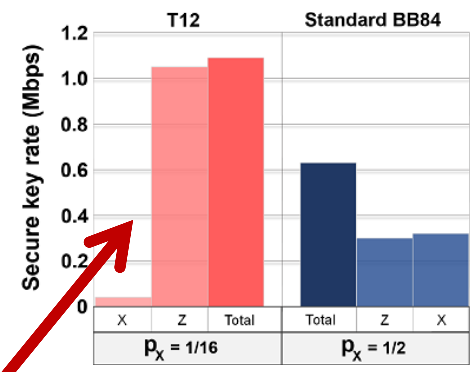


~100km in Fibre

Quantum Key Rate 1MB/s at 50km (Fibre)

- •**Provide secured quantum keys for any encryption device**
- •**Scalable: one quantum key server can distribute keys for up to 100Gbps of data**
- •**Fully automated key exchange with continuous key renewal**
- •**Integrated entropy source based on a**
- •**<u>Quantum Random Number Generator</u>**
- •**Adaptable: Works on dark fibre and**
- •**WDM networks**





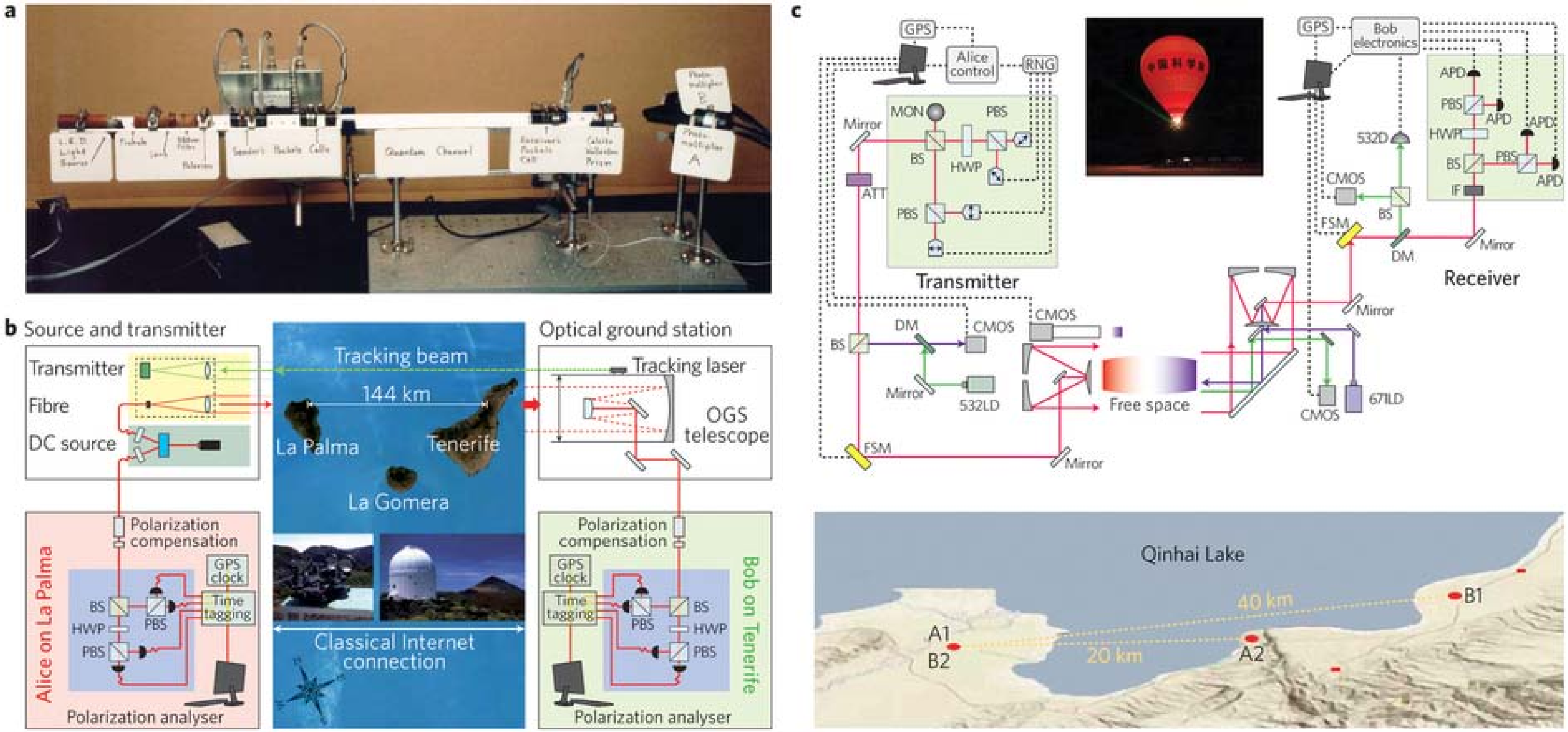
"Decoy" rate

Toshiba.com

ID Quantique.com

QKD (revisited) Status - Free Space

Lo et al 2014



a, First free-space demonstration of QKD[19] realized two decades ago over a distance of 32 cm. The system uses a light-emitting diode (LED) in combination with Pockels cells to prepare and measure the different signal states.

b, Entanglement-based QKD set-up connecting the two Canary Islands La Palma and Tenerife[6]. The optical link is 144 km long. OGS, optical ground station; GPS, Global Positioning System; PBS, polarizing beamsplitter; BS, beamsplitter; HWP, half-wave plate.

c, Schematic of a decoy-state BB84 QKD experiment between ground and a hot-air balloon[20].

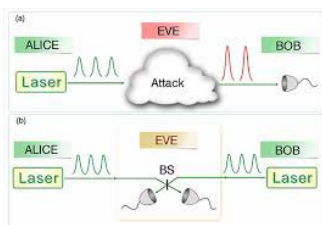
QKD (revisited) Status - Quantum Hacking

"Our hack gave 100% knowledge of the key, with zero disturbance to the system,"

Vadim Makarov

Vad1.com

Hackers blind quantum cryptographers
Lasers crack commercial encryption systems, leaving no trace.
Nature News.



The Next Battleground In The War Against Quantum Hacking
Ever since the first hack of a commercial quantum cryptography device, security specialists have been fighting back. Here's an update on the battle.
MIT Technology Review August 20, 2014

Google protects Chrome against quantum hacking before it can even happen!

Current internet encryption methods would have no way to stand up to quantum computers. Luckily, Google's working on it.

Cnet.com 2016

Images, zdnet.com, aps.org

QKD (revisited) Status - Security

Testing of Models
e.g. by embedding into larger models
- requires experience based cut-off

➔ no scientific proof possible

Software and Hardware Implementation
- verified software (development & execution)
- hardware security perimeter
- key management

Model of Devices
- e.g. quantum mechanical description
- quantum security perimeter
- classical security perimeter

Exact Protocol
- sequence of protocol steps
- Error Correction method
- Privacy Amplification function
- security parameters

Scientific Security Proof
"perfect secret key with exception of probability ^{2}"

Security Statement: The security statement of a QKD protocol is of a probabilistic nature. The final key can be claimed to be completely random and completely private, except with a probability ε. With that probability ε, one pessimistically assumes that an adversary might know the complete key. Any QKD device therefore shall have to quote not only the length of key that it creates in a given time over specified distances, but also the parameter ε associated with this key.

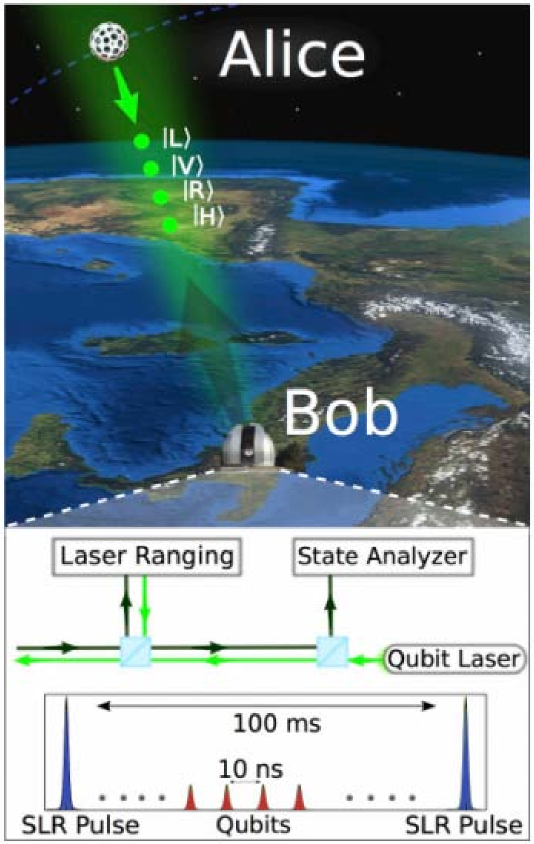
"Theoretical" unconditional security approaches perfection in infinite limit
(see also "Device Independent" QKD- later)

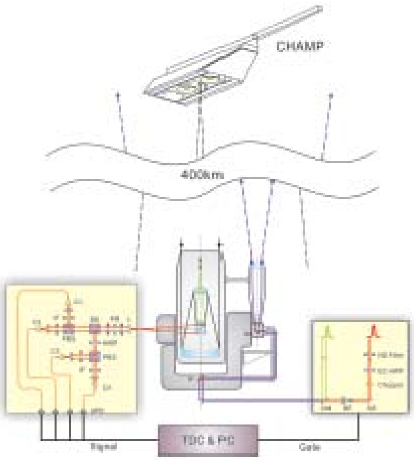
Images & text –ETSI. ISG

Satellite Communications - Status

Thehackernews.com. 2016

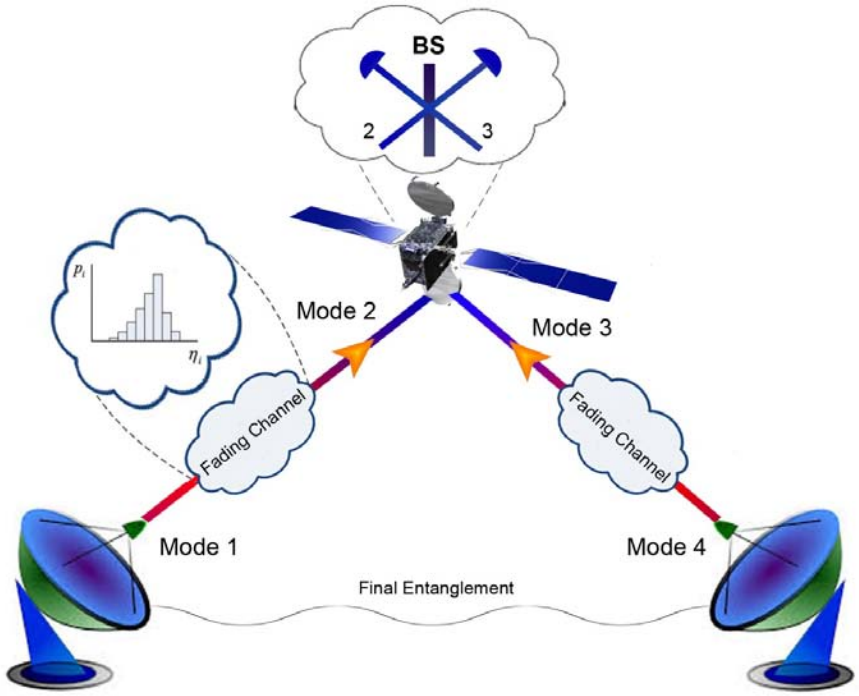
Will build on single photon tests bounced of satellite by Yin *et al* (2013) and error rate measurements by Vallone *et al* (2014).





UNSW ENGINEERING
THE UNIVERSITY OF NEW SOUTH WALES

QKD (revisited) – Device Independence

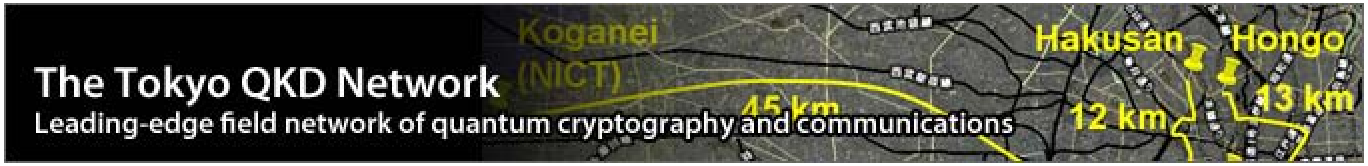


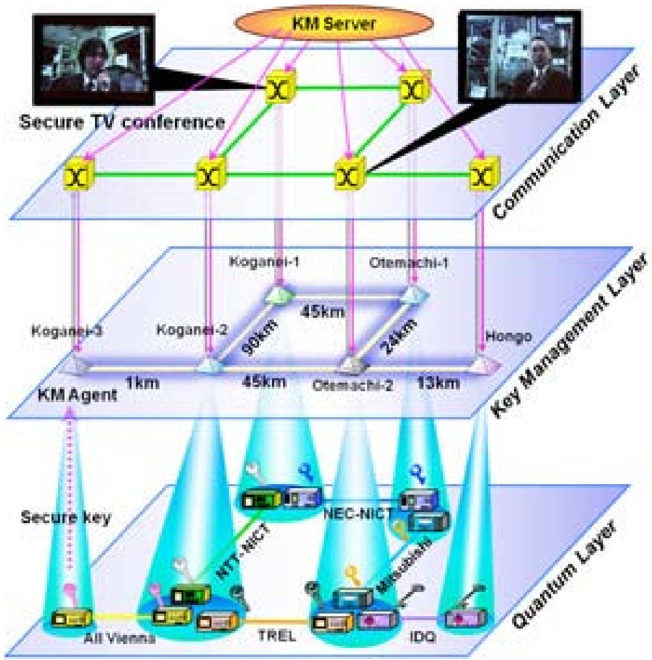
Every "prepare and measure" (PM) QKD has a corresponding "entanglement based" (EB) version.

As an example, based on EB analysis it can be shown how of positive key rates can be obtained from sending coherent pulses to a satellite
even if adversary controls the satellite

Hosseinidehaj & Malaney 2016a

Large Scale Systems – Towards the Quantum Internet





Operational performance of long-distance quantum key distribution over a field-installed 90-km fiber-optic loop

Images –http://www.uqcc.org/.

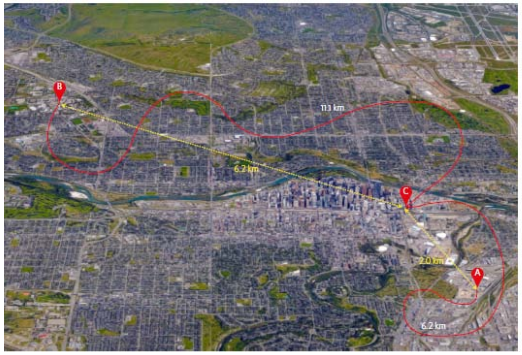
Large Scale Systems – Towards the Quantum Internet

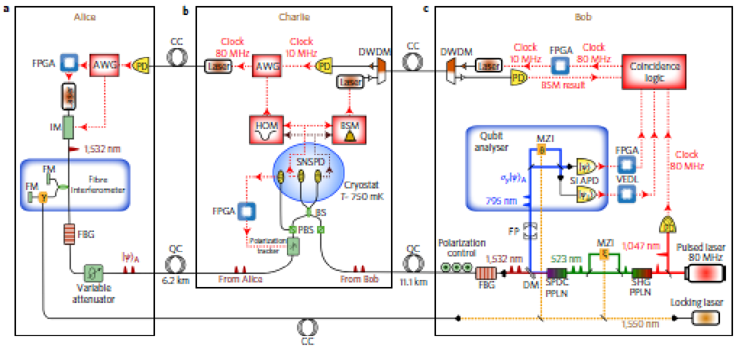
Two Recent Important Network Results

Hefei, China
Sun et al 2016.

However, in the past not a single quantum-teleportation experiment has been realized with independent quantum sources, entanglement distribution prior to the Bell-state measurement (BSM) and feedforward operation simultaneously, even in the laboratory environment. We take the challenge and report the construction of a 30 km optical-fibre-based quantum network distributed over a 12.5 km area.

Calgary, Canada
Valivarthi et al 2016.

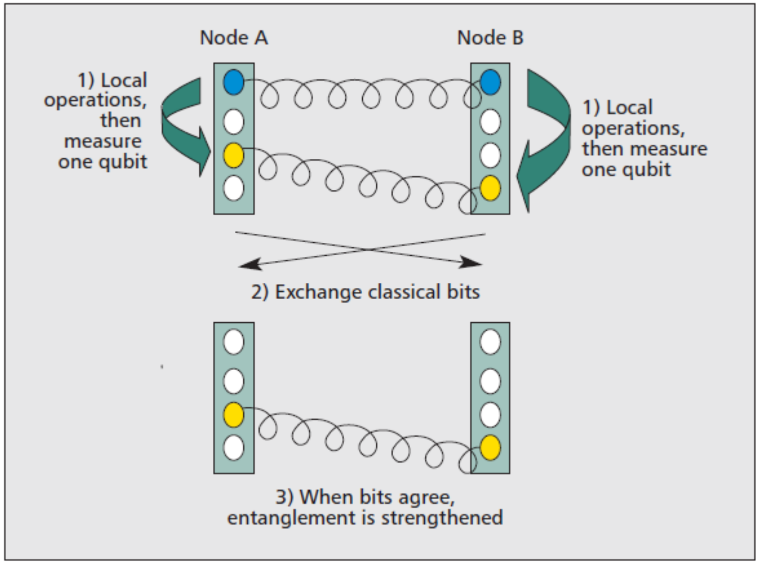




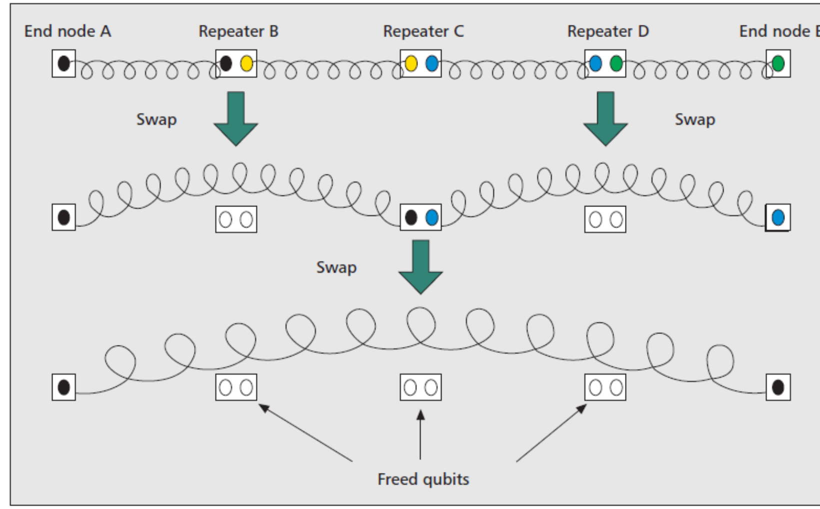
Here, using the Calgary fibre network, we report quantum teleportation from a telecom photon at 1,532 nm wavelength, interacting with another telecom photon after both have travelled several kilometres and over a combined beeline distance of 8.2 km, onto a photon at 795 nm wavelength. This improves the distance over which teleportation takes place to 6.2 km. Our demonstration establishes an important requirement for quantum repeater-based communications[5] and constitutes a milestone towards a global quantum internet[6].

Large Scale Systems – Towards the Quantum Internet

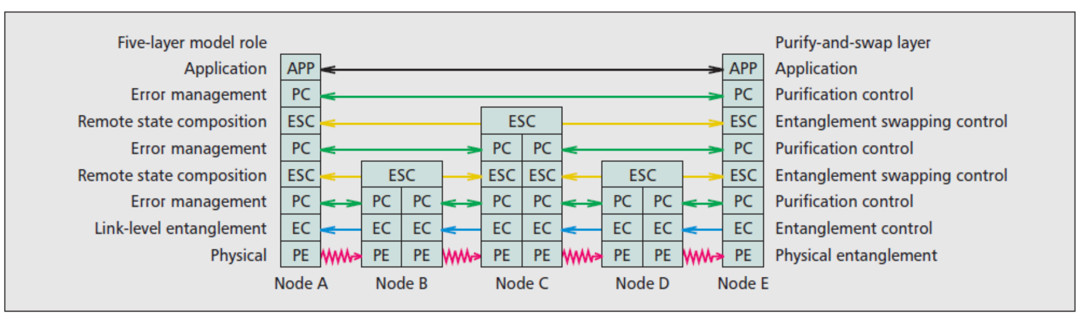
Enabling Technologies



Distillation



Entanglement Swapping



Network Control

Images –Van Meter, Touch, 2013.

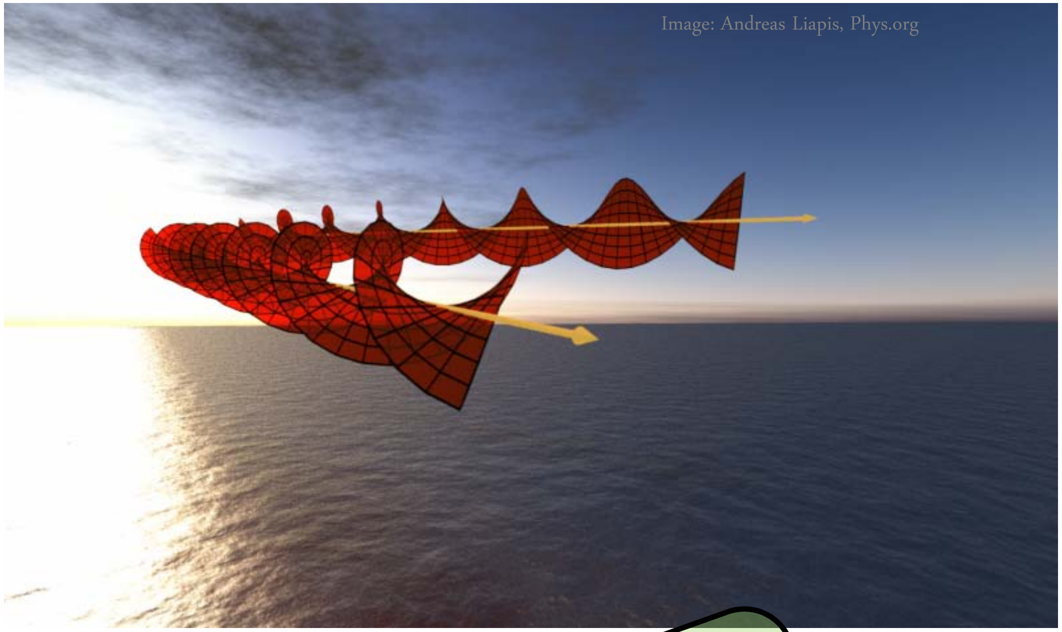
Large Scale Systems –
Towards the Quantum Internet

Large Scale Networks – The Ultimate Goal?

Figure 1. Multipartite quantum network based on graphs: network nodes together with links between them constitute a graph. Both network nodes and repeater stations receive and send quantum particles. They prepare qubits (in the $|+\rangle$-state), perform entangling quantum gates (C_Z-gates) and measurements (in the X-basis). The number of such actions for a given node depends on its number of neighbours. Arrows indicate the transmission direction. Some examples are illustrated. Note that repeater stations have exactly two neighbours, while network nodes may have more than two neighbours.

Epping et al 2016.

Orbital Angular Momentum (OAM)



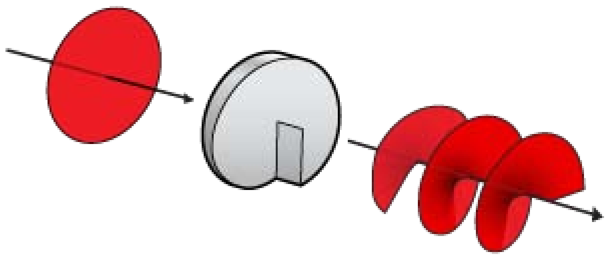
Twisted Light Could Dramatically Boost Data Rates

Orbital angular momentum could take optical and radio communication to new heights

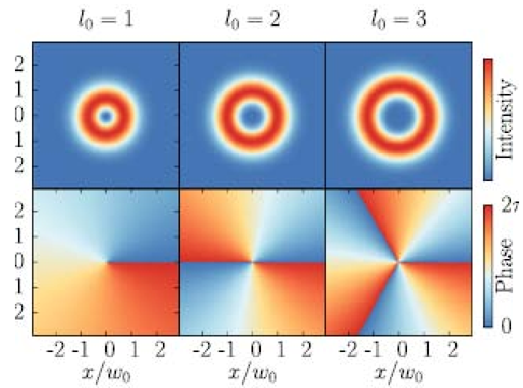
IEEE Spectrum 2016

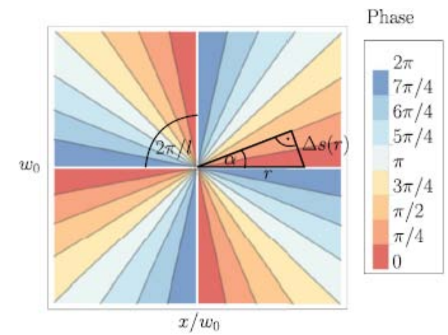
Orbital Angular Momentum (OAM)

Image: J. Provost, IEEE Spectrum



Leonhardt et al 2015

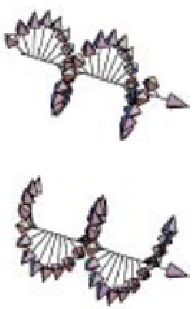


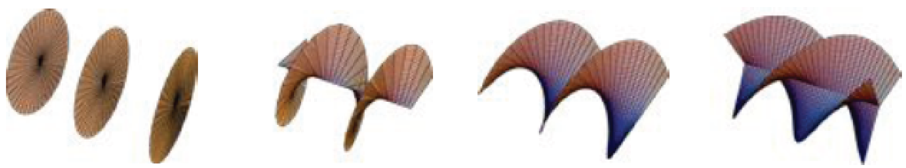


- Spin angular momentum
  - Circular polarisation
  - $\sigma\hbar$ per photon
- Orbital angular momentum
  - Helical phasefronts
  - $\ell\hbar$ per photon

$\sigma = +1$

$\sigma = -1$





$\ell = 0$ $\ell = 1$ $\ell = 2$ $\ell = 3$ etc

Image: Miles Padgett

Orbital Angular Momentum (OAM)

Cylindrically symmetric solutions to the EM wave equation

Laguerre polynomial with p + 1 radial nodes

Gaussian with beam waist

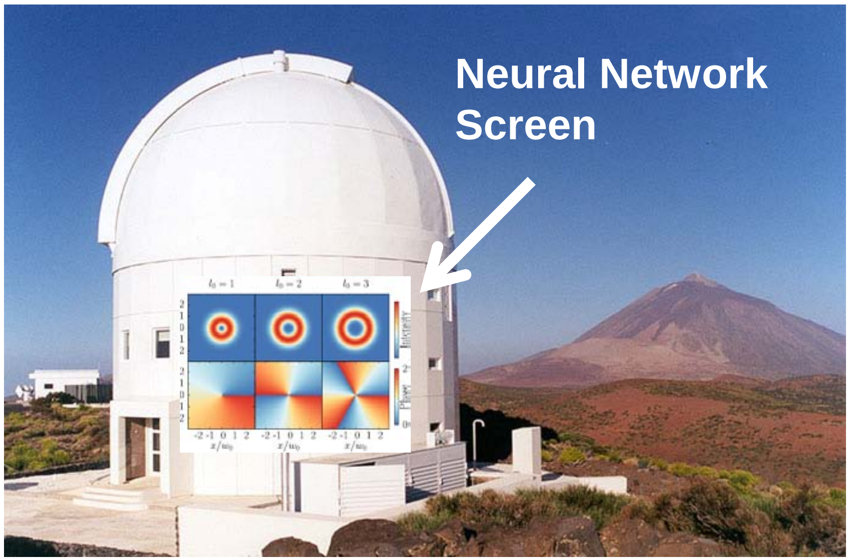
$$u_p^\ell(r,\phi) \propto r^\ell L_p^\ell\left(2r^2/\omega^2\right) e^{-r^2/\omega^2} e^{-i\ell\phi}$$

Laguerre-Gaussian modes

Vortex with ***topological charge*** ℓ

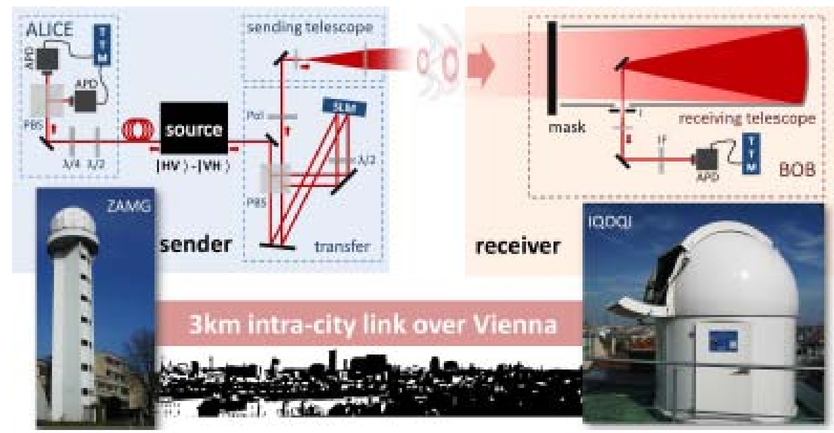
Orbital angular momentum ℓh per photon

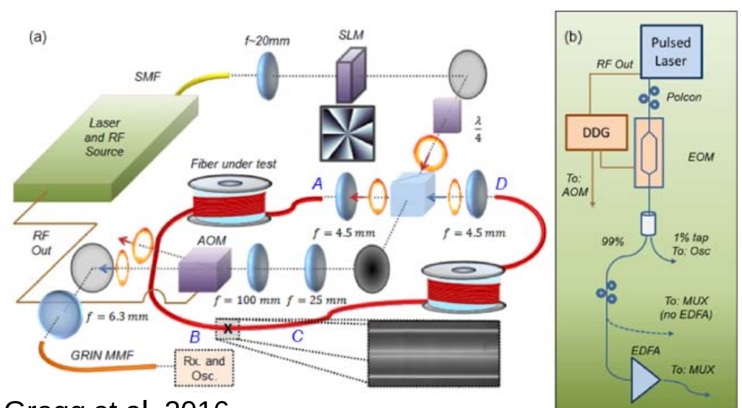
Orbital Angular Momentum (OAM)



143km through air – Krenn et al, 2016

3km through air – Krenn et al, 2014
(16 Multiplexed)





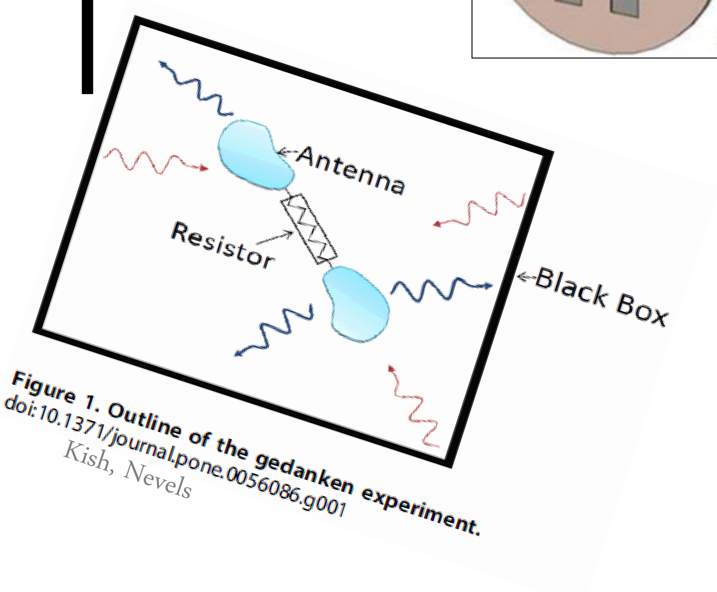
13km through fibre - Gregg et al, 2016

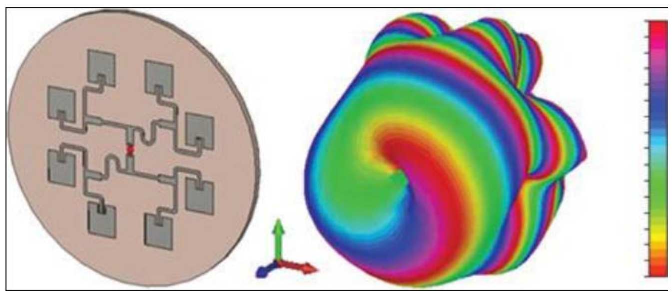
UNSW ENGINEERING
THE UNIVERSITY OF NEW SOUTH WALES

Orbital Angular Momentum (OAM) Radio

Towards infinite-capacity wireless networks, with twisted vortex radio waves
ExtremeTech.com Sept. 2014

?

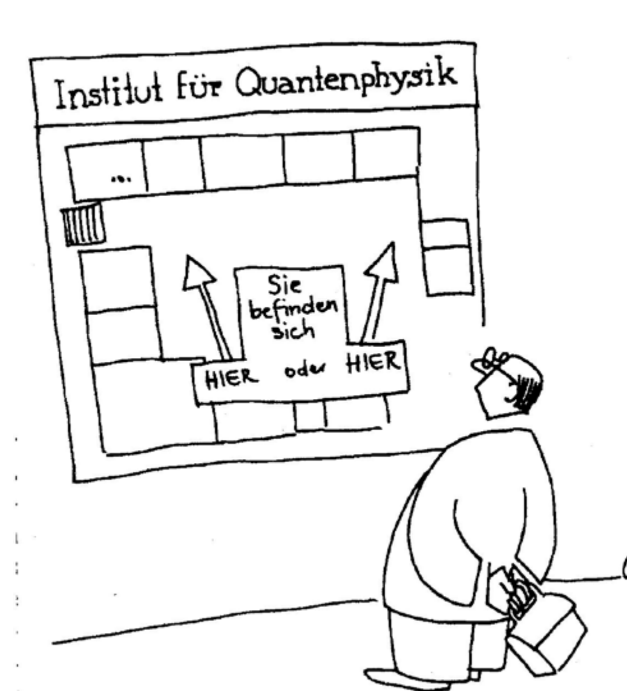




MIMO-Radio Based OAM,
Bai et al 2014

But where is the Far **Field?**

The Far Side



Orbital Angular Momentum (OAM) - Radio

But where is the Far **Field?**

A) Sort of far………..

TABLE 1—DEFINITIONS OF THE NEAR-FIELD/FAR-FIELD BOUNDARY

Definition for shielding	Remarks	Reference
$\lambda/2\pi$	1/r terms dominant	Ott, White
$5\lambda/2\pi$	Wave impedance=377Ω	Kaiser
For antennas		
$\lambda/2\pi$	1/r terms dominant	Krause
3λ	D not >>λ	Fricitti, White, Mil-STD-449C
$\lambda/16$	Measurement error<0.1 dB	Krause, White
$\lambda/8$	Measurement error<0.3 dB	Krause, White
$\lambda/4$	Measurement error<1 dB	Krause, White
$\lambda/2\pi$	Satisfies the Rayleigh criteria	Berkowitz
$\lambda/2\pi$	For antennas with D<<λ and printed-wiring-board traces	White, Mardiguian
$2D^2/\lambda$	For antennas with D>>λ	White, Mardiguian
$2D^2/\lambda$	If transmitting antenna has less than 0.4D of the receiving antenna	MIL-STD 462
$(d+D)^2/\lambda$	If d>0.4D	MIL-STD 462
$4D^2/\lambda$	For high-accuracy antennas	Kaiser
$50D^2/\lambda$	For high-accuracy antennas	Kaiser
$3\lambda/16$	For dipoles	White
$(D^2+d^2)/\lambda$	If transmitting antenna is 10 times more powerful than receiving antenna, D	MIL-STD-449D

98 EDN | August 16, 2001 www.ednmag.com

Capps, 2001

Orbital Angular Momentum (OAM) - Radio

Thide et al 2007

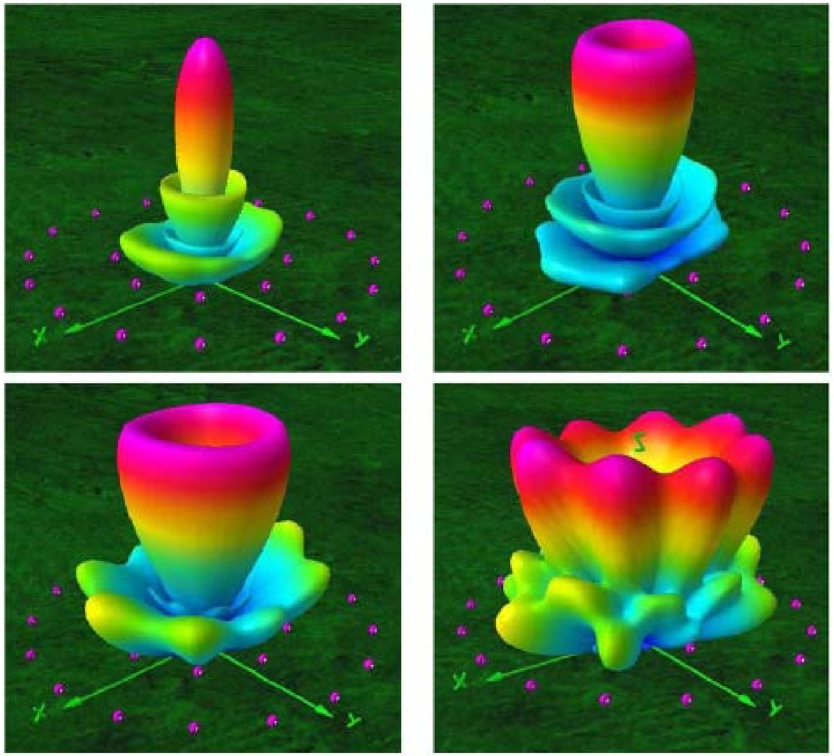


FIG. 1 (color online). Radiation patterns for radio beams generated by one circle of 8 antennas and radius λ plus a concentric circle with 16 antennas and radius 2λ; all antennas are 0.25λ over the ground. Notice the influence of l on the radiation pattern. Here $l = 0$ (upper left), $l = 1$ (upper right), $l = 2$ (lower left), and $l = 4$ (lower right).

Edfors, Johansson,2011

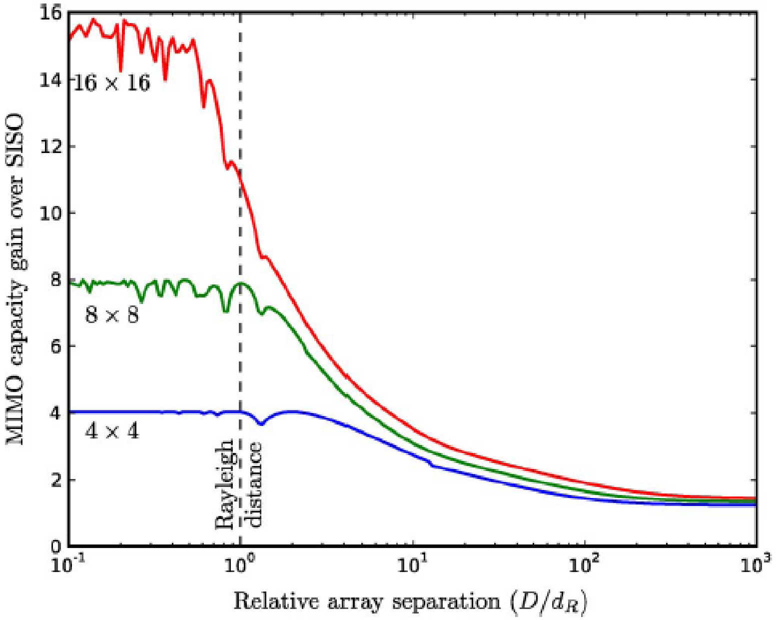
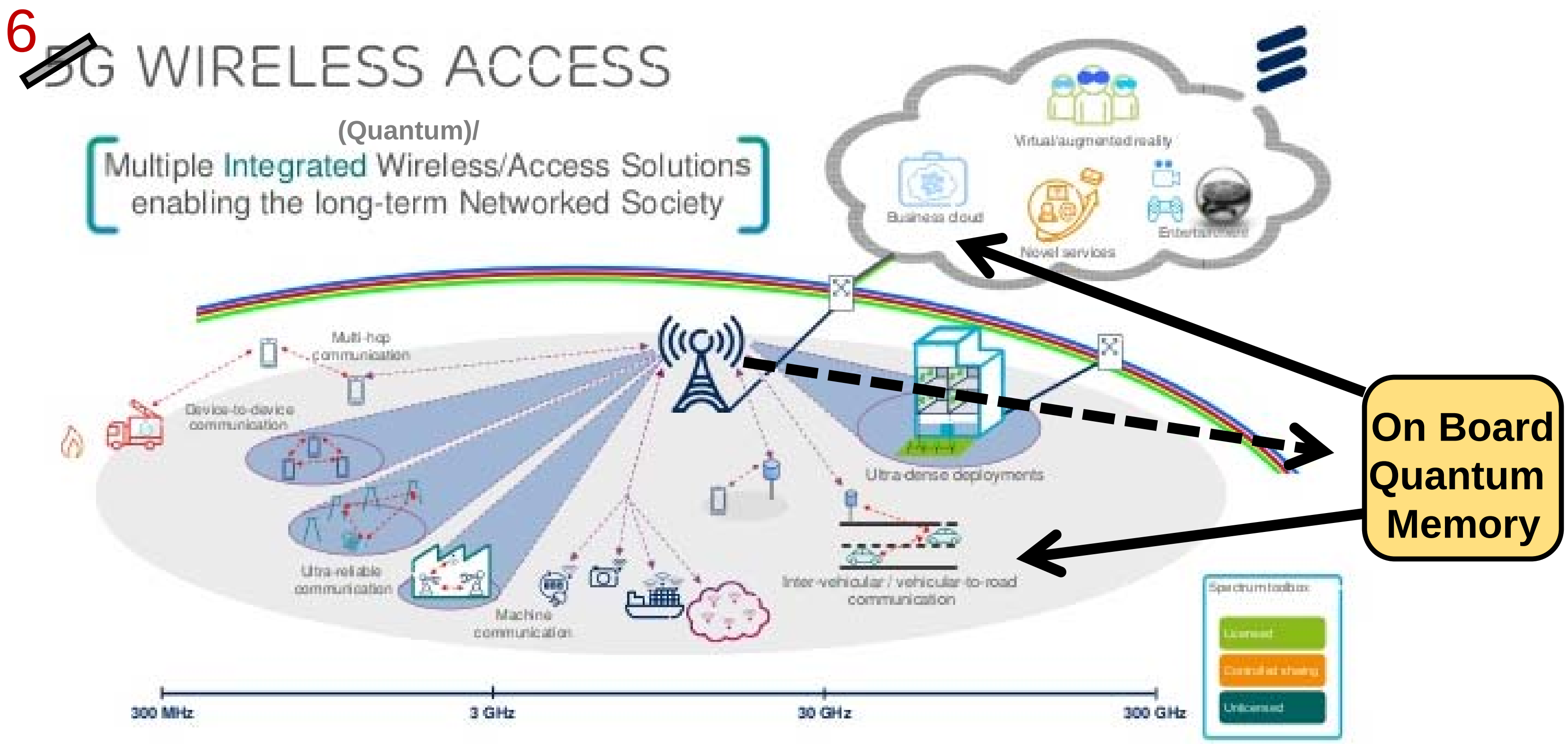


Fig. 6. Capacity gain over single antenna (SISO) system at at UCA sizes 4×4, 8×8, and 16×16, at an SNR of 30 dB. Curves are calculated for array radii 100λ and array separation distances from 10 times below to 1000 times above the Rayleigh distance (20.0000λ).

6G
Combined Quantum-Wireless Networks

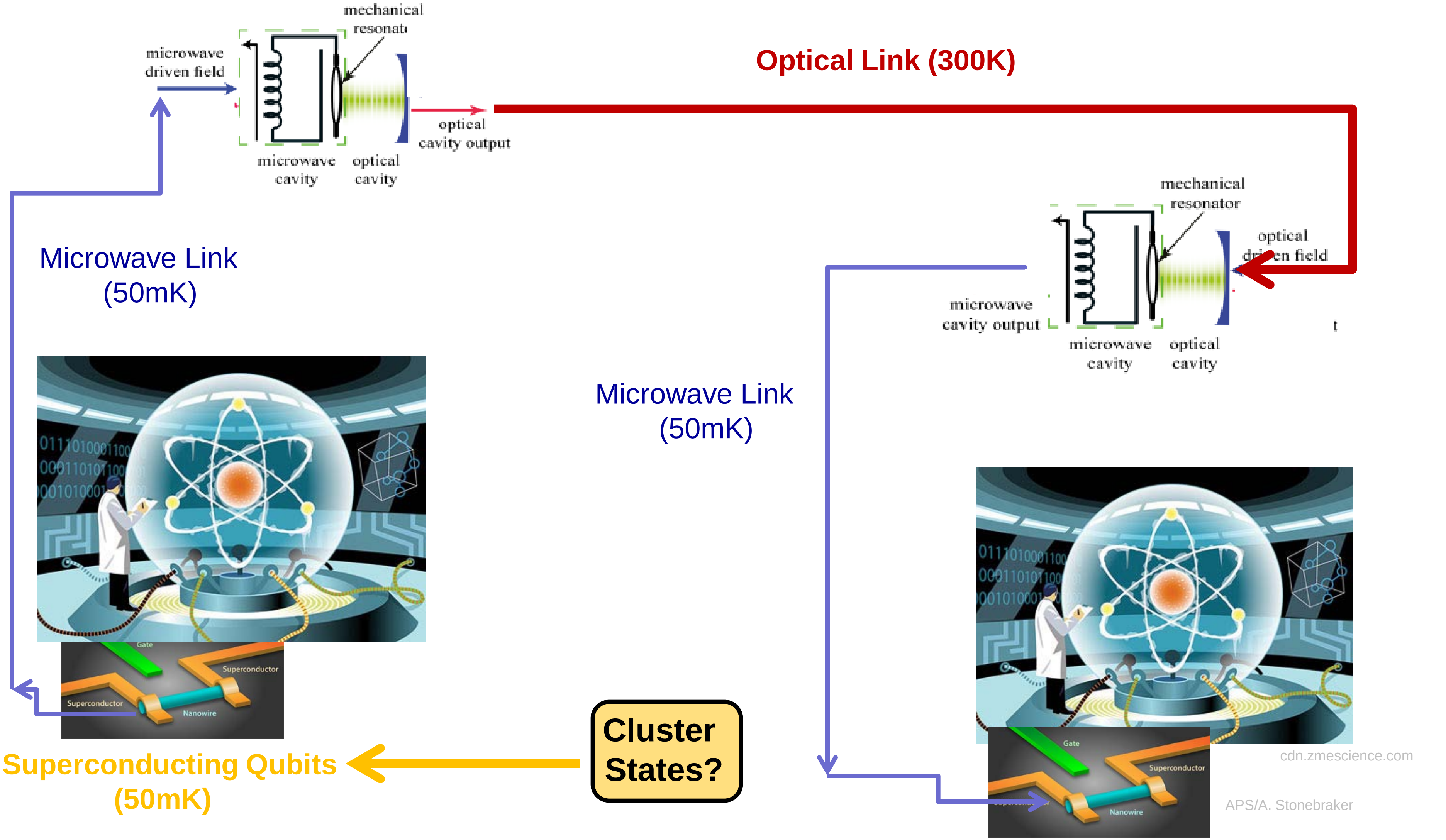
Modified from Forbes.com



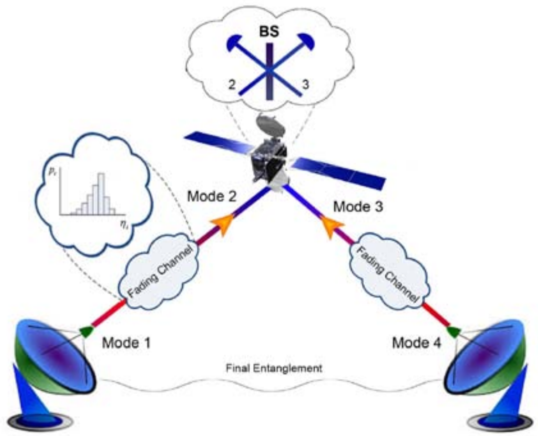
e..g. Malaney 2016a

Communications for Quantum Computers

Barzanjeh et al 2015



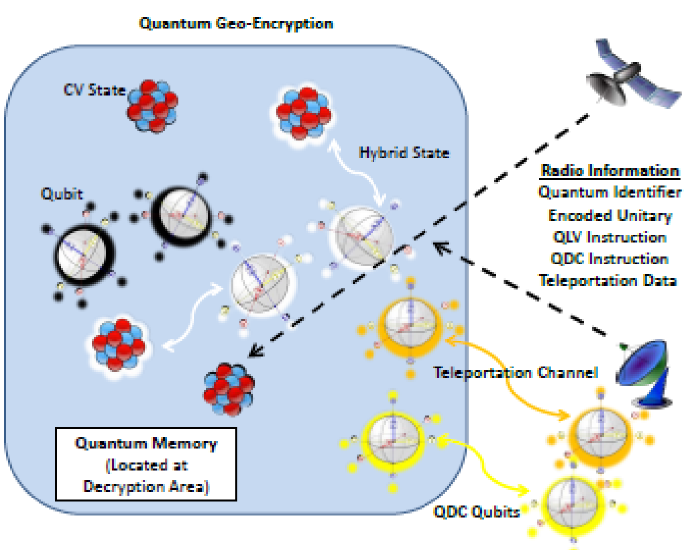
Some of my own work at this meeting



Generating quantum keys from Earth-to-Space with **laser pulses** (CV QKD)

I will be presenting a technical paper on "*CV-QKD with Gaussian and non-Gaussian Entangled States over Satellite-based Channels"* during the meeting
SAC-SSC.2: System Tuesday 11am

Hosseinidehaj & Malaney 2016b



Use quantum states to **ensure** data can **only** be decrypted at a **specific location** and time

I will be presenting a technical paper on *"Quantum geo-encryption"* during the meeting
CISS.9: Cryptography and Network Security, Wednesday 11am

Malaney 2016b

6G is coming….

THE q-PHONE

Quantum Neural Network Processor

Driverless Car Collision Avoidance

Embedded Quantum Memory

1TB Data Transfer

Massive MIMO Millimetre Beamforming Reception

Entanglement On Demand

Teleportation On Demand

Location-Based Quantum Encryption

Quantum Bitcoin

General Relativistic Corrections to Quantum Satellites

"Un-hackable" Communications

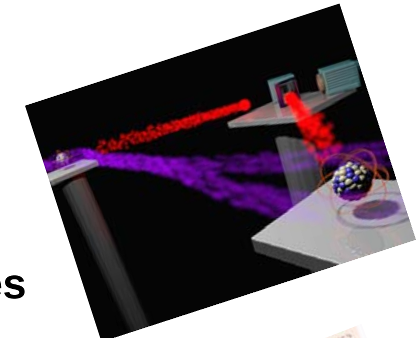
Classical/Quantum Interface

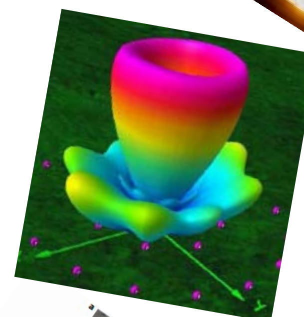
Location Verification

Conclusions

Quantum Communications is an exciting new area for engineers – it is here to stay. It will deliver the ultimate cyber-security solutions to next-generation networks.

There are many real-world problems looking for real-world engineering solutions. Specific engineering challenges highlighted here include -



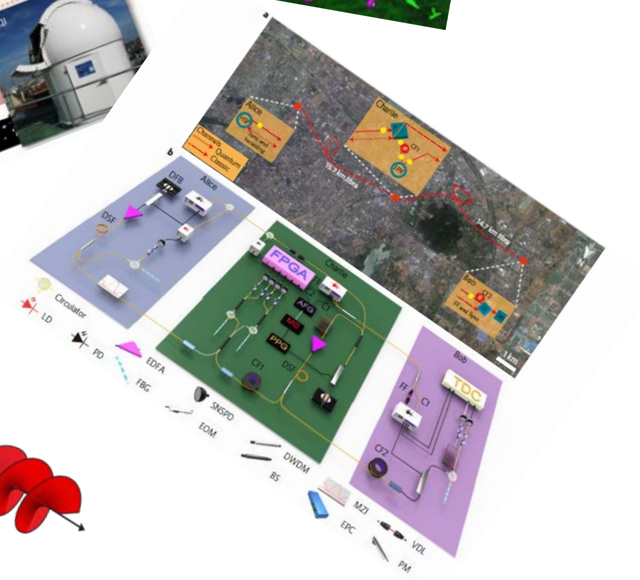


Large-scale City-wide Networks

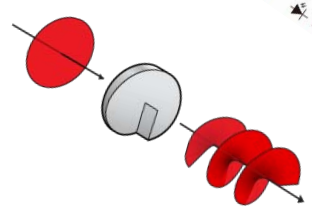
Space-based Communications

The Global Quantum Internet

New Multiplexing Schemes (OAM)



Next-Generation (6G) Wireless Communications



Quantum Computer Communications

References

Adesso, Entanglement of Gaussian States, PhD Thesis, (2007).

Bai, et al, IET Electronics Letters, Vol. 50, 20, 1414, (2014).

Bennett and Brassard, Proceedings of IEEE Inter. Conf. on Computers, Systems and Signal Processing, Vol. 175, 8, (1984).

Bruss, et al, ACM Computing Surveys, No. 2, Article 6, (2007).

Barzanjeh et al, Physical Review Letters, 114, 080503 (2015).

Capps, EET.com, http://m.eet.com/media/1140931/19213-150828.pdf (2001).

Chrapkiewicz et al, Nature Photonics 10, 576 (2016).

Edfors & Johansson, IEEE Trans. on Antennas and Propagation, Vol. 60, No. 2, 1126 (2012).

Epping et al, New J. Phys. 18, 053036 (2016).

Gregg et al, Optics Express, Vol. 24, 17, 18938 (2016).

Hosseinidehaj* & Malaney, arXiv:1605.05445 (2016a).

Hosseinidehaj & Malaney, Globecom, Washington DC (2016b).

Krenn et al, New J. Phys. 16, 113028 (2014).

Krenn et al, PNAS, doi: 10.1073/pnas.1612023113 (2016).

Leonhard et al, Physical Review. A. 91,0123345 (2015).

Lo et al, Nature Photonics, 8, 595 (2014).

Malaney, DOI: 10.1109/LWC.2016.2607740 (2016a).

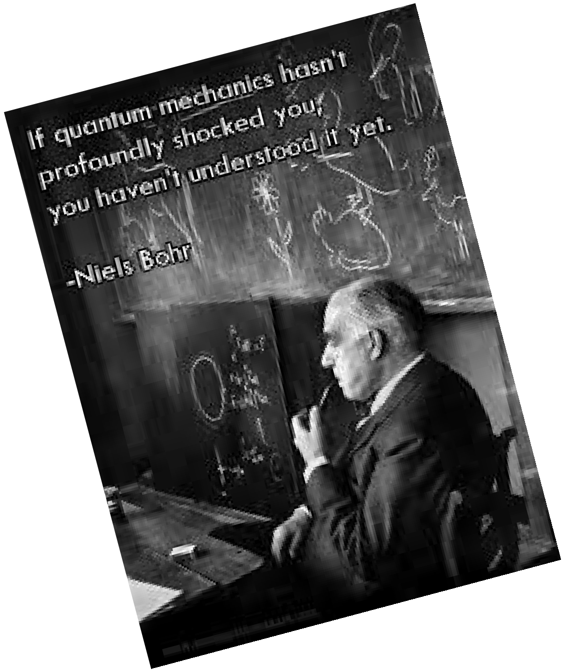
Malaney, Globecom, Washington DC (2016b).

van Meter & Touch, IEEE Communications Magazine, August (2013).

Smith & Yard, Science Vol. 321, Issue 5897, 1812 (2008).

Shadbolt et al, Nature, 409, 46 (2001).

Shor, Phys. Rev. A., 52, R2493 (1995).



References (Cont.)

Sun at al, Nature Photonics 10, 671–675 (2016).

Thide et al, Physical Review Letters.,99, 087701 (2007).

Ursin et al, Nature Physics 3, 481 (2007).

Valivarthi et al., Nature Photonics 10, 676–680 (2016).

Vallone et al, Physical Review Letters 115, 040502 (2015).

Wootters & Zurek , Nature, 299, 802 (1982).

Yin et al, Optics Express 21 (17), 20032 (2013).

Zeilinger, www.univie.ac.at/qfp/publications3/pdffiles/2006-10.pdf (2006).

Zeilinger, Scientific American, Vol. 282, No. 4, 50 (2000).

"The word 'classical' in physics means only one thing: it's wrong!" - J.R. Oppenheimer

General Reading (from which I have borrowed in some slides)

A useful beginners guide to Quantum Information is

"Protecting Information: From Classical Error Correction to Quantum Cryptography", Susan Loepp, and William Wootters, Cambridge University Press (2006).

The classic reference text of the field is

"Quantum Computation and Quantum Information", Michael A. Nielsen and Isaac L. Chuang, Cambridge University Press (2000).

A good introduction to CV states and quantum optics is

"Introductory Quantum Optics", Christopher Gerry and Peter Knight, Cambridge University Press (2005).

**My thanks to N. Hosseinidehaj for assisting with some of these slides.*