Quantum Cryptography

Bertrand Bonnefoy-Claudet   Zachary Estrada

Crypto against modern computers

- No known attack against RSA, AES, ... yet
- They are not proven (and they cannot be)

Crypto against modern computers

- No known attack against RSA, AES, … yet
- They are not proven (and they cannot be)

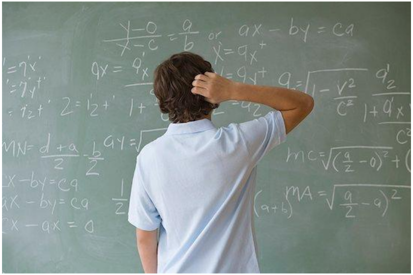
Crypto against modern computers

- No known attack against RSA, AES, ... yet
- They are not proven (and they cannot be)

Crypto against modern computers

- No known attack against RSA, AES, . . . yet
- They are not proven (and they cannot be)

Modern crypto relies on computational difficulty



Crypto against quantum computers

- AES 256 as strong as AES 128 w/conventional
- RSA&Co solved in polynomial time (Shor's algorithm)
- Good candidates to replace RSA but same principle (computational)

Crypto against quantum computers

- AES 256 as strong as AES 128 w/conventional
- RSA&Co solved in polynomial time (Shor's algorithm)
- Good candidates to replace RSA but same principle (computational)

Crypto against quantum computers

- AES 256 as strong as AES 128 w/conventional
- RSA&Co solved in polynomial time (Shor's algorithm)
- Good candidates to replace RSA but same principle (computational)

Crypto against quantum computers

- AES 256 as strong as AES 128 w/conventional
- RSA&Co solved in polynomial time (Shor's algorithm)
- Good candidates to replace RSA but same principle (computational)

Crypto against quantum computers

- AES 256 as strong as AES 128 w/conventional
- RSA&Co solved in polynomial time (Shor's algorithm)
- Good candidates to replace RSA but same principle (computational)

What is secure?

Proven security

Secure cipher

Cyphertext gives zero knowledge about message or key

Required properties of a key:

- as long as message
- random
- used only once

Proven security

Secure cipher

Cyphertext gives zero knowledge about message or key

Required properties of a key:

- as long as message
- random
- used only once

Proven security

Secure cipher

Cyphertext gives zero knowledge about message or key

Required properties of a key:

- as long as message
- random
- used only once

Vernam cipher (or one time pad)

One time pad

Modulo-2 addition (or XOR):

```
Message:    0000110011110010
Key:        0110101010101101
Ciphertext: 0110011001011111
```

One time pad

Modulo-2 addition (or XOR):

```
Message:    0000110011110010
Key:        0110101010101101
Ciphertext: 0110011001011111
```

- OTP is for encryption, authentication equivalent: universal hashing
- So, we must generate and exchange a key securely

One time pad

Modulo-2 addition (or XOR):

```
Message:    0000110011110010
Key:        0110101010101101
Ciphertext: 0110011001011111
```

- OTP is for encryption, authentication equivalent: universal hashing
- So, we must generate and exchange a key securely

One time pad

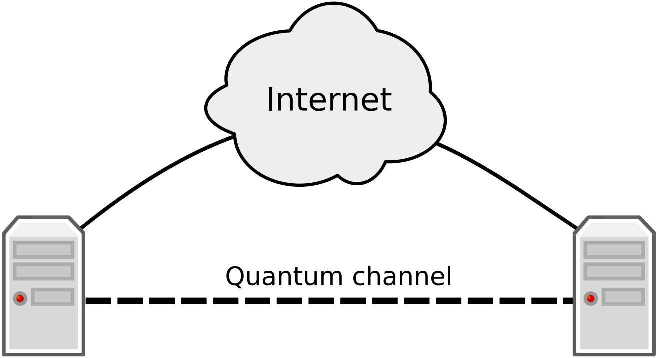
Modulo-2 addition (or XOR):

```
Message:    0000110011110010
Key:        0110101010101101
Ciphertext: 0110011001011111
```

- OTP is for encryption, authentication equivalent: universal hashing
- So, we must generate and exchange a key securely

Let's rely on nature

Quantum channel



Key exchange

- Qubits cannot be measured without being modified
- Key exchange protocol over quantum channel
- Why not send message directly?

Key exchange

- Qubits cannot be measured without being modified
- Key exchange protocol over quantum channel
- Why not send message directly?

Key exchange

- Qubits cannot be measured without being modified
- Key exchange protocol over quantum channel
- Why not send message directly?

Key exchange

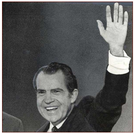
- Qubits cannot be measured without being modified
- Key exchange protocol over quantum channel
- Why not send message directly?

Some Background Physics

Some Background Physics



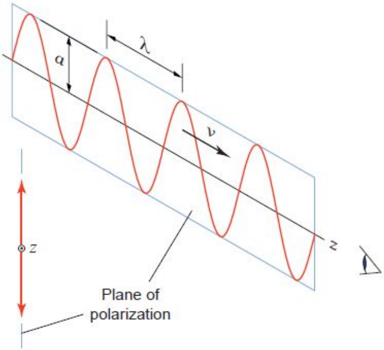




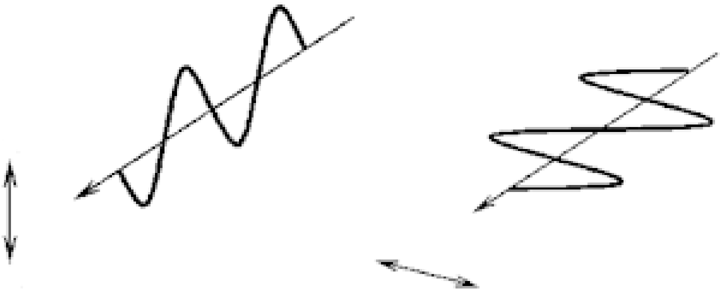

Classical Waves

Polarization

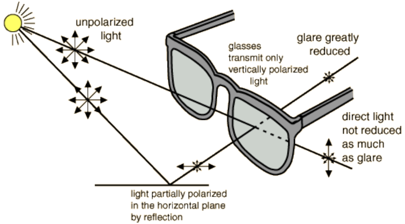
Simplified wave: $\vec{E}$ field 'pointing' in an alternating directions like a moving sine function.



Yes, this started out as a lowres gif



Exploiting polarization can useful:



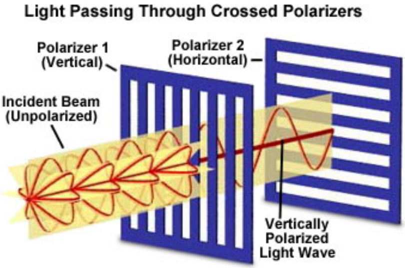
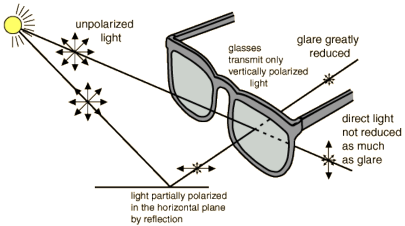


Figure 1

We will see that you can also to encode information in polarization states

Polarization (cont.)

Exploiting polarization can useful:



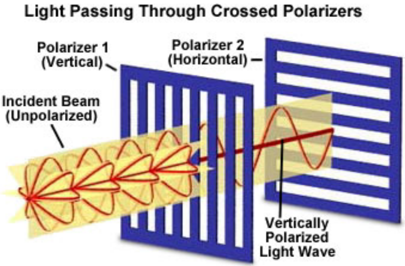
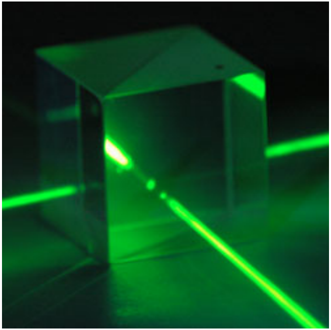


Figure 1

We will see that you can also to encode information in polarization states

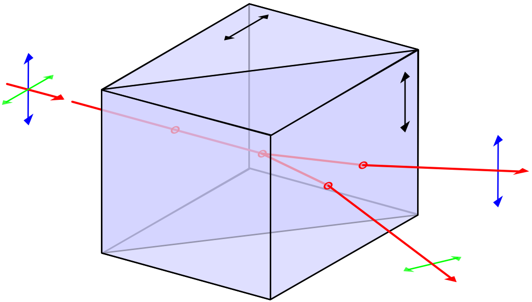
Beamsplitters

Earlier in lecture we've talked about 'half-silvered mirrors' or beamsplitters



Beamsplitters (cont.)

By using the right combination of materials, a beamsplitter can split on polarization state:



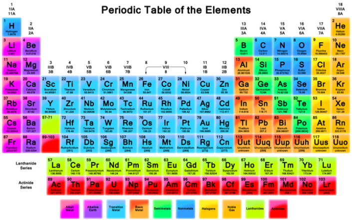
We call this a Polarizing BeamSplitter (PBS)

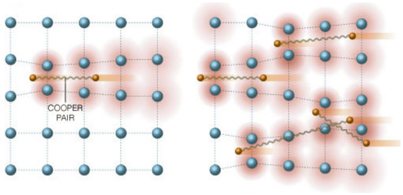
Quantum Mechanics

> I think I can safely say that nobody understands quantum mechanics.
> –Richard Feynman

Quantum Mechanics

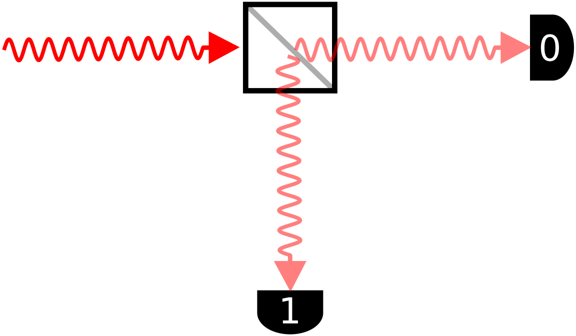
Quantum Mechanics has been used to explain many things





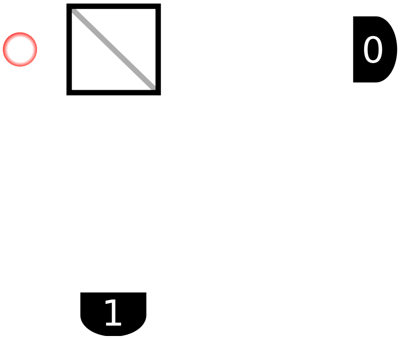
QM example - photon counting

- Consider a monochromatic light source, a beam splitter, and two detectors



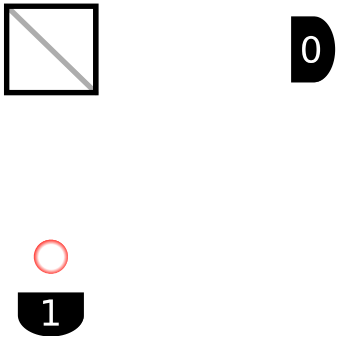
QM example - photon counting

- So we saw two waves with half-intensity. What happens for a single photon?



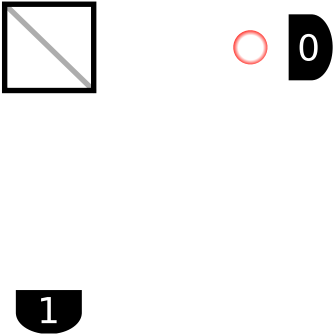
QM example - photon counting

- So we saw two waves with half-intensity. What happens for a single photon?



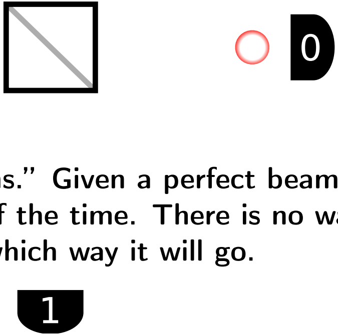
QM example - photon counting

- So we saw two waves with half-intensity. What happens for a single photon?



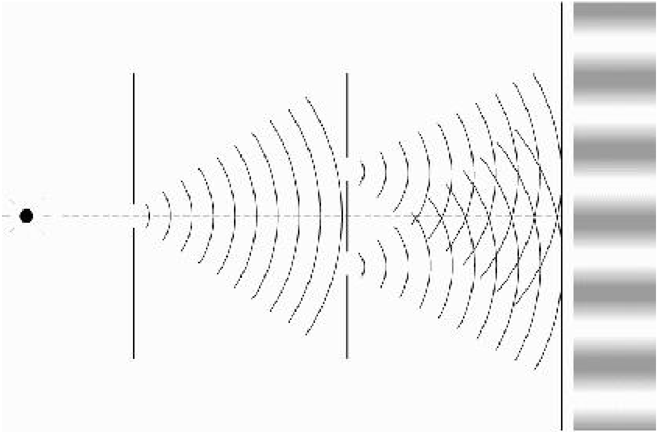
QM example - photon counting

- So we saw two waves with half-intensity. What happens for a single photon?



There are no "half-photons." Given a perfect beamsplitter, each detector clicks half of the time. There is no way for us to predict which way it will go.

QM example - double slit



http://www.toutestquantique.fr/#dualite

Superposition

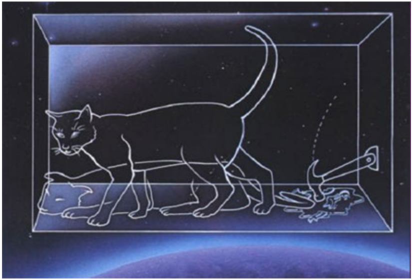
Quantum Superposition

It is perfectly valid for a quantum particle (e.g photon) to 'exist' in more than one state at a time (until it is measured)

Superposition

Quantum Superposition

It is perfectly valid for a quantum particle (e.g photon) to 'exist' in more than one state at a time (until it is measured)



Uncertainty

Probability and Uncertainty in Nature

At the quantum scale, it is *impossible* to predict the *exact* outcome of certain events. Furthermore, certain quantities are *fundamentally unknowable*.

Uncertainty

Probability and Uncertainty in Nature

At the quantum scale, it is *impossible* to predict the *exact* outcome of certain events. Furthermore, certain quantities are *fundamentally unknowable*.

Entanglement - an example

Pauli Exclusion Principle

Two electrons cannot occupy the exact same state

- Consider two electrons in a helium atom, in the lowest energy state ($1s^2$, if you remember chemistry) with spin 0.
- This means that one e^- is $\uparrow$ and the other is $\downarrow$
- If we look at one e^-'s spin, we immediately know the other's

Entanglement - an example

Pauli Exclusion Principle

Two electrons cannot occupy the exact same state

- Consider two electrons in a helium atom, in the lowest energy state ($1s^2$, if you remember chemistry) with spin 0.
- This means that one e^- is $\uparrow$ and the other is $\downarrow$
- If we look at one e^-'s spin, we immediately know the other's

Entanglement - an example

Pauli Exclusion Principle

Two electrons cannot occupy the exact same state

- Consider two electrons in a helium atom, in the lowest energy state ($1s^2$, if you remember chemistry) with spin 0.
- This means that one e^- is $\uparrow$ and the other is $\downarrow$
- If we look at one e^-'s spin, we immediately know the other's

Entanglement - an example

Pauli Exclusion Principle

Two electrons cannot occupy the exact same state

- Consider two electrons in a helium atom, in the lowest energy state ($1s^2$, if you remember chemistry) with spin 0.
- This means that one e^- is $\uparrow$ and the other is $\downarrow$
- If we look at one e^-'s spin, we immediately know the other's

Entanglement - an example (cont.)

- We can make it such that the e^-s are in a superposition of spin states, each is equally likely to be $\uparrow$ or $\downarrow$
- Our rules say that if we measure the spin of one e^-, we 'force' it to take a definite spin value
- The other e^- must be in the opposite spin state
- Measuring one e^- caused the other's spin to be 'defined' - we call these particles 'spin-entangled electrons.'
- Note for completeness: This is NOT the only valid spin state for two electrons in He, but a special state called the "spin singlet."

Entanglement - an example (cont.)

- We can make it such that the e^-s are in a superposition of spin states, each is equally likely to be $\uparrow$ or $\downarrow$
- Our rules say that if we measure the spin of one e^-, we 'force' it to take a definite spin value
- The other e^- must be in the opposite spin state
- Measuring one e^- caused the other's spin to be 'defined' - we call these particles 'spin-entangled electrons.'
- Note for completeness: This is NOT the only valid spin state for two electrons in He, but a special state called the "spin singlet."

Entanglement - an example (cont.)

- We can make it such that the e^-s are in a superposition of spin states, each is equally likely to be $\uparrow$ or $\downarrow$
- Our rules say that if we measure the spin of one e^-, we 'force' it to take a definite spin value
- The other e^- must be in the opposite spin state
- Measuring one e^- caused the other's spin to be 'defined' - we call these particles 'spin-entangled electrons.'
- Note for completeness: This is NOT the only valid spin state for two electrons in He, but a special state called the "spin singlet."

Entanglement - an example (cont.)

- We can make it such that the e^-s are in a superposition of spin states, each is equally likely to be $\uparrow$ or $\downarrow$
- Our rules say that if we measure the spin of one e^-, we 'force' it to take a definite spin value
- The other e^- must be in the opposite spin state
- Measuring one e^- caused the other's spin to be 'defined' - we call these particles 'spin-entangled electrons.'
- Note for completeness: This is NOT the only valid spin state for two electrons in He, but a special state called the "spin singlet."

Entanglement - an example (cont.)

- We can make it such that the e^-s are in a superposition of spin states, each is equally likely to be $\uparrow$ or $\downarrow$
- Our rules say that if we measure the spin of one e^-, we 'force' it to take a definite spin value
- The other e^- must be in the opposite spin state
- Measuring one e^- caused the other's spin to be 'defined' - we call these particles 'spin-entangled electrons.'
- Note for completeness: This is NOT the only valid spin state for two electrons in He, but a special state called the "spin singlet."

Entanglement - an example (cont.) (cont.)

- If we somehow rip an electron out of the atom w/o 'measuring' its spin, they will still be correlated
- As long as this state is preserved, there's no dependence on distance
- This is called *non-locality*
- Einstein called it "spooky action at a distance"

Entanglement - an example (cont.) (cont.)

- If we somehow rip an electron out of the atom w/o 'measuring' its spin, they will still be correlated
- As long as this state is preserved, there's no dependence on distance
- This is called *non-locality*
- Einstein called it "spooky action at a distance"

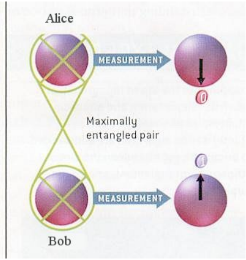
Entanglement - an example (cont.) (cont.)

- If we somehow rip an electron out of the atom w/o 'measuring' its spin, they will still be correlated
- As long as this state is preserved, there's no dependence on distance
- This is called *non-locality*
- Einstein called it "spooky action at a distance"

Entanglement - an example (cont.) (cont.)

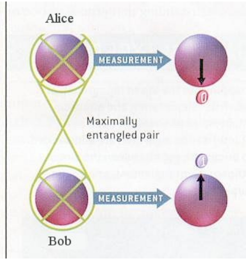
- If we somehow rip an electron out of the atom w/o 'measuring' its spin, they will still be correlated
- As long as this state is preserved, there's no dependence on distance
- This is called *non-locality*
- Einstein called it "spooky action at a distance"

Entanglement - an example (cont.) (cont.) (cont.)



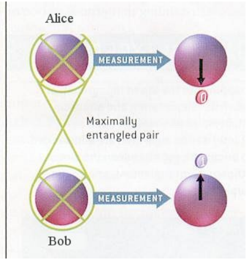
- Notice that we didn't force a *particular* spin value - we can't
- So no 'faster-than-light' information transfer is present
- Entanglement is perfectly random, but perfectly correlated!
- Bell Tests have a good experimental track record

Entanglement - an example (cont.) (cont.) (cont.)



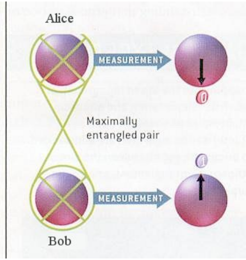
- Notice that we didn't force a *particular* spin value - we can't
- So no 'faster-than-light' information transfer is present
- Entanglement is perfectly random, but perfectly correlated!
- Bell Tests have a good experimental track record

Entanglement - an example (cont.) (cont.) (cont.)



- Notice that we didn't force a *particular* spin value - we can't
- So no 'faster-than-light' information transfer is present
- Entanglement is perfectly random, but perfectly correlated!
- Bell Tests have a good experimental track record

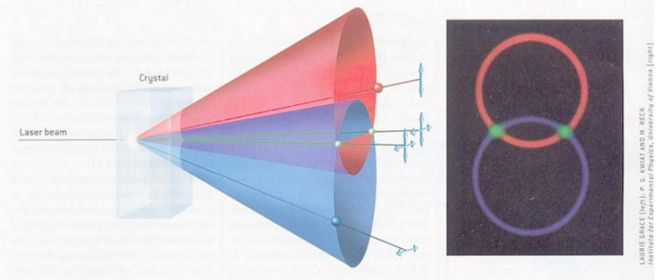
Entanglement - an example (cont.) (cont.) (cont.)



- Notice that we didn't force a *particular* spin value - we can't
- So no 'faster-than-light' information transfer is present
- Entanglement is perfectly random, but perfectly correlated!
- Bell Tests have a good experimental track record

Making entangled photons

BBO: Spontaneous parametric down-conversion converts one photon into two photons



ENTANGLED PHOTON PAIRS are created when a laser beam passes through a crystal such as beta barium borate. The crystal occasionally converts a single ultraviolet photon into two photons of lower energy, one polarized vertically (*on red cone*), one polarized horizontally (*on blue cone*). If the photons happen to travel along the cone intersections (*green*), neither photon has a definite polarization, but their relative polarizations are complementary; they are then entangled. Colorized image (*at right*) is a photograph of down-converted light. Colors do not represent the color of the light.

Making entangled photons - for real real

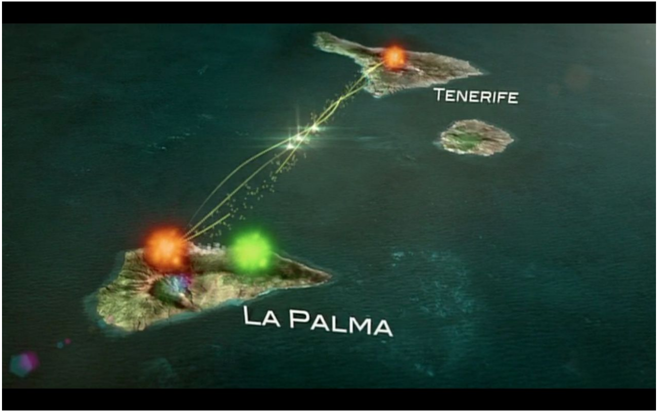
Experimentally, this "spooky action" does occur at a distance.

In 1982, researchers demonstrated entanglement between photons 13m apart

Making entangled photons - for real real

Experimentally, this “spooky action” does occur at a distance.
In 1982, researchers demonstrated entanglement between photons 13m apart

In 2012, **144km**



QM - wrapup

From Gisin *et al.*, Quantum Cryptography (2002):

- One cannot take a measurement without perturbing the system.
- One cannot determine simultaneously the position and the momentum of a particle with arbitrarily high accuracy.
- One cannot simultaneously measure the polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis.
- One cannot draw pictures of individual quantum processes. (You can only measure observables)
- One cannot duplicate an unknown quantum state.

QM - wrapup

From Gisin *et al.*, Quantum Cryptography (2002):

- One cannot take a measurement without perturbing the system.
- One cannot determine simultaneously the position and the momentum of a particle with arbitrarily high accuracy.
- One cannot simultaneously measure the polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis.
- One cannot draw pictures of individual quantum processes. (You can only measure observables)
- One cannot duplicate an unknown quantum state.

QM - wrapup

From Gisin *et al.*, Quantum Cryptography (2002):

- One cannot take a measurement without perturbing the system.
- One cannot determine simultaneously the position and the momentum of a particle with arbitrarily high accuracy.
- One cannot simultaneously measure the polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis.
- One cannot draw pictures of individual quantum processes. (You can only measure observables)
- One cannot duplicate an unknown quantum state.

QM - wrapup

From Gisin *et al.*, Quantum Cryptography (2002):

- One cannot take a measurement without perturbing the system.
- One cannot determine simultaneously the position and the momentum of a particle with arbitrarily high accuracy.
- One cannot simultaneously measure the polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis.
- One cannot draw pictures of individual quantum processes. (You can only measure observables)
- One cannot duplicate an unknown quantum state.

QM - wrapup

From Gisin *et al.*, Quantum Cryptography (2002):

- One cannot take a measurement without perturbing the system.
- One cannot determine simultaneously the position and the momentum of a particle with arbitrarily high accuracy.
- One cannot simultaneously measure the polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis.
- One cannot draw pictures of individual quantum processes. (You can only measure observables)
- One cannot duplicate an unknown quantum state.

Quantum Cryptography
(or Quantum Key Distribution)

Goal

Exchange a key

Example: BB84

Let's start with an example: BB84

- Published in 1984 by Charles Bennett and Gilles Brassard
- Originally used polarization

Example: BB84

Let's start with an example: BB84

- Published in 1984 by Charles Bennett and Gilles Brassard
- Originally used polarization

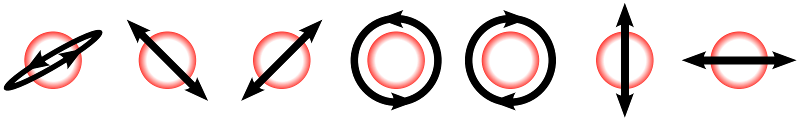
Example: BB84

Let's start with an example: BB84

- Published in 1984 by Charles Bennett and Gilles Brassard
- Originally used polarization

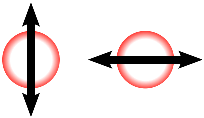
Polarization

Many kinds of polarization:



Bases

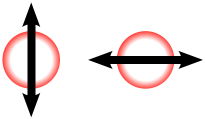
- A basis:



- Components are linearly independent
- From this basis and **superposition**, you can get all other states

Bases

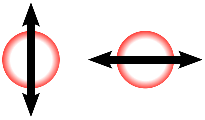
- A basis:



- Components are linearly independent
- From this basis and **superposition**, you can get all other states

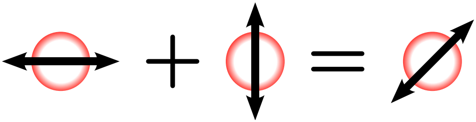
Bases

- A basis:

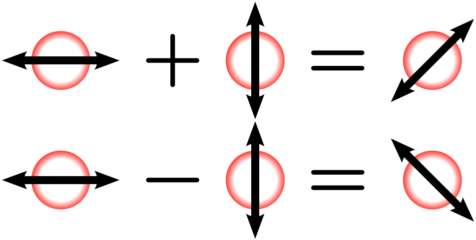


- Components are linearly independent
- From this basis and **superposition**, you can get all other states

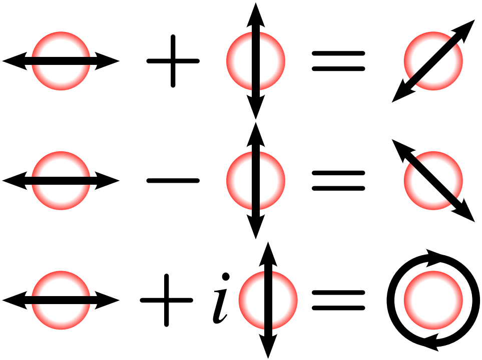
Superposition



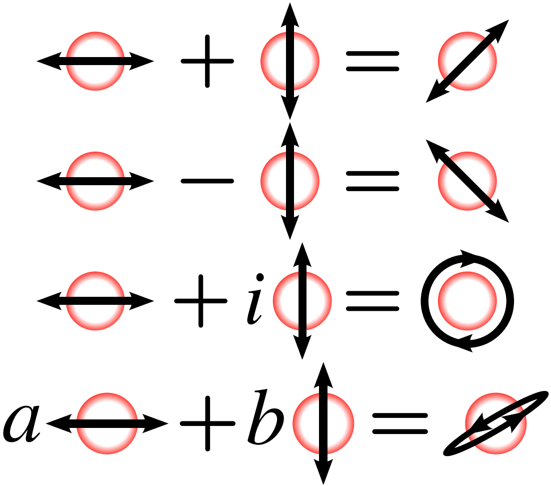
Superposition



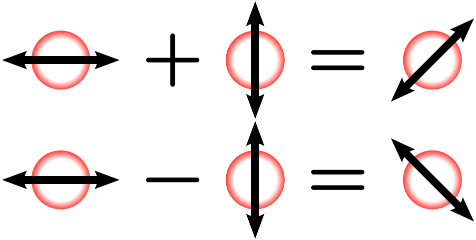
Superposition



Superposition



Superposition



We'll focus on these.

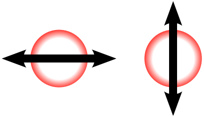
Two bases

- Horizontal – Vertical

- Diagonal – Antidiagonal

Two bases

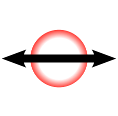
- Horizontal – Vertical



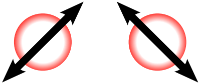
- Diagonal – Antidiagonal

Two bases

- Horizontal – Vertical

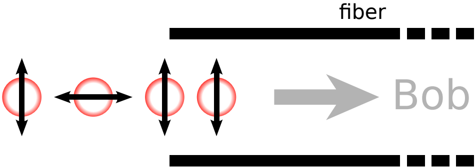


- Diagonal – Antidiagonal



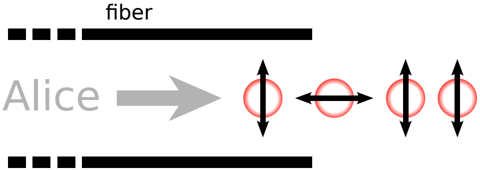
Sending bits

Alice sends 1101:

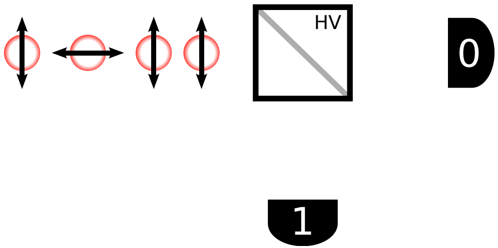


Receiving bits

Bob receives. . .

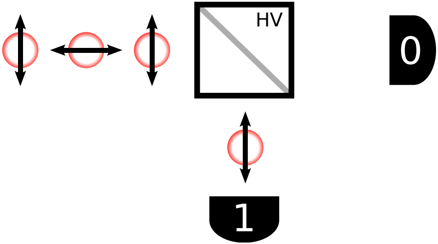


Receiving bits



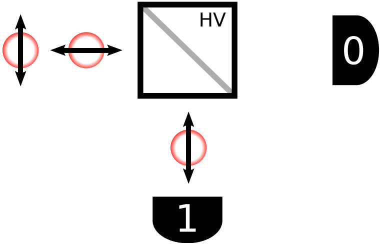
Bob gets:

Receiving bits



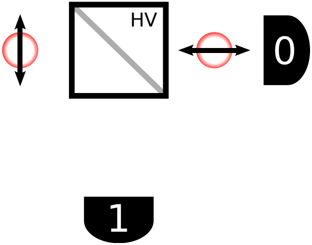
Bob gets: 1

Receiving bits



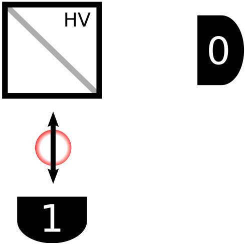
Bob gets: 11

Receiving bits



Bob gets: 110

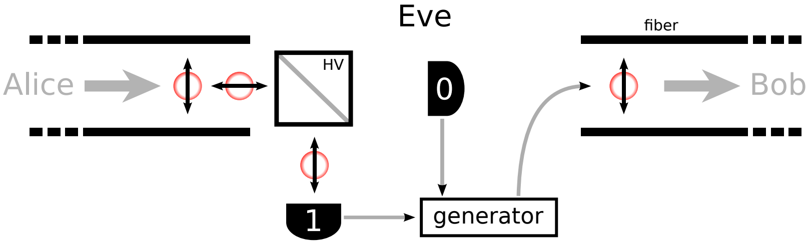
Receiving bits



Bob gets: 1101

Eavesdropping

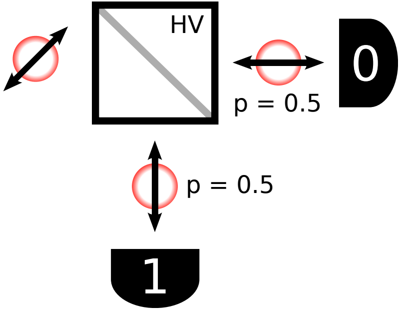
Basis is known, so Eve can measure and regenerate:



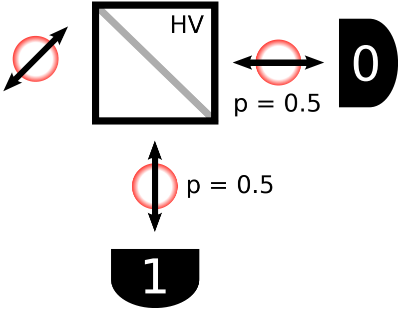
Choose bases randomly

Message	1	1	0	1
Basis	HV	DA	DA	HV
Polarization				

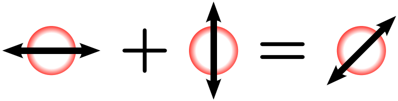
Measurement with wrong basis



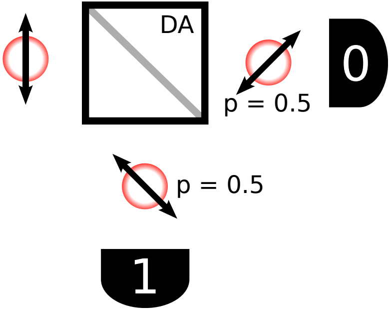
Measurement with wrong basis



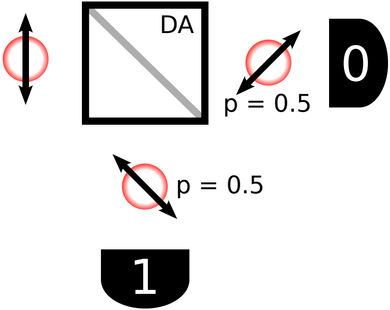
It comes from superposition:



Measurement with wrong basis



Measurement with wrong basis



Superposition, too:

Measurement with wrong basis

Using the wrong basis implies:

- measurement unreliability
- quantum state perturbation

Measurement with wrong basis

Using the wrong basis implies:

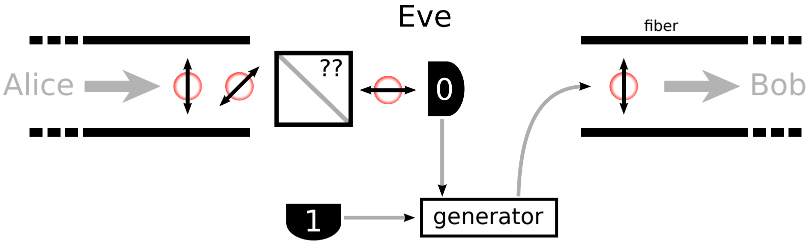
- measurement unreliability
- quantum state perturbation

Measurement with wrong basis

Using the wrong basis implies:

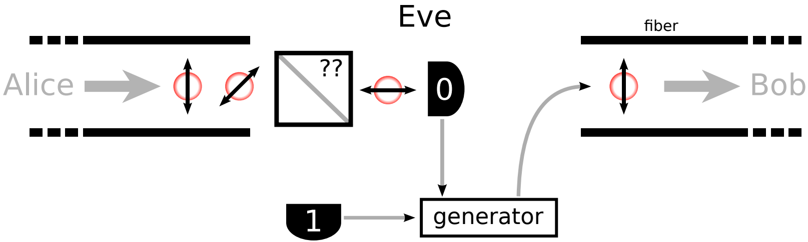
- measurement unreliability
- quantum state perturbation

Eavesdropping: fail



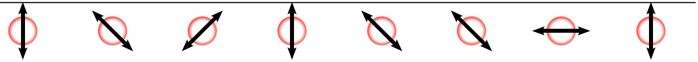
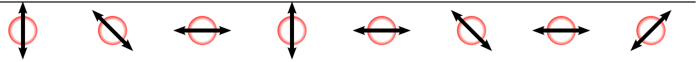
- Not obvious, what about Bob?

Eavesdropping: fail

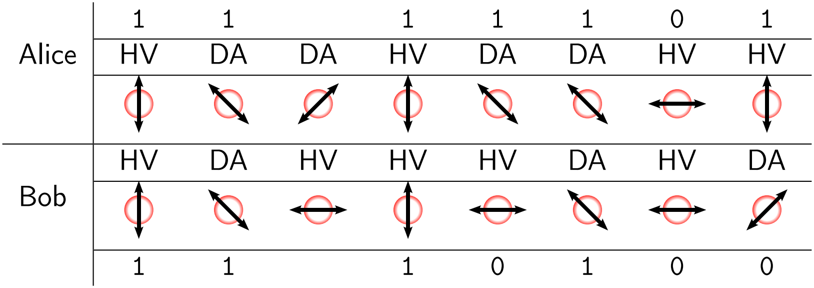


- Not obvious, what about Bob?

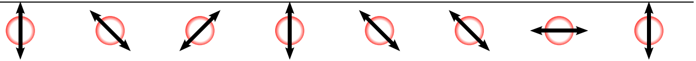
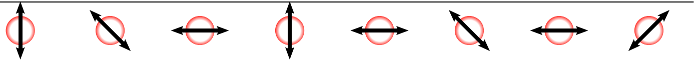
Agreement

Alice	1	1	0	1	1	1	0	1
	HV	DA	DA	HV	DA	DA	HV	HV
								
Bob	HV	DA	HV	HV	HV	DA	HV	DA
								
	1	1	0	1	0	1	0	0

Agreement


Alice
1 1 1 1 1 0 1
HV DA DA HV DA DA HV HV
Bob
HV DA HV HV HV DA HV DA
1 1 1 0 1 0 0

Agreement

	1	1		1		1	0	1
Alice	HV	DA	DA	HV	DA	DA	HV	HV
								
Bob	HV	DA	HV	HV	HV	DA	HV	DA
								
	1	1		1		1	0	0

Agreement

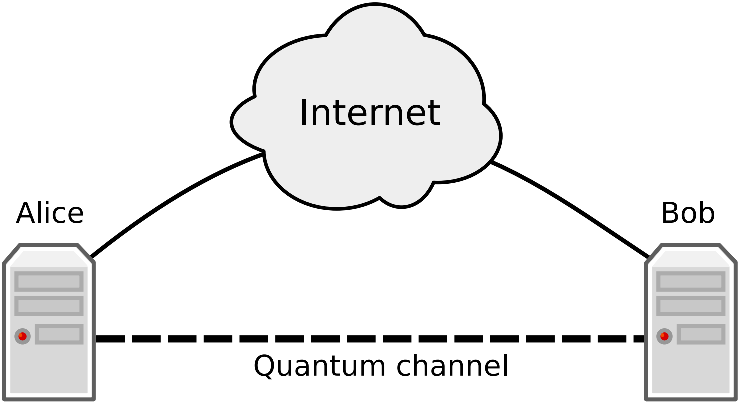
Alice	1	1		1		1	0	
	HV	DA	DA	HV	DA	DA	HV	HV
	↕	⤡	⤢	↕	⤡	⤡	↔	↕
Bob	HV	DA	HV	HV	HV	DA	HV	DA
	↕	⤡	↔	↕	↔	⤡	↔	⤢
	1	1		1		1	0	

Agreement

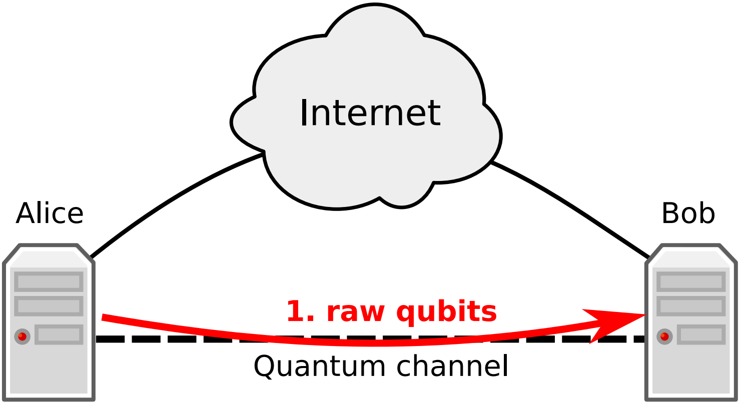
Alice	1	1		1		1	0	
	HV	DA	DA	HV	DA	DA	HV	HV
	↕	⤡	⤢	↕	⤡	⤡	↔	↕
Bob	HV	DA	HV	HV	HV	DA	HV	DA
	↕	⤡	↔	↕	↔	⤡	↔	⤢
	1	1		1		1	0	

They end up with the same bits, called a sifted key

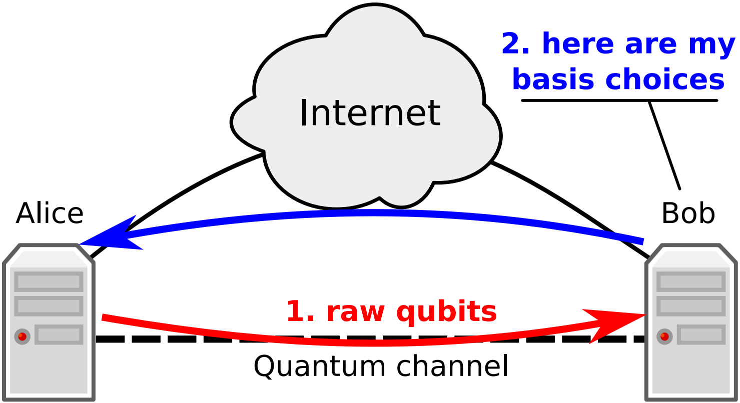
Agreement



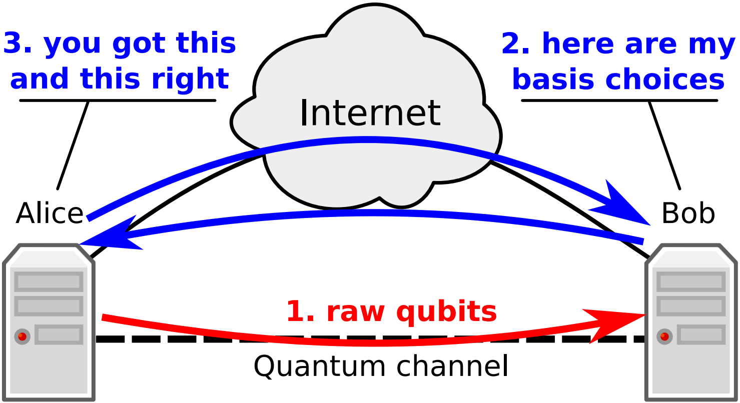
Agreement



Agreement


Internet
2. here are my basis choices
Alice
Bob
1. raw qubits
Quantum channel

Agreement


3. you got this and this right
Internet
2. here are my basis choices
Alice
Bob
1. raw qubits
Quantum channel

Secure?

- Messages must be authenticated
- Alice and Bob loose 50% of the raw bits on average
- Eve can get some information from bits and messages
- How much?
    - 75% of correct bits (but she wouldn't necessarily know which ones)
    - More info with messages
- Can she be detected?

Secure?

- Messages must be authenticated
- Alice and Bob loose 50% of the raw bits on average
- Eve can get some information from bits and messages
- How much?
  - 75% of correct bits (but she wouldn't necessarily know which ones)
  - More info with messages
- Can she be detected?

Secure?

- Messages must be authenticated
- Alice and Bob loose 50% of the raw bits on average
- Eve can get some information from bits and messages
- How much?
  - 75% of correct bits (but she wouldn't necessarily know which ones)
  - More info with messages
- Can she be detected?

Secure?

- Messages must be authenticated
- Alice and Bob loose 50% of the raw bits on average
- Eve can get some information from bits and messages
- How much?
    - 75% of correct bits (but she wouldn't necessarily know which ones)
    - More info with messages
- Can she be detected?

Secure?

- Messages must be authenticated
- Alice and Bob loose 50% of the raw bits on average
- Eve can get some information from bits and messages
- How much?
    - 75% of correct bits (but she wouldn't necessarily know which ones)
    - More info with messages
- Can she be detected?

Secure?

- Messages must be authenticated
- Alice and Bob loose 50% of the raw bits on average
- Eve can get some information from bits and messages
- How much?
  - 75% of correct bits (but she wouldn't necessarily know which ones)
  - More info with messages
- Can she be detected?

Secure?

- Messages must be authenticated
- Alice and Bob loose 50% of the raw bits on average
- Eve can get some information from bits and messages
- How much?
  - 75% of correct bits (but she wouldn't necessarily know which ones)
  - More info with messages
- Can she be detected?

Secure?

- Messages must be authenticated
- Alice and Bob loose 50% of the raw bits on average
- Eve can get some information from bits and messages
- How much?
  - 75% of correct bits (but she wouldn't necessarily know which ones)
  - More info with messages
- Can she be detected?

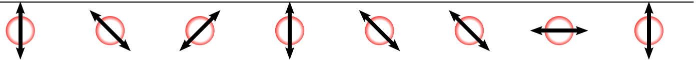
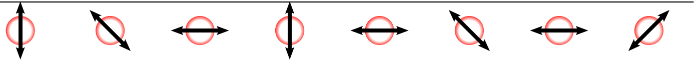
Agreement and sacrifice

	1	1	0	1	1	1	0	1
Alice	HV	DA	DA	HV	DA	DA	HV	HV
	↕	⤡	⤢	↕	⤡	⤡	↔	↕
	HV	DA	HV	HV	HV	DA	HV	DA
Bob	↕	⤡	↔	↕	↔	⤡	↔	⤢
	1	1	0	1	0	1	0	0

Agreement and sacrifice

Alice	1	1		1	1	1	0	1
	HV	DA	DA	HV	DA	DA	HV	HV
	↕	⤡	⤢	↕	⤡	⤡	↔	↕
Bob	HV	DA	HV	HV	HV	DA	HV	DA
	↕	⤡	↔	↕	↔	⤡	↔	⤢
	1	1		1	0	1	0	0

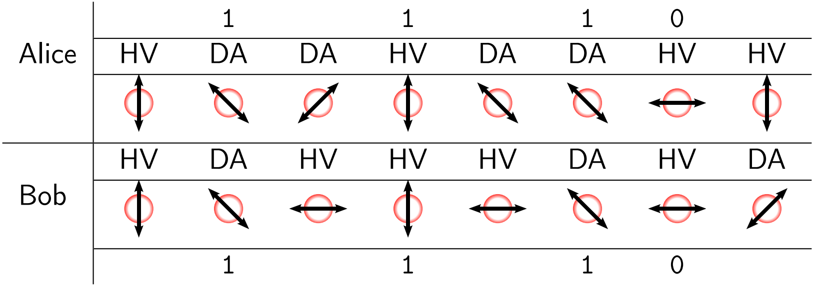
Agreement and sacrifice

Alice	1	1		1		1	0	1
	HV	DA	DA	HV	DA	DA	HV	HV
								
Bob	HV	DA	HV	HV	HV	DA	HV	DA
								
	1	1		1		1	0	0

Agreement and sacrifice

Alice	1	1		1		1	0	
	HV	DA	DA	HV	DA	DA	HV	HV
	↕	⤡	⤢	↕	⤡	⤡	↔	↕
Bob	HV	DA	HV	HV	HV	DA	HV	DA
	↕	⤡	↔	↕	↔	⤡	↔	⤢
	1	1		1		1	0	

Agreement and sacrifice



Agreement and sacrifice

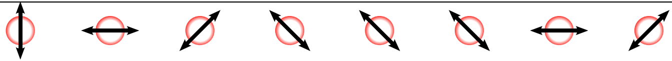
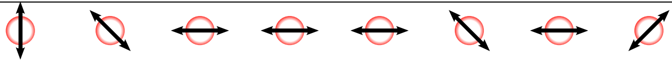
		1				1	0	
Alice	HV	DA	DA	HV	DA	DA	HV	HV
	↕	⤡	⤢	↕	⤡	⤡	↔	↕
Bob	HV	DA	HV	HV	HV	DA	HV	DA
	↕	⤡	↔	↕	↔	⤡	↔	⤢
		1				1	0	

Agreement and sacrifice

		1				1	0	
Alice	HV	DA	DA	HV	DA	DA	HV	HV
	↕	⤡	⤢	↕	⤡	⤡	↔	↕
Bob	HV	DA	HV	HV	HV	DA	HV	DA
	↕	⤡	↔	↕	↔	⤡	↔	⤢
		1				1	0	

Smaller sifted key

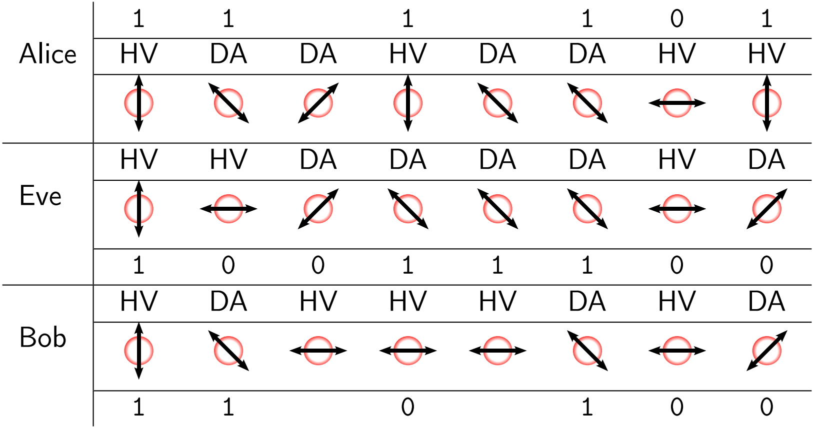
Eavesdropping defeated

Alice	1	1	0	1	1	1	0	1
	HV	DA	DA	HV	DA	DA	HV	HV
								
Eve	HV	HV	DA	DA	DA	DA	HV	DA
								
	1	0	0	1	1	1	0	0
Bob	HV	DA	HV	HV	HV	DA	HV	DA
								
	1	1	0	0	0	1	0	0

Eavesdropping defeated

Alice	1	1		1	1	1	0	1
	HV	DA	DA	HV	DA	DA	HV	HV
	↕	⤡	⤢	↕	⤡	⤡	↔	↕
Eve	HV	HV	DA	DA	DA	DA	HV	DA
	↕	↔	⤢	⤡	⤡	⤡	↔	⤢
	1	0	0	1	1	1	0	0
Bob	HV	DA	HV	HV	HV	DA	HV	DA
	↕	⤡	↔	↔	↔	⤡	↔	⤢
	1	1		0	0	1	0	0

Eavesdropping defeated



Eavesdropping defeated

Alice	1	1		1		1	0	
	HV	DA	DA	HV	DA	DA	HV	HV
	↕	⤡	⤢	↕	⤡	⤡	↔	↕
Eve	HV	HV	DA	DA	DA	DA	HV	DA
	↕	↔	⤢	⤡	⤡	⤡	↔	⤢
	1	0	0	1	1	1	0	0
Bob	HV	DA	HV	HV	HV	DA	HV	DA
	↕	⤡	↔	↔	↔	⤡	↔	⤢
	1	1		0		1	0	

Eavesdropping defeated

Alice		1		1		1	0	
	HV	DA	DA	HV	DA	DA	HV	HV
	↕	⤡	⤢	↕	⤡	⤡	↔	↕
Eve	HV	HV	DA	DA	DA	DA	HV	DA
	↕	↔	⤢	⤡	⤡	⤡	↔	⤢
	1	0	0	1	1	1	0	0
Bob	HV	DA	HV	HV	HV	DA	HV	DA
	↕	⤡	↔	↔	↔	⤡	↔	⤢
		1		0		1	0	

Eavesdropping defeated

Alice		1		1		1	0	
	HV	DA	DA	HV	DA	DA	HV	HV
	↕	⤡	⤢	↕	⤡	⤡	↔	↕
Eve	HV	HV	DA	DA	DA	DA	HV	DA
	↕	↔	⤢	⤡	⤡	⤡	↔	⤢
	1	0	0	1	1	1	0	0
Bob	HV	DA	HV	HV	HV	DA	HV	DA
	↕	⤡	↔	↔	↔	⤡	↔	⤢
		1		0		1	0	

Error detected

Errors

Where can they come from?

- Loss (fiber, filters, etc)
- Polarization perturbation
- Beamsplitter bias
- Detection error

Errors

Where can they come from?

- Loss (fiber, filters, etc)
- Polarization perturbation
- Beamsplitter bias
- Detection error

Errors

Where can they come from?

- Loss (fiber, filters, etc)
- Polarization perturbation
- Beamsplitter bias
- Detection error

Errors

Where can they come from?

- Loss (fiber, filters, etc)
- Polarization perturbation
- Beamsplitter bias
- Detection error

Errors

Where can they come from?

- Loss (fiber, filters, etc)
- Polarization perturbation
- Beamsplitter bias
- Detection error

Protocols overview

Different protocols but similar properties

- BB84: 4 quantum states and random basis choices
- B92: Similar but with 2 quantum states
- E91: Entangled states and Bell test

Protocols overview

Different protocols but similar properties

- BB84: 4 quantum states and random basis choices
- B92: Similar but with 2 quantum states
- E91: Entangled states and Bell test

Protocols overview

Different protocols but similar properties

- BB84: 4 quantum states and random basis choices
- B92: Similar but with 2 quantum states
- E91: Entangled states and Bell test

Protocols overview

Different protocols but similar properties

- BB84: 4 quantum states and random basis choices
- B92: Similar but with 2 quantum states
- E91: Entangled states and Bell test

E91: Artur Eckert's protocol

- Entangled pairs generator
- Bell test to detect eavesdropping

E91: Artur Eckert's protocol

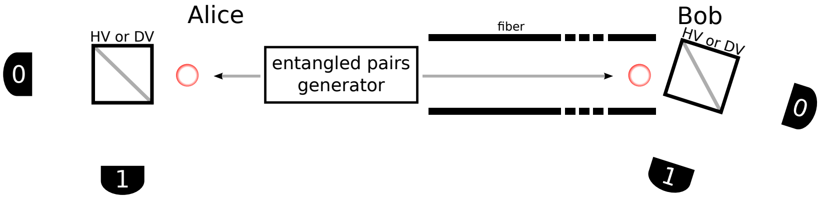
- Entangled pairs generator
- Bell test to detect eavesdropping

E91: Artur Eckert's protocol

- Entangled pairs generator
- Bell test to detect eavesdropping

E91: Artur Eckert's protocol

- Entangled pairs generator
- Bell test to detect eavesdropping



Common steps

- Raw key generation
- Sifting (50%)
- Error correction and detection (depends on error rate)
- Privacy amplification (depends on level of security)

Common steps

- Raw key generation
- Sifting (50%)
- Error correction and detection (depends on error rate)
- Privacy amplification (depends on level of security)

Common steps

- Raw key generation
- Sifting (50%)
- Error correction and detection (depends on error rate)
- Privacy amplification (depends on level of security)

Common steps

- Raw key generation
- Sifting (50%)
- Error correction and detection (depends on error rate)
- Privacy amplification (depends on level of security)

Common steps

- Raw key generation
- Sifting (50%)
- Error correction and detection (depends on error rate)
- Privacy amplification (depends on level of security)

Security

The previous scheme is vulnerable if active eavesdropping is assumed.

- Simple MITM attack (Eve can impersonate Bob)

Security

The previous scheme is vulnerable if active eavesdropping is assumed.

- Simple MITM attack (Eve can impersonate Bob)

Shared secret and key growing

- Perform several rounds
- Key should grow at each round

Round

- Initial key
- Qubits distribution
- Messages authenticated with **part of the initial key**
- Final key larger than initial key (hopefully!)

Shared secret and key growing

- Perform several rounds
- Key should grow at each round

Round

- Initial key
- Qubits distribution
- Messages authenticated with **part of the initial key**
- Final key larger than initial key (hopefully!)

Shared secret and key growing

- Perform several rounds
- Key should grow at each round

Round

- Initial key
- Qubits distribution
- Messages authenticated with **part of the initial key**
- Final key larger than initial key (hopefully!)

Shared secret and key growing

- Perform several rounds
- Key should grow at each round

Round

- Initial key
- Qubits distribution
- Messages authenticated with **part of the initial key**
- Final key larger than initial key (hopefully!)

Breaking QKD

QKD is theoretically proven to be secure, but is there a large gap between ideal theory and actual implementations? What about side channels?

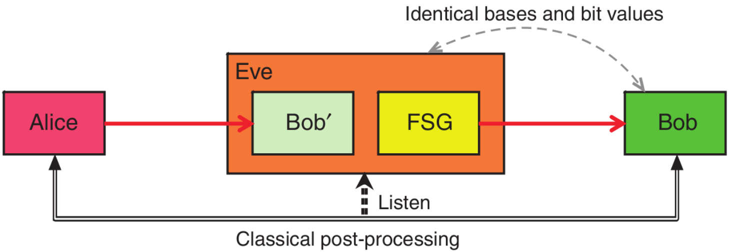
Fake states

The *no-cloning* theorem prevents us from making an exact copy of a quantum state. However, we can create classical states that have the same observable properties as quantum states.

Fake states

The *no-cloning* theorem prevents us from making an exact copy of a quantum state. However, we can create classical states that have the same observable properties as quantum states.

Fake State Generator

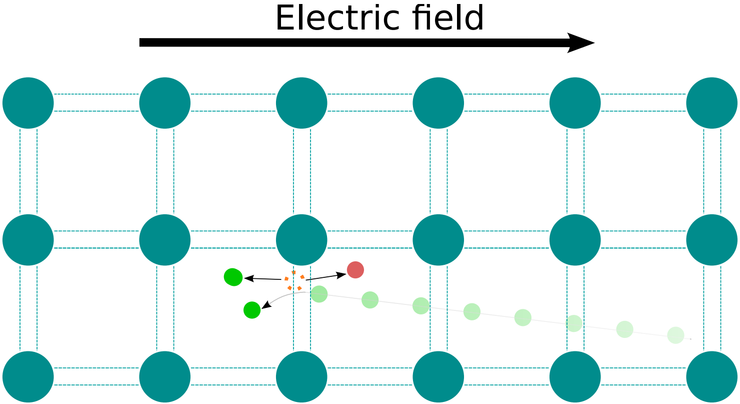


The attack

- Used an actual QKD system (E91 protocol) from previous experiments
- Inserted Eve into a $\sim$ 300 m setup
- Eve uses identical measuring equipment
- Eve also forces Bob's polarization basis choice
- Again, the Quantum parts are still valid and secure

A quick background on detectors

Impact ionization



A quick background on detectors (cont.)

- Impact ionization in an area with a high electric field can lead to an "avalanche current"
- An external circuit is used to then quench the avalanche current and then recharge the circuit
- Main idea: a single photon is enough to cause a macroscopic current because of the avalanche process

A quick background on detectors (cont.)

- Impact ionization in an area with a high electric field can lead to an "avalanche current"
- An external circuit is used to then quench the avalanche current and then recharge the circuit
- Main idea: a single photon is enough to cause a macroscopic current because of the avalanche process

A quick background on detectors (cont.)

- Impact ionization in an area with a high electric field can lead to an "avalanche current"
- An external circuit is used to then quench the avalanche current and then recharge the circuit
- Main idea: a single photon is enough to cause a macroscopic current because of the avalanche process

Faking states

If Eve measures the photons, could we use classical light instead of single photons to control the detector?

- We wouldn't have asked if the answer wasn't yes!
- There is a stray capacitance that needs to recharge for the next avalanche
- If enough photons keep hitting the diode so that the cap can't recharge, the avalanche current decreases (c.w.)
- Bob's detector is now blinded and the PD's current now responds classically - with a threshold power $\gg$ a single photon

Faking states

If Eve measures the photons, could we use classical light instead of single photons to control the detector?

- We wouldn't have asked if the answer wasn't yes!
- There is a stray capacitance that needs to recharge for the next avalanche
- If enough photons keep hitting the diode so that the cap can't recharge, the avalanche current decreases (c.w.)
- Bob's detector is now blinded and the PD's current now responds classically - with a threshold power $\gg$ a single photon

Faking states

If Eve measures the photons, could we use classical light instead of single photons to control the detector?

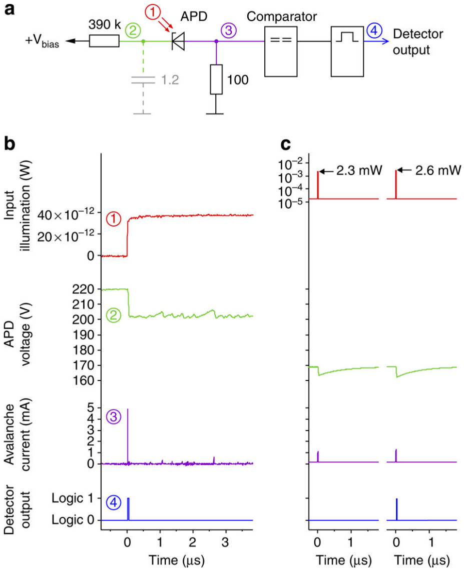
- We wouldn't have asked if the answer wasn't yes!
- There is a stray capacitance that needs to recharge for the next avalanche
- If enough photons keep hitting the diode so that the cap can't recharge, the avalanche current decreases (c.w.)
- Bob's detector is now blinded and the PD's current now responds classically - with a threshold power $\gg$ a single photon

Faking states

If Eve measures the photons, could we use classical light instead of single photons to control the detector?

- We wouldn't have asked if the answer wasn't yes!
- There is a stray capacitance that needs to recharge for the next avalanche
- If enough photons keep hitting the diode so that the cap can't recharge, the avalanche current decreases (c.w.)
- Bob's detector is now blinded and the PD's current now responds classically - with a threshold power $\gg$ a single photon

Faking states (cont.)



Hooray for faked states

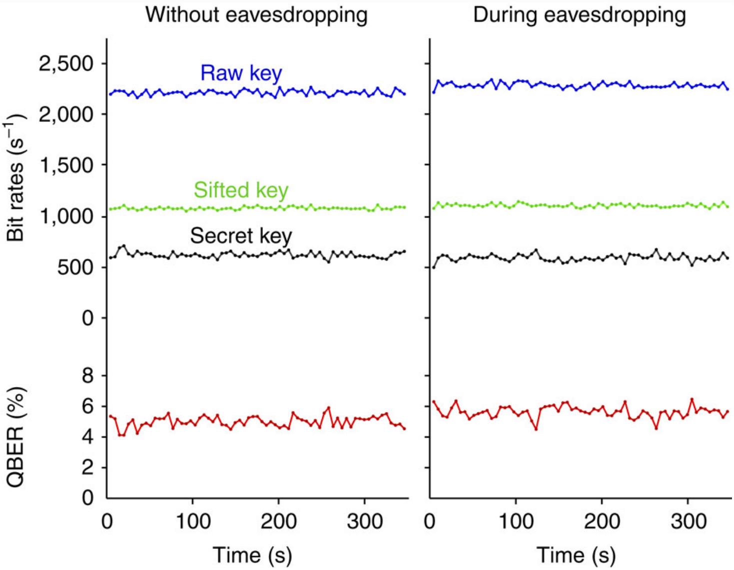
Faked states sent		Clicks at Bob's Detector			
		V	A	H	D
1,702,067	V	1,693,799 (99.51%)	0	0	0
2,055,059	A	0	2,048,072 (99.66%)	0	0
2,620,099	H	0	0	2,614,918 (99.80%)	0
2,359,494	D	0	0	0	2,358,418 (99.95%)

Hooray for faked states

Faked states sent		Clicks at Bob's Detector			
		V	A	H	D
1,702,067	V	1,693,799 (99.51%)	0	0	0
2,055,059	A	0	2,048,072 (99.66%)	0	0
2,620,099	H	0	0	2,614,918 (99.80%)	0
2,359,494	D	0	0	0	2,358,418 (99.95%)

The wrong detector is NEVER triggered!

Hooray for faked states (cont.)



Some thoughts on this attack

- It is based on a specific implementation
- Requires passive basis choice, but...
- Could be detected by measuring intensity
- Brings up a good point: Does the security of QKD actually rely on nature? Or just how well we can build systems?

Some thoughts on this attack

- It is based on a specific implementation
- Requires passive basis choice, but...
- Could be detected by measuring intensity
- Brings up a good point: Does the security of QKD actually rely on nature? Or just how well we can build systems?

Some thoughts on this attack

- It is based on a specific implementation
- Requires passive basis choice, but...
- Could be detected by measuring intensity
- Brings up a good point: Does the security of QKD actually rely on nature? Or just how well we can build systems?

Some thoughts on this attack

- It is based on a specific implementation
- Requires passive basis choice, but...
- Could be detected by measuring intensity
- Brings up a good point: Does the security of QKD actually rely on nature? Or just how well we can build systems?

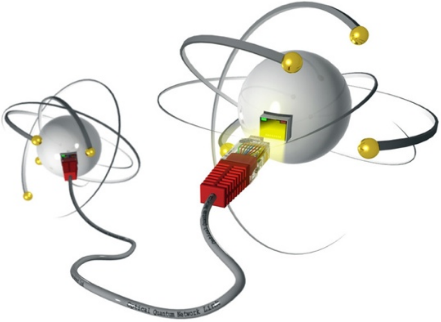
Some thoughts on this attack

- It is based on a specific implementation
- Requires passive basis choice, but...
- Could be detected by measuring intensity
- Brings up a good point: Does the security of QKD actually rely on nature? Or just how well we can build systems?

Some thoughts on this attack

- It is based on a specific implementation
- Requires passive basis choice, but...
- Could be detected by measuring intensity
- Brings up a good point: Does the security of QKD actually rely on nature? Or just how well we can build systems?

Quantum Networks



What are they?

A quantum network is a set of quantum nodes connected by quantum channels

Main motivations for building quantum networks:

- Connecting quantum computing/communication elements
- Investigating quantum interactions (fundamental research)

This can be achieved by sending quantum particles or distributing entanglement interactions.

What are they?

A quantum network is a set of quantum nodes connected by quantum channels

Main motivations for building quantum networks:

- Connecting quantum computing/communication elements
- Investigating quantum interactions (fundamental research)

This can be achieved by sending quantum particles or distributing entanglement interactions.

Forget (almost) everything you just learned

And focus on the problem: we need to establish a quantum channel over a long distance. Don't worry about polarization encoding, one-time-pads, etc...

Forget (almost) everything you just learned

And focus on the problem: we need to establish a quantum channel over a long distance. Don't worry about polarization encoding, one-time-pads, etc...

The problem

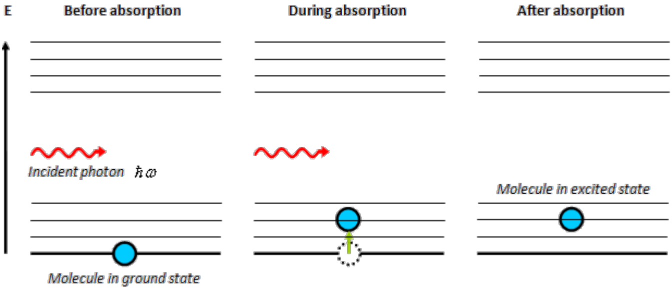
Earlier in lecture: optical fiber has attenuation of ≈ 0.15 dB/km

But what does that mean physically?

The problem

Earlier in lecture: optical fiber has attenuation of ≈ 0.15 dB/km

But what does that mean physically?



For a single photon, probability of absorption $\sim \exp(L_{\text{fiber}})$

The problem (cont.)

Earlier, we said no cloning . . . so amplifiers are out.

The problem (cont.)

Earlier, we said no cloning . . . so amplifiers are out.

What if instead of copying states, we extended them so that they would cover the necessary range?

Introducing Quantum Repeaters:

- The idea is to create entanglement pairs over long distances
- This can be accomplished by utilizing intermediate "connection points"
- At these connection points, we can swap entanglement states
- Remember, we aren't copying - we're transferring
- Major challenge: heralding

The problem (cont.)

Earlier, we said no cloning . . . so amplifiers are out.

What if instead of copying states, we extended them so that they would cover the necessary range?

Introducing Quantum Repeaters:

- The idea is to create entanglement pairs over long distances
- This can be accomplished by utilizing intermediate "connection points"
- At these connection points, we can swap entanglement states
- Remember, we aren't copying - we're transferring
- Major challenge: heralding

The problem (cont.)

Earlier, we said no cloning . . . so amplifiers are out.

What if instead of copying states, we extended them so that they would cover the necessary range?

Introducing Quantum Repeaters:

- The idea is to create entanglement pairs over long distances
- This can be accomplished by utilizing intermediate "connection points"
- At these connection points, we can swap entanglement states
- Remember, we aren't copying - we're transferring
- Major challenge: heralding

The problem (cont.)

Earlier, we said no cloning . . . so amplifiers are out.

What if instead of copying states, we extended them so that they would cover the necessary range?

Introducing Quantum Repeaters:

- The idea is to create entanglement pairs over long distances
- This can be accomplished by utilizing intermediate "connection points"
- At these connection points, we can swap entanglement states
- Remember, we aren't copying - we're transferring
- Major challenge: heralding

The problem (cont.)

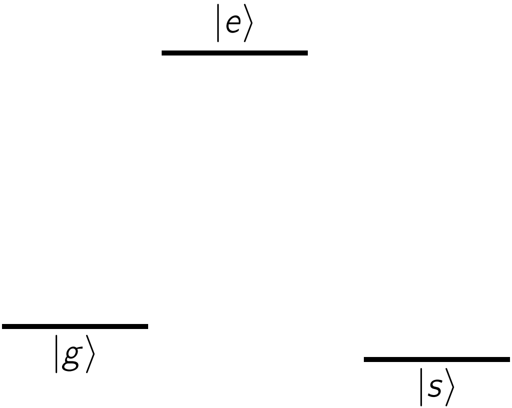
Earlier, we said no cloning . . . so amplifiers are out.

What if instead of copying states, we extended them so that they would cover the necessary range?

Introducing Quantum Repeaters:

- The idea is to create entanglement pairs over long distances
- This can be accomplished by utilizing intermediate “connection points”
- At these connection points, we can swap entanglement states
- Remember, we aren’t copying - we’re transferring
- Major challenge: heralding

A little bit more on atoms and photons



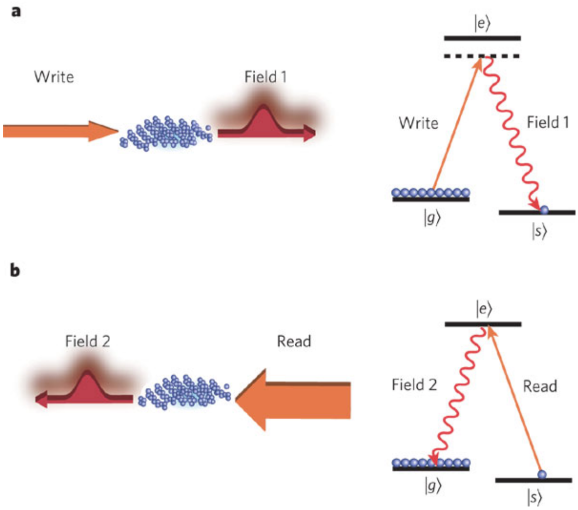
State transfer using atomic energy levels

- If we can force a transition from $|g\rangle \rightarrow |e\rangle \rightarrow |s\rangle$, then detection of the photon from the $|e\rangle \rightarrow |s\rangle$ transition can herald our storage
- However, ensuring a particular photon couples with a specific atom is difficult for many reasons

State transfer using atomic energy levels

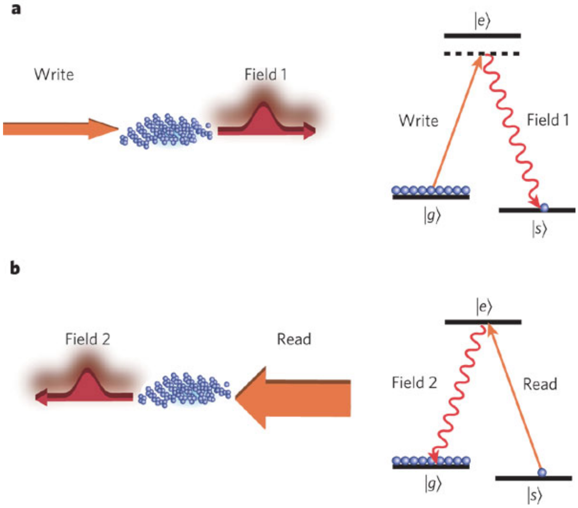
- If we can force a transition from $|g\rangle \to |e\rangle \to |s\rangle$, then detection of the photon from the $|e\rangle \to |s\rangle$ transition can herald our storage
- However, ensuring a particular photon couples with a specific atom is difficult for many reasons
- So use lots of photons and lots of atoms!

State transfer using many-body systems (picture form)



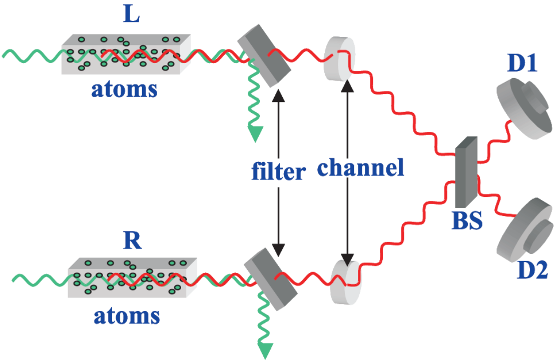
That's nice, but we were really interested in entanglement

State transfer using many-body systems (picture form)



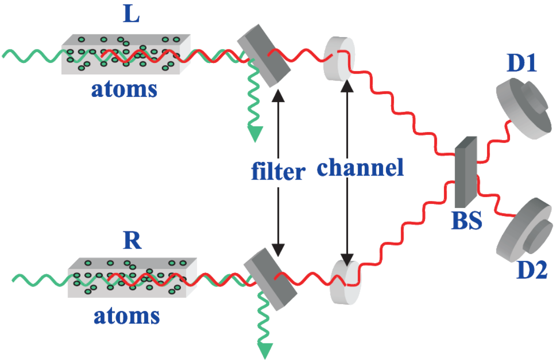
That's nice, but we were really interested in entanglement

Duan, Lukin, Cirac and Zoller (DLCZ) Protocol



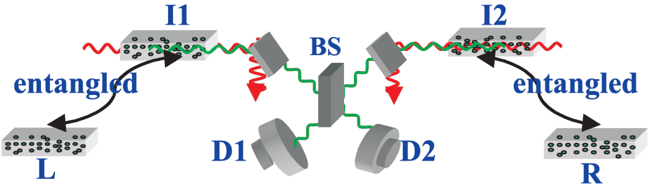
- The pulses from the photons interfere at the 50/50 NPBS
- A click at only one of D_1 or D_2 $\Rightarrow$ ensembles are entangled

Duan, Lukin, Cirac and Zoller (DLCZ) Protocol



- The pulses from the photons interfere at the 50/50 NPBS
- A click at only one of D_1 or D_2 $\Rightarrow$ ensembles are entangled
- A single click indicates that one of the ensembles (we don't know which) has transitioned from $|g\rangle$ to $|s\rangle$

DLCZ Repeater

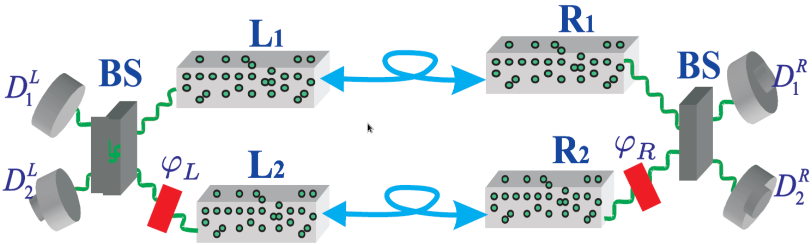


- Prepare two entangled pairs
- "Read" the states simultaneously
- Just like before, the photons interfere at the BS and a click signals success (L & R are entangled)
- This allows for quantum communication over long distances

DLCZ Repeater thoughts

- Can tolerate certain inefficiencies very well - photon detectors 50% or lower efficiency should work
- However, this is still a highly intricate system
- But, the error rate is projected to be $\ll$ than the attenuation
- Still waiting on some good experiments

QKD using DLCZ



The Grand Conclusion

- QKD is theorectically secure and appears to be feasible (with existing commercial implementations)
- As always, implementation is a key detail regarding security
- Quantum networks are a long, long way off
- Research on quantum computing seems to be worse off than communication, so you've still got time left on your private keys

References I

M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*.
Cambridge ; New York: Cambridge University Press, 2000.

I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," *Nature Communications*, vol. 2, p. 349, June 2011.

K. D. Greve, L. Yu, P. L. McMahon, J. S. Pelc, C. M. Natarajan, N. Y. Kim, E. Abe, S. Maier, C. Schneider, M. Kamp, S. Höfling, R. H. Hadfield, A. Forchel, M. M. Fejer, and Y. Yamamoto, "Quantum-dot spin-photon entanglement via frequency downconversion to telecom wavelength," *Nature*, vol. 491, pp. 421–425, Nov. 2012.

H. J. Kimble, "The quantum internet," *Nature*, vol. 453, pp. 1023–1030, June 2008.

References II

V. Makarov * and D. R. Hjelme, “Faked states attack on quantum cryptosystems,” *Journal of Modern Optics*, vol. 52, no. 5, pp. 691–705, 2005.

R. P. Feynman, *QED : the strange theory of light and matter*. Princeton, N.J.: Princeton University Press, 1988.

N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Reviews of Modern Physics*, vol. 74, pp. 145–195, Mar. 2002.

D. J. Rogers, *Broadband quantum cryptography*. [San Rafael, Calif.]: Morgan & Claypool Publishers, 2010.

Caltech Quantum Optics, “Quantum networking with atomic ensembles.” `http://www.its.caltech.edu/~qoptics/lab2/index.html`, Mar. 2013.

References III

- H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, pp. 5932–5935, Dec 1998.
- L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, pp. 413–418, Nov. 2001.
- M. S. Mendes and D. Felinto, "Perspectives for laboratory implementation of the duan-lukin-cirac-zoller protocol for quantum repeaters," *Physical Review A*, vol. 84, p. 062303, Dec. 2011.
- M. D. Eisaman, S. Polyakov, M. Hohensee, J. Fan, P. Hemmer, and A. Migdall, "Optimizing the storage and retrieval efficiency of a solid-state quantum memory through tailored state preparation," pp. 67800K–67800K, Sept. 2007.