Introduction to Quantum Cryptography

Yan Li <yanli@cs.ucsc.edu>

CMPS 290X, Spring, 2013

University of California, Santa Cruz

Baskin Engineering
UC SANTA CRUZ

Agenda

Introduction to quantum cryptography

The elements of quantum physics

Quantum key exchange

Technological challenges

Experimental results

Eavesdropping

Two major areas of quantum cryptography

Quantum key exchange

exchanging bits securely via a quantum channel, with the help of a classical channel, which can be public but must be authentic

Cryptography on quantum computers

Shor's algorithm, anything else?

Quantum key exchange

Transferring data via a quantum channel is inefficient

used for key exchange only

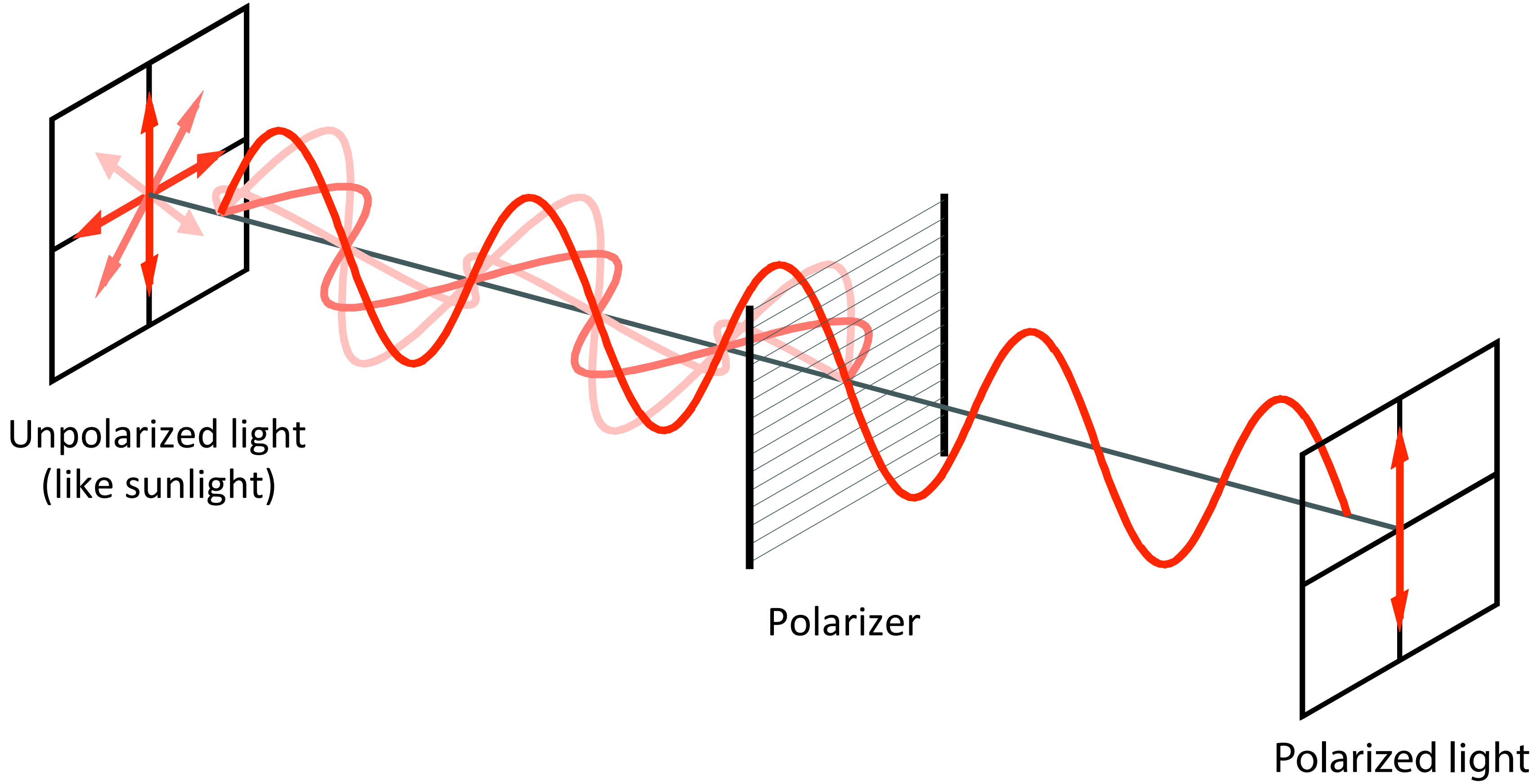
Need a public classical channel

for coordinating the key exchange and transferring data

Can be used for one-time pad or with other symmetrical ciphers

The elements of quantum physics

Unpolarized light through a polarizer



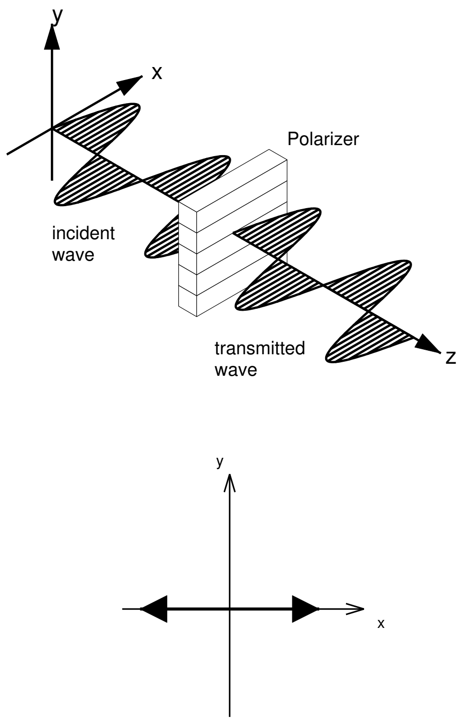
http://en.wikipedia.org/wiki/File:Wire-grid-polarizer.svg

Polarized light through another polarizer

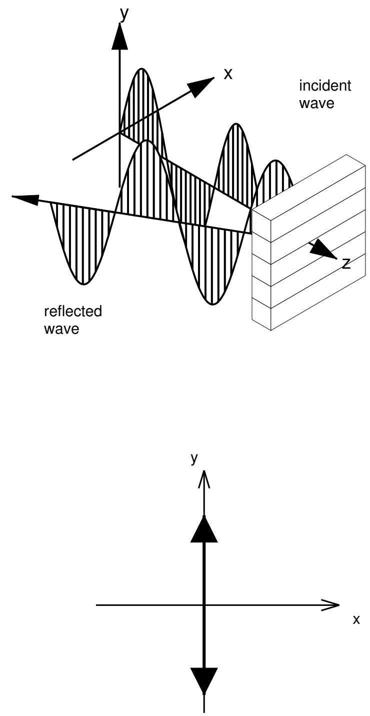
polarizer in front of a computer flat screen

http://en.wikipedia.org/wiki/File:Animation_polariseur_2.gif

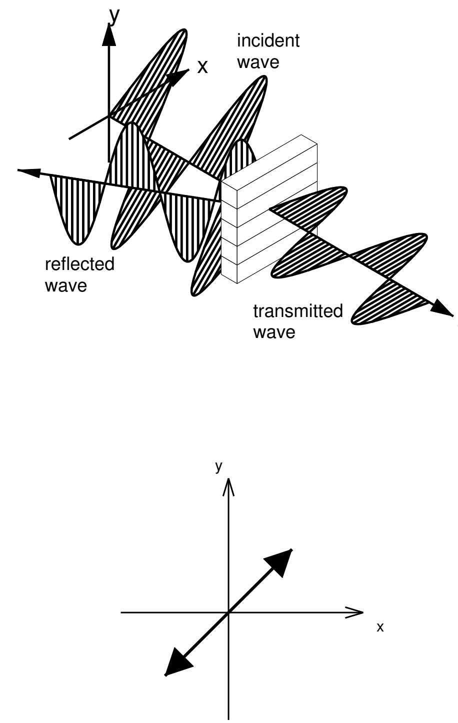
Polarized light through a polarizer



Horizontal polarization



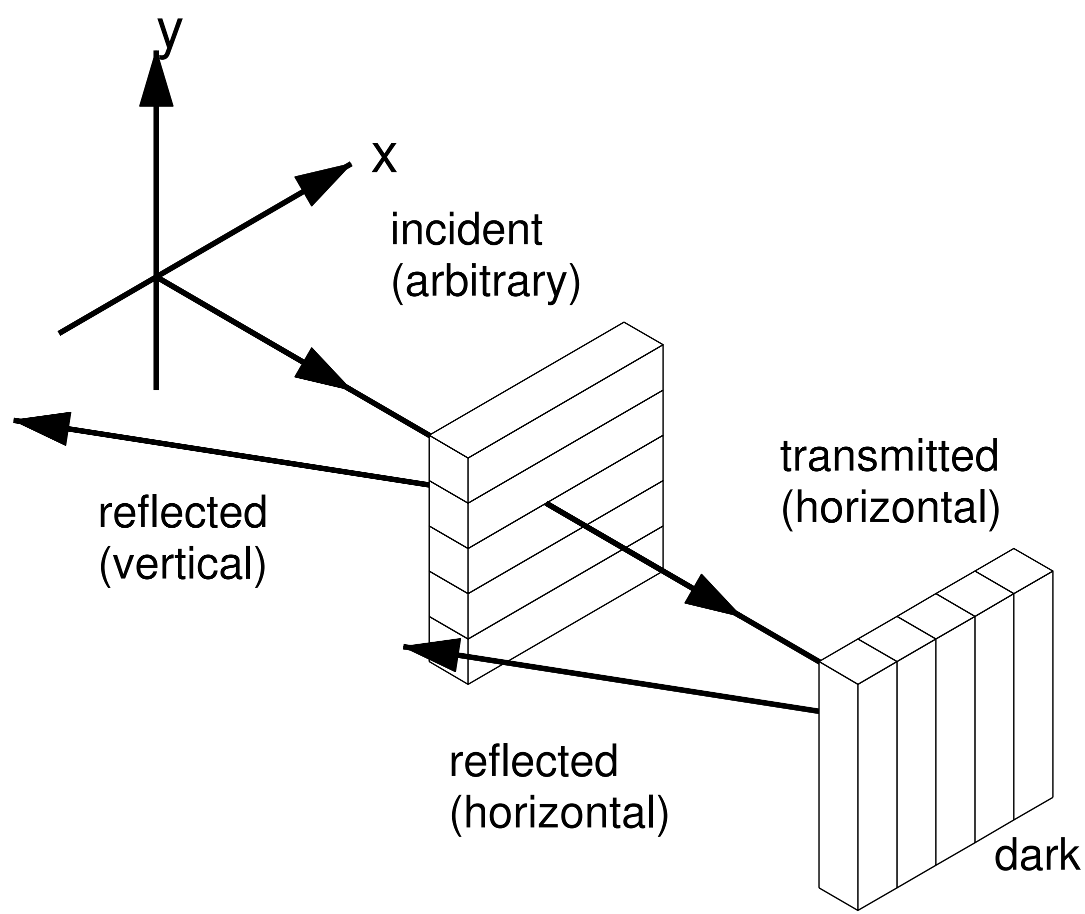
Vertical polarization



Arbitrary linear polarization

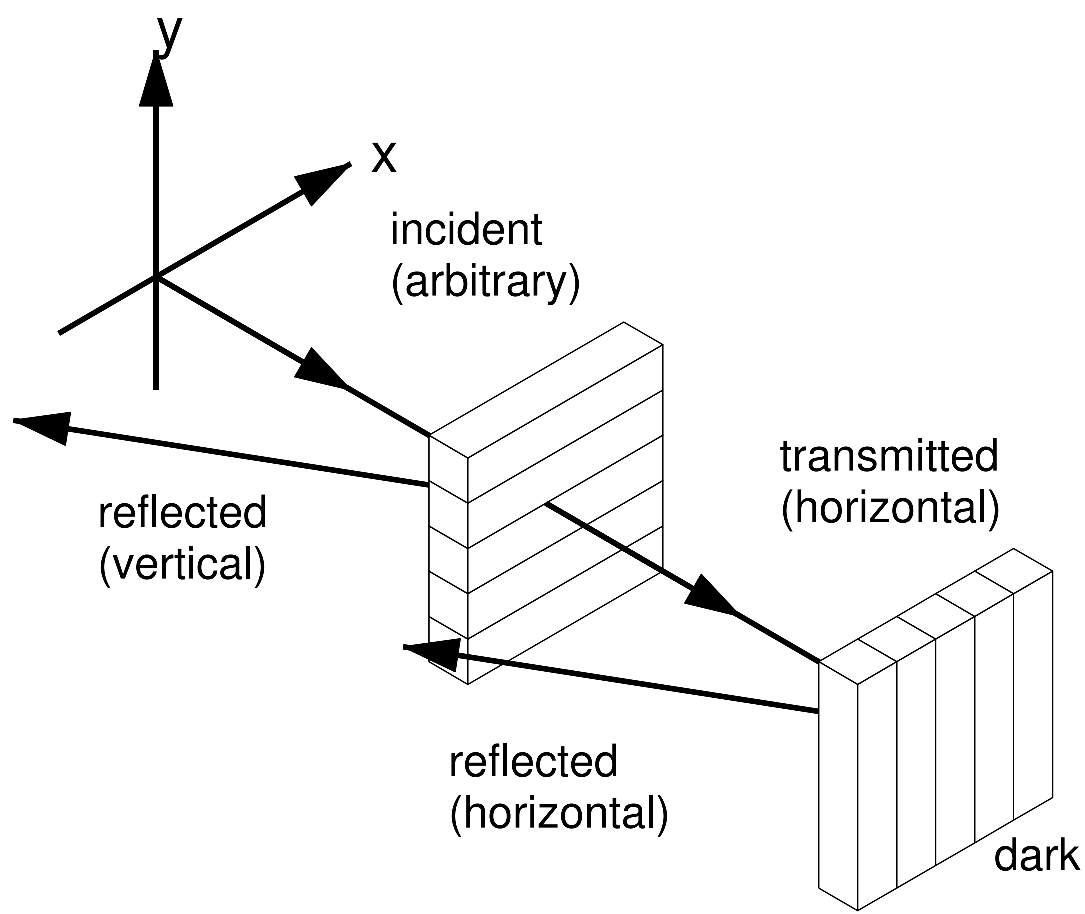
http://www.physics.metu.edu.tr/~sturgut/p507/pol.pdf

No light can pass orthogonal polarizers



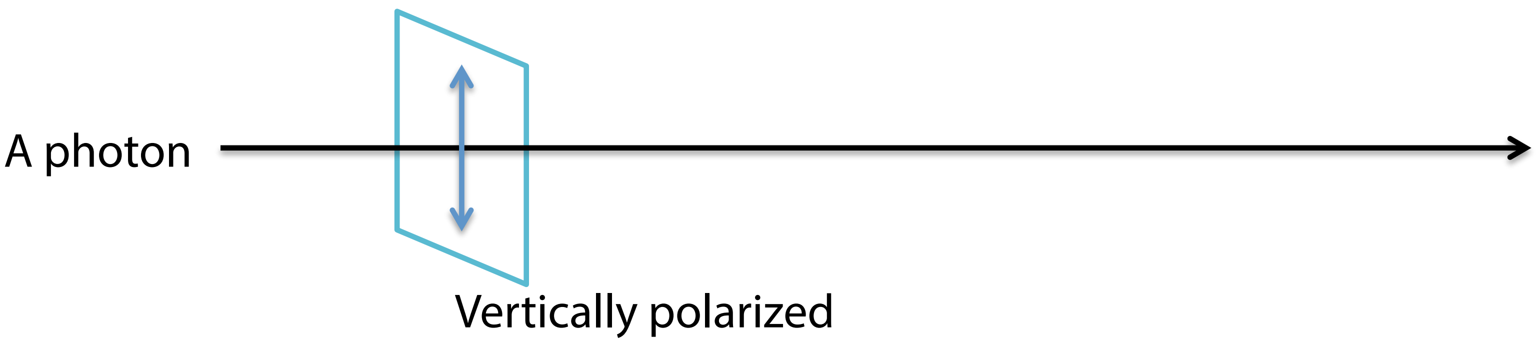
http://www.physics.metu.edu.tr/~sturgut/p507/pol.pdf

Same for photons



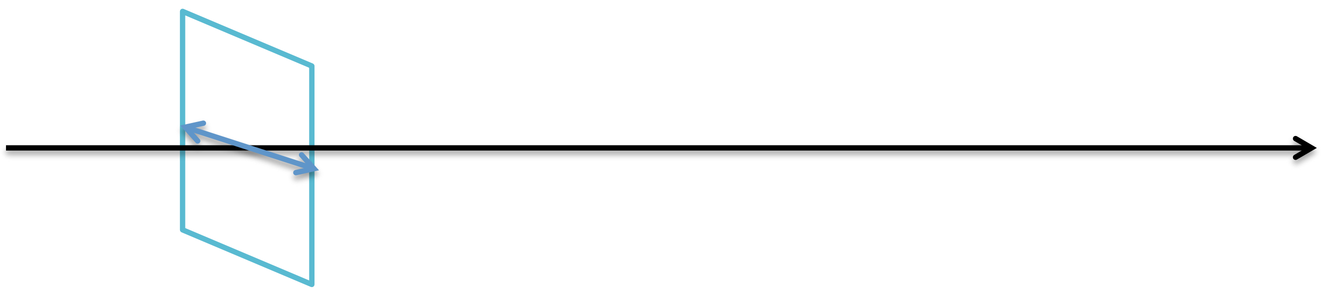
http://www.physics.metu.edu.tr/~sturgut/p507/pol.pdf

Polarization state of a photon



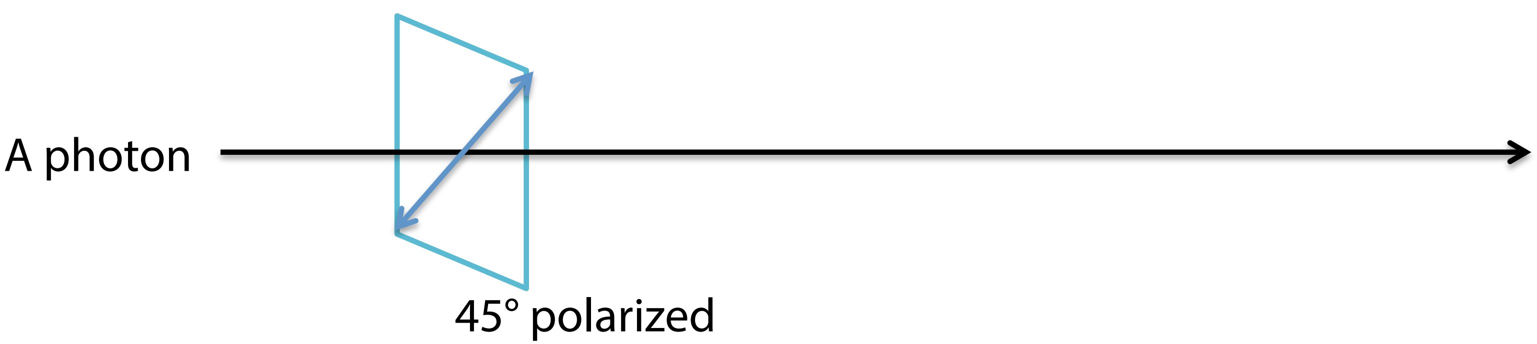
Polarization state of a photon

A photon

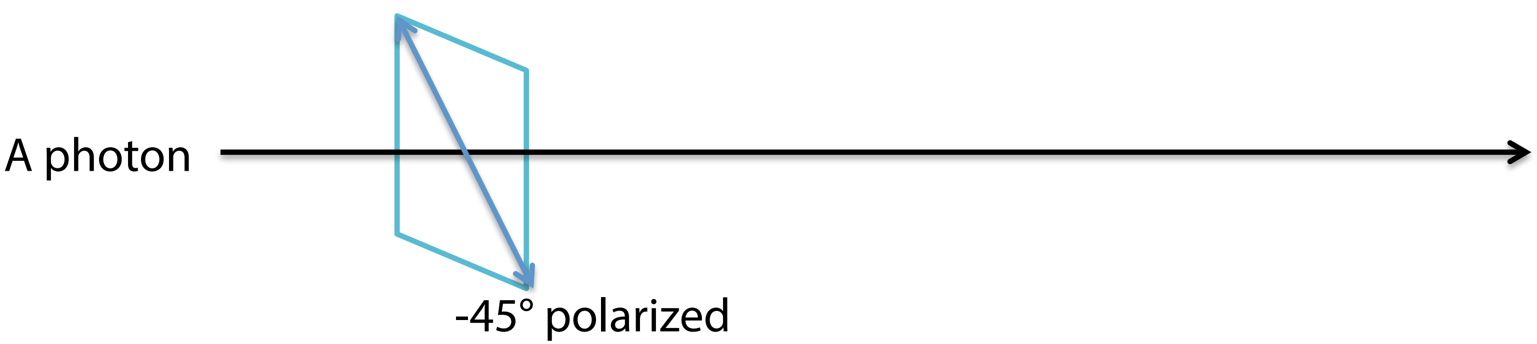


Horizontally polarized

Polarization state of a photon



Polarization state of a photon



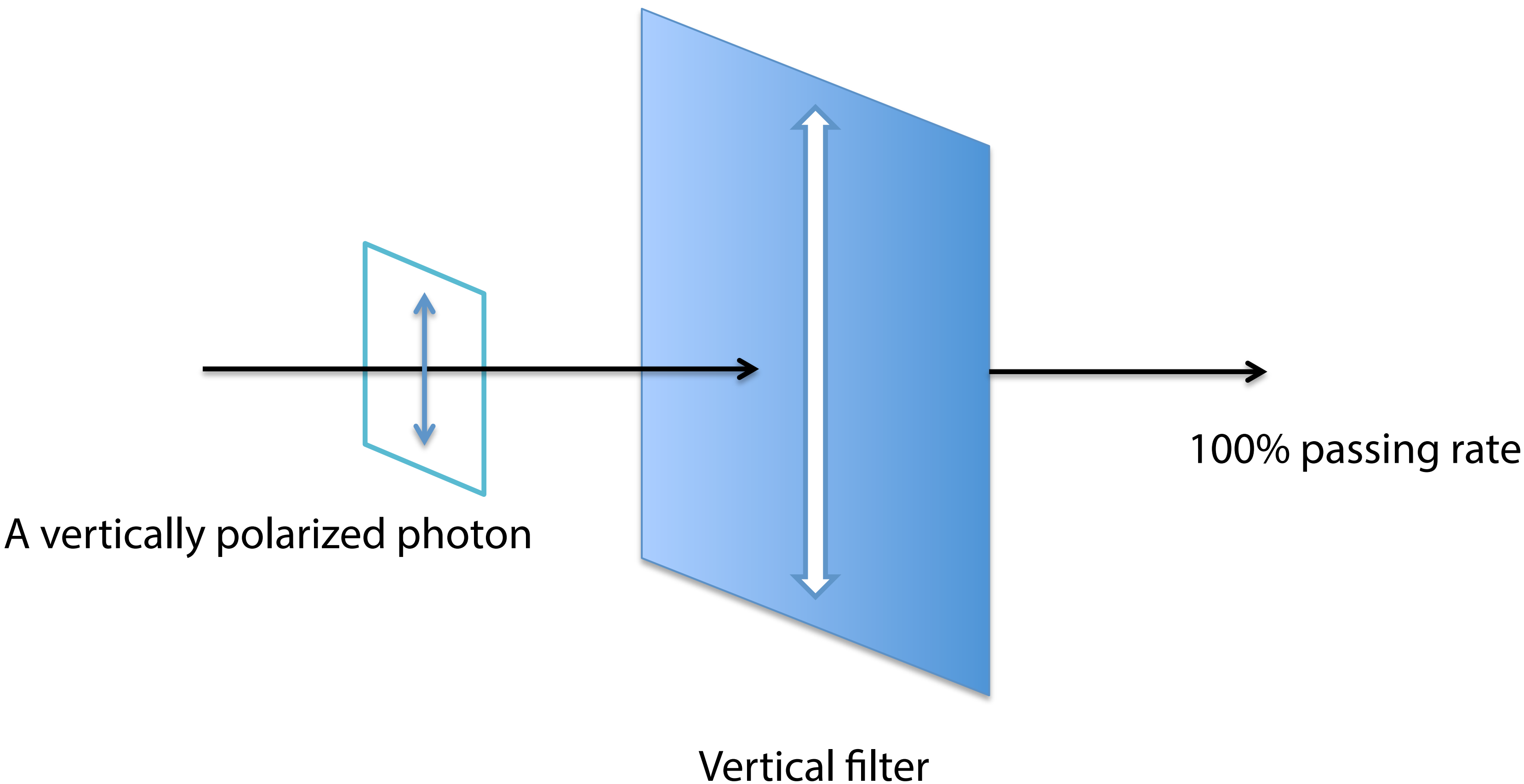
Quantum indeterminism

a fundamental principle of quantum mechanics

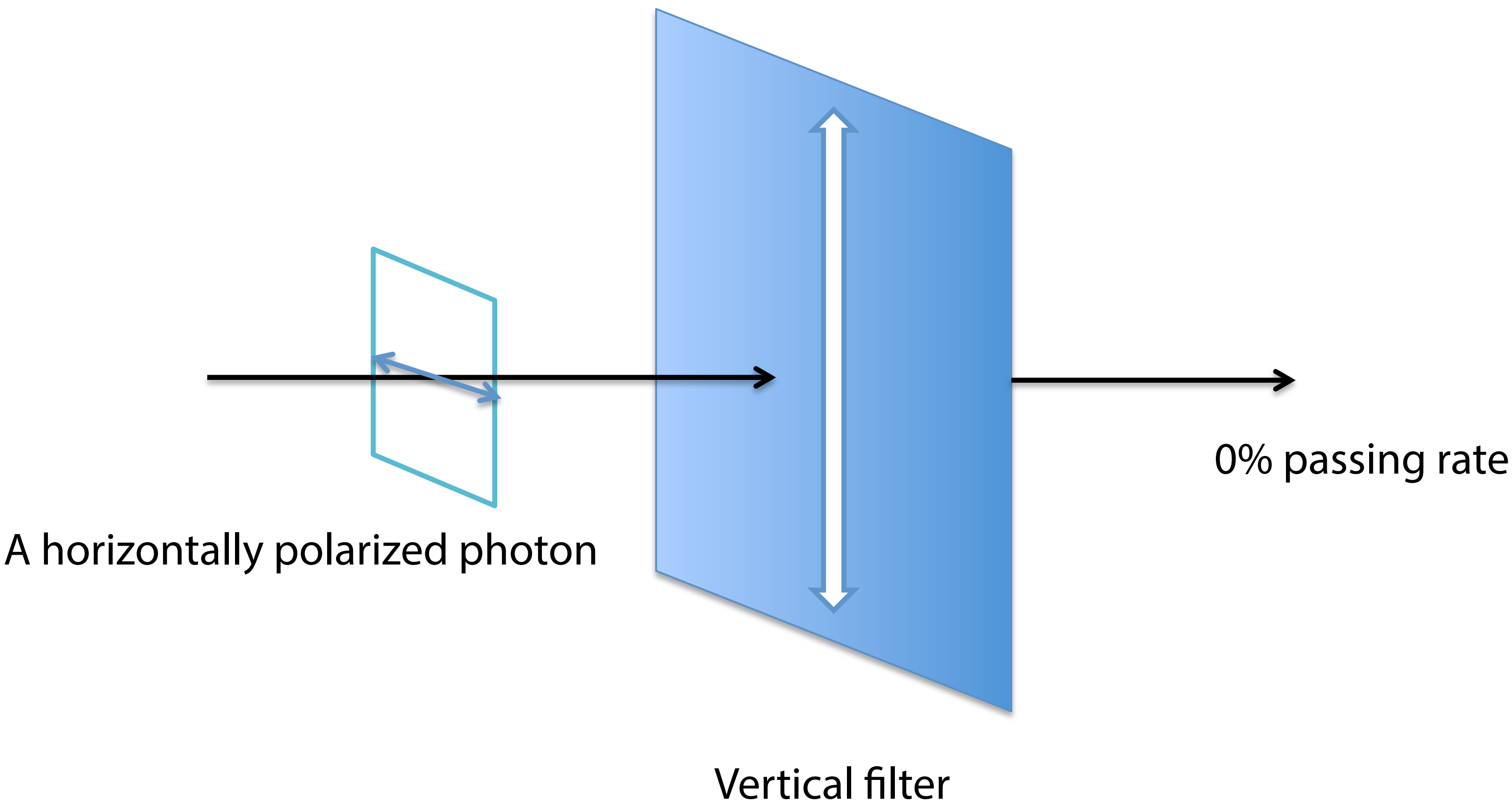
A physical system—such as a photon—exists partly in **all** its particular, theoretically **possible states** simultaneously; but, when measured or observed, it gives a result corresponding to only one of the possible configurations.

http://en.wikipedia.org/wiki/Quantum_superposition

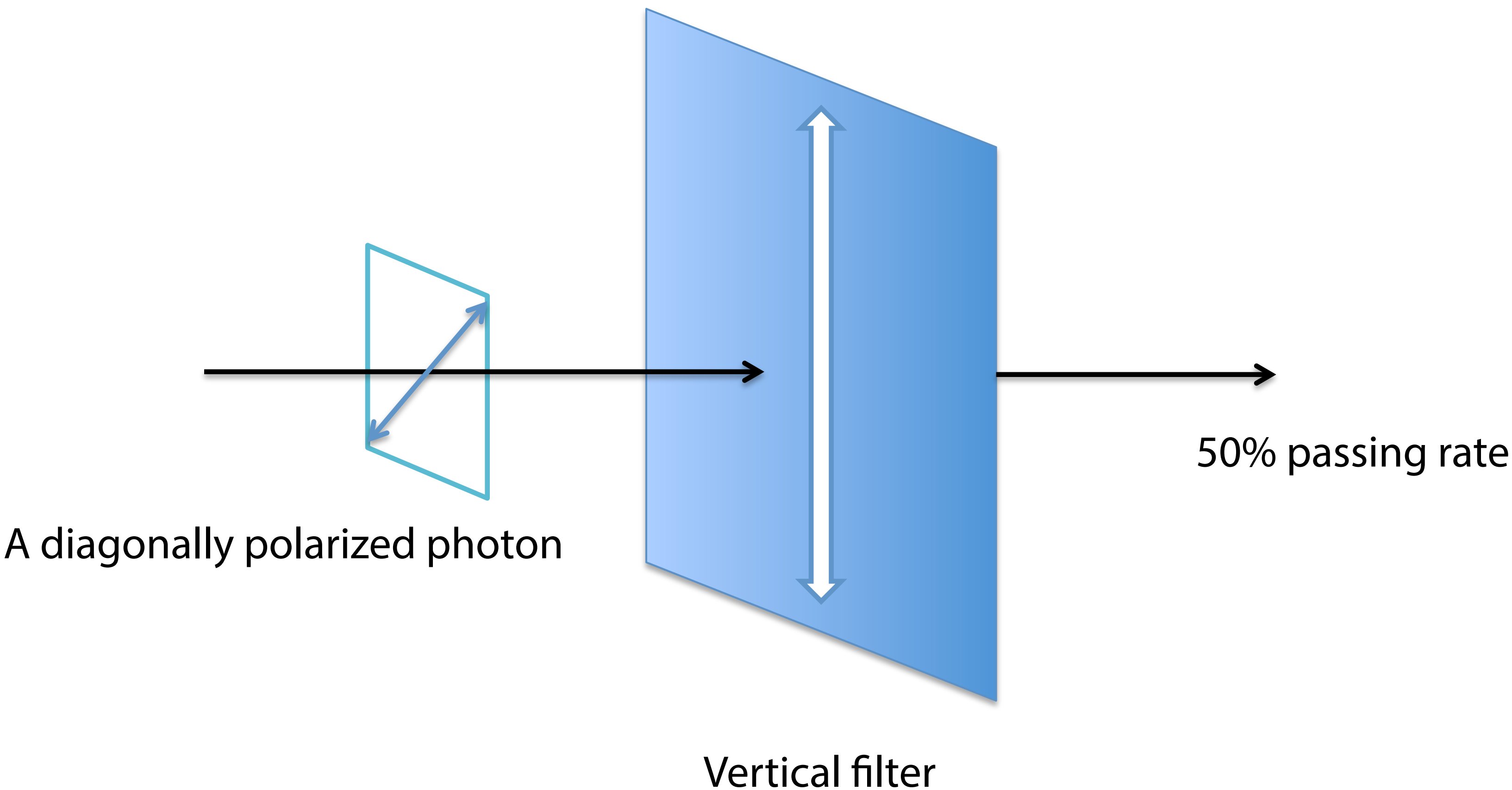
Photons passing a polarizer



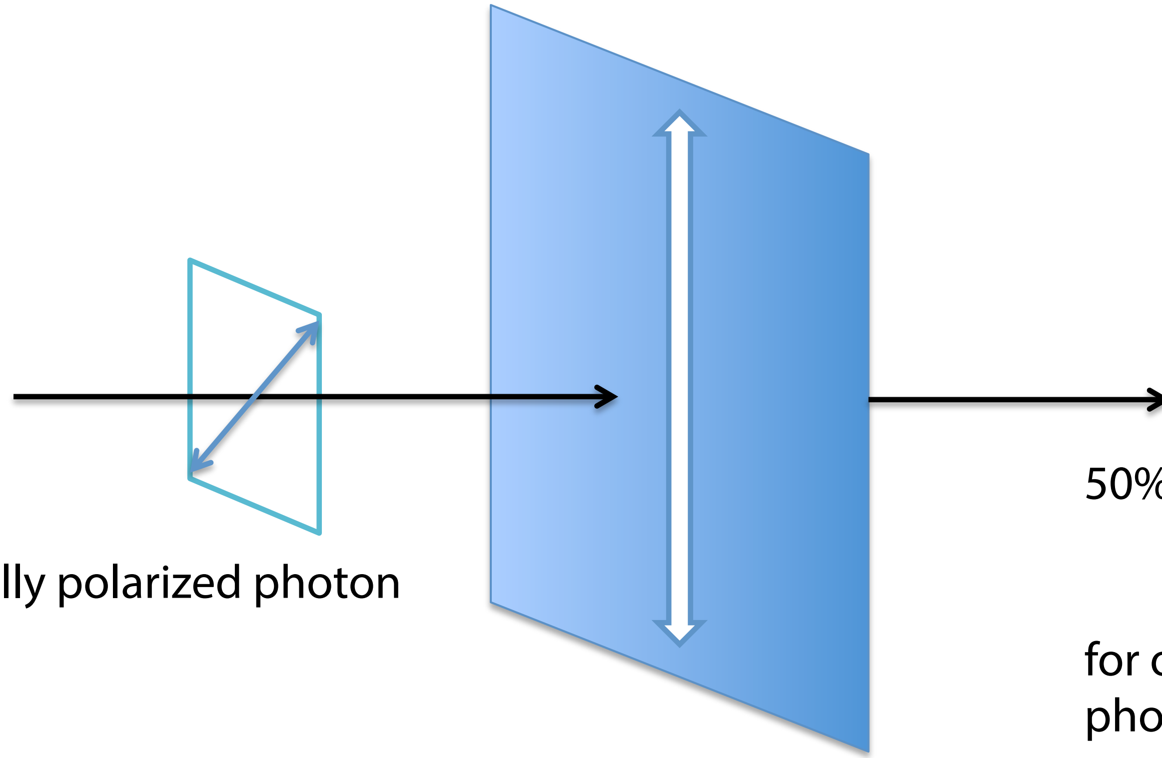
Photons passing a polarizer



Photons passing a polarizer



Photons passing a polarizer



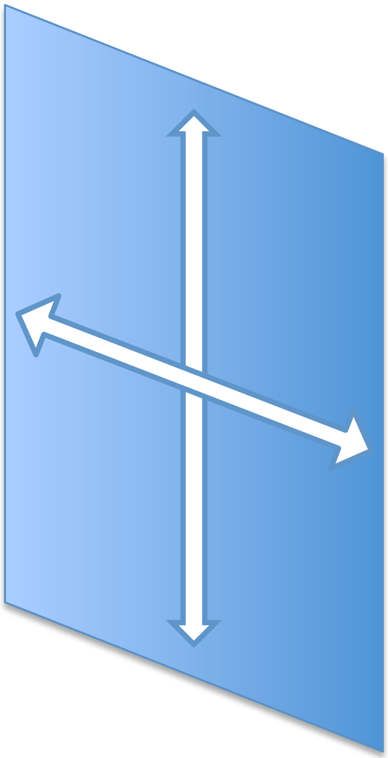
A diagonally polarized photon

Vertical filter

50% passing rate

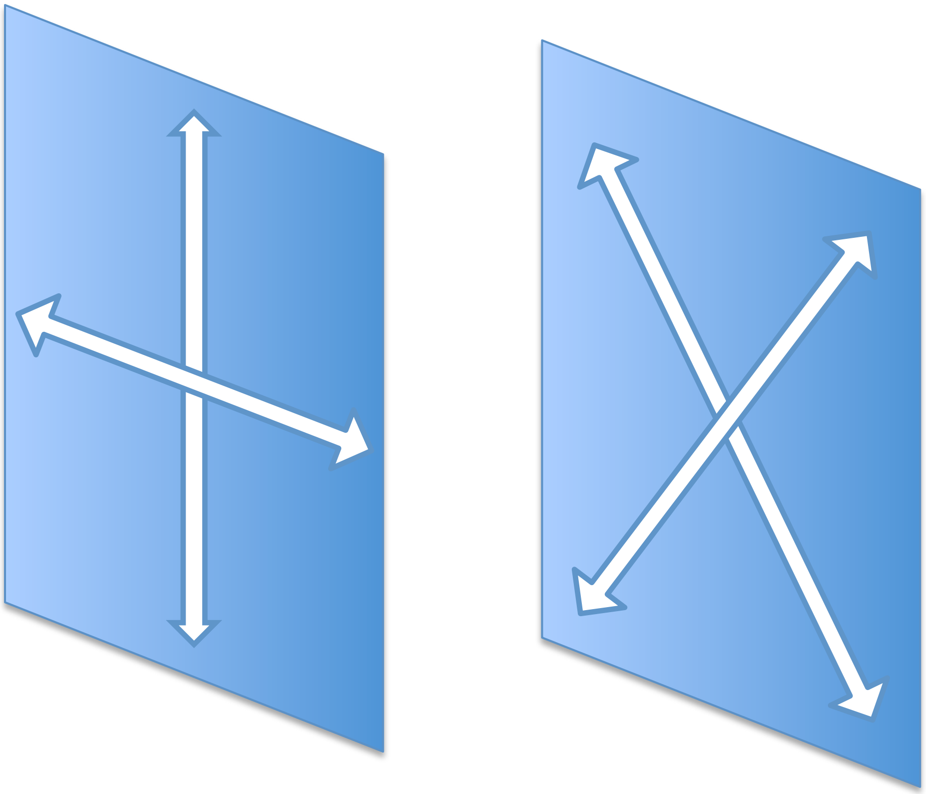
for one specific photon, the result is totally random and unpredictable

Two quantum states constitute a basis



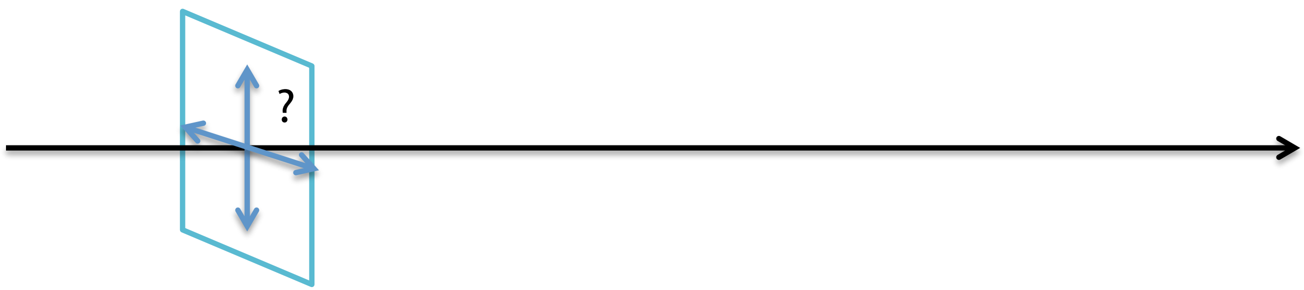
a basis

Two quantum states constitute a basis



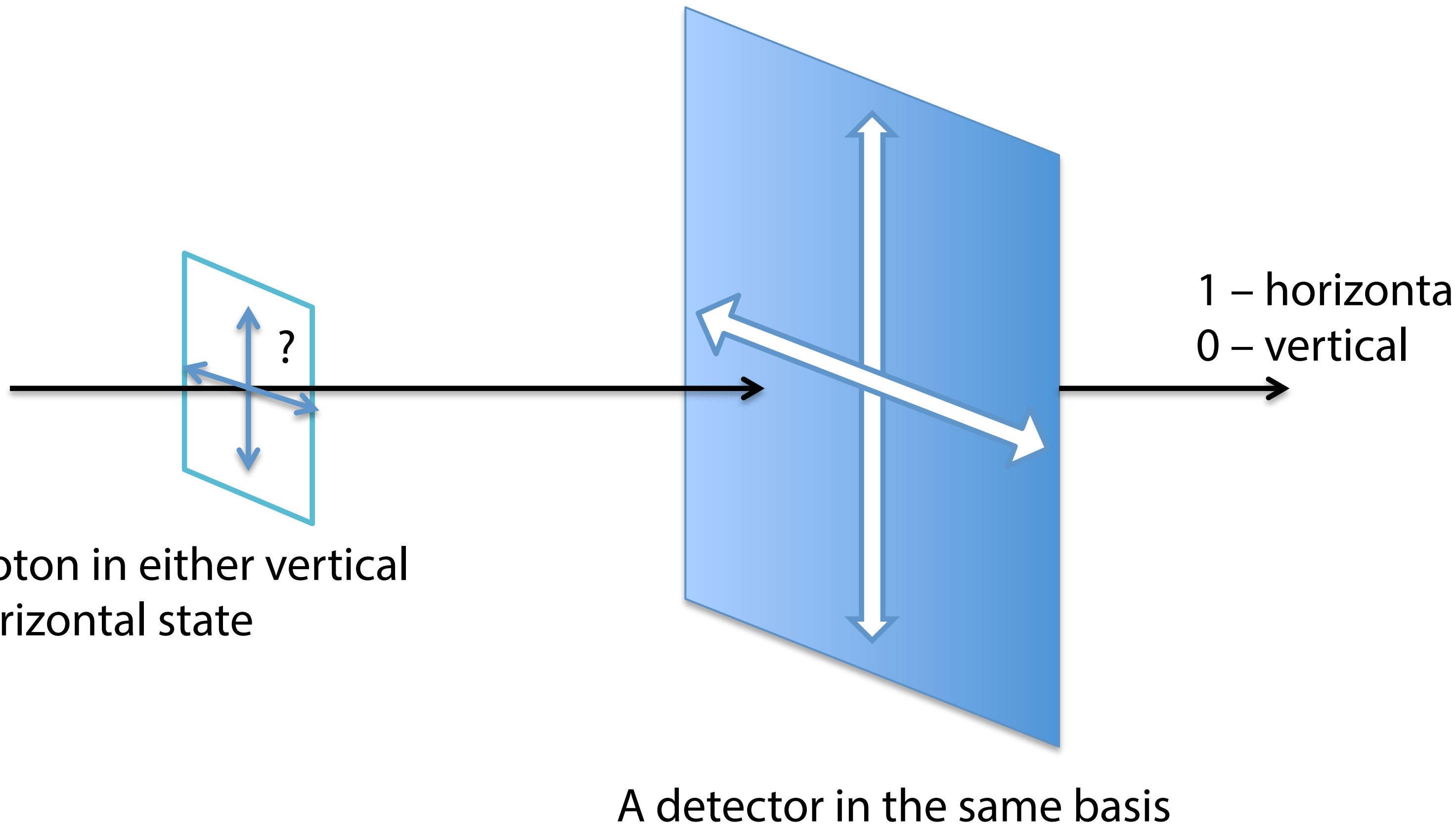
two different bases

Detecting a photon's state

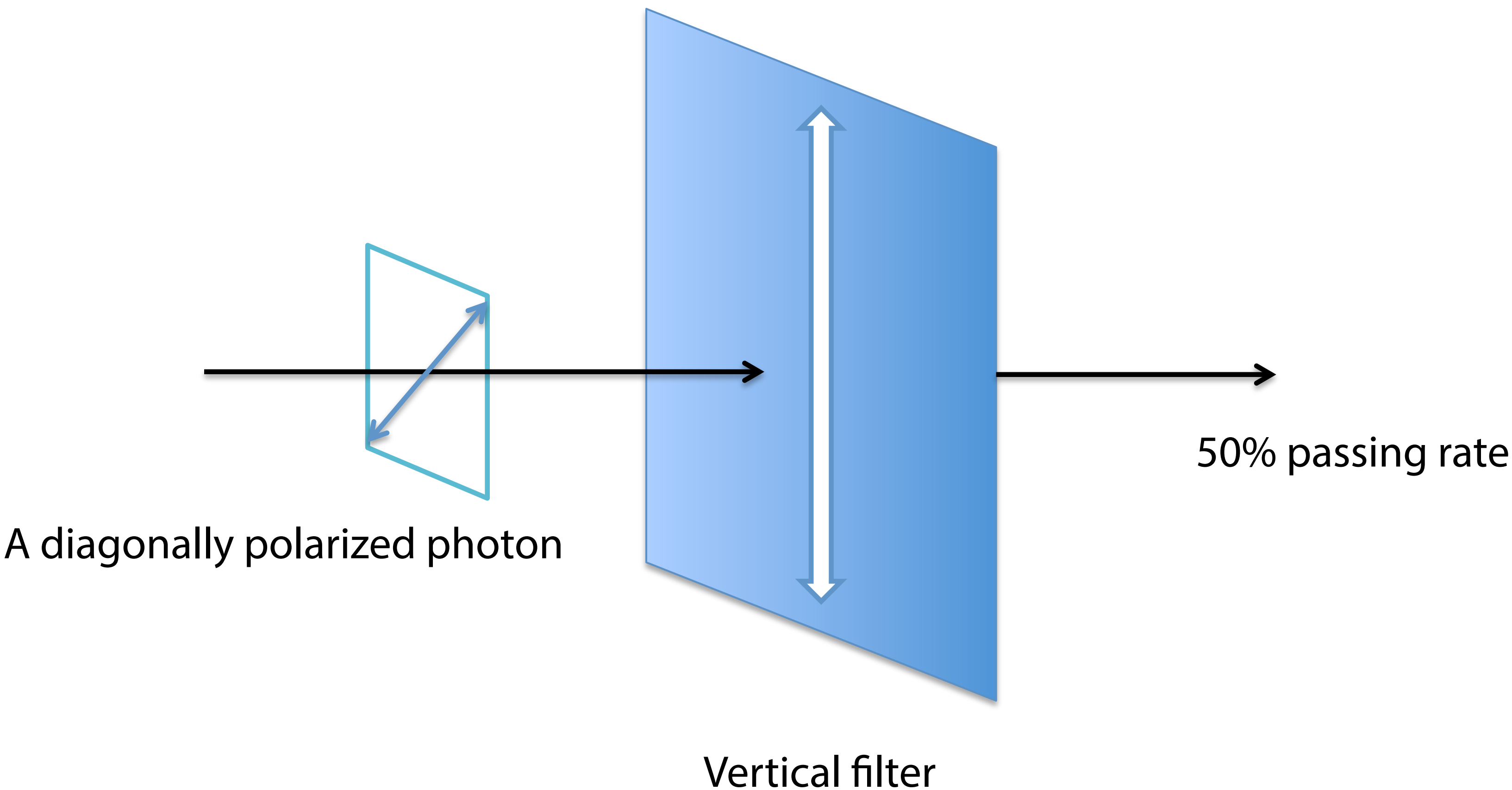


A photon in either vertical
or horizontal state

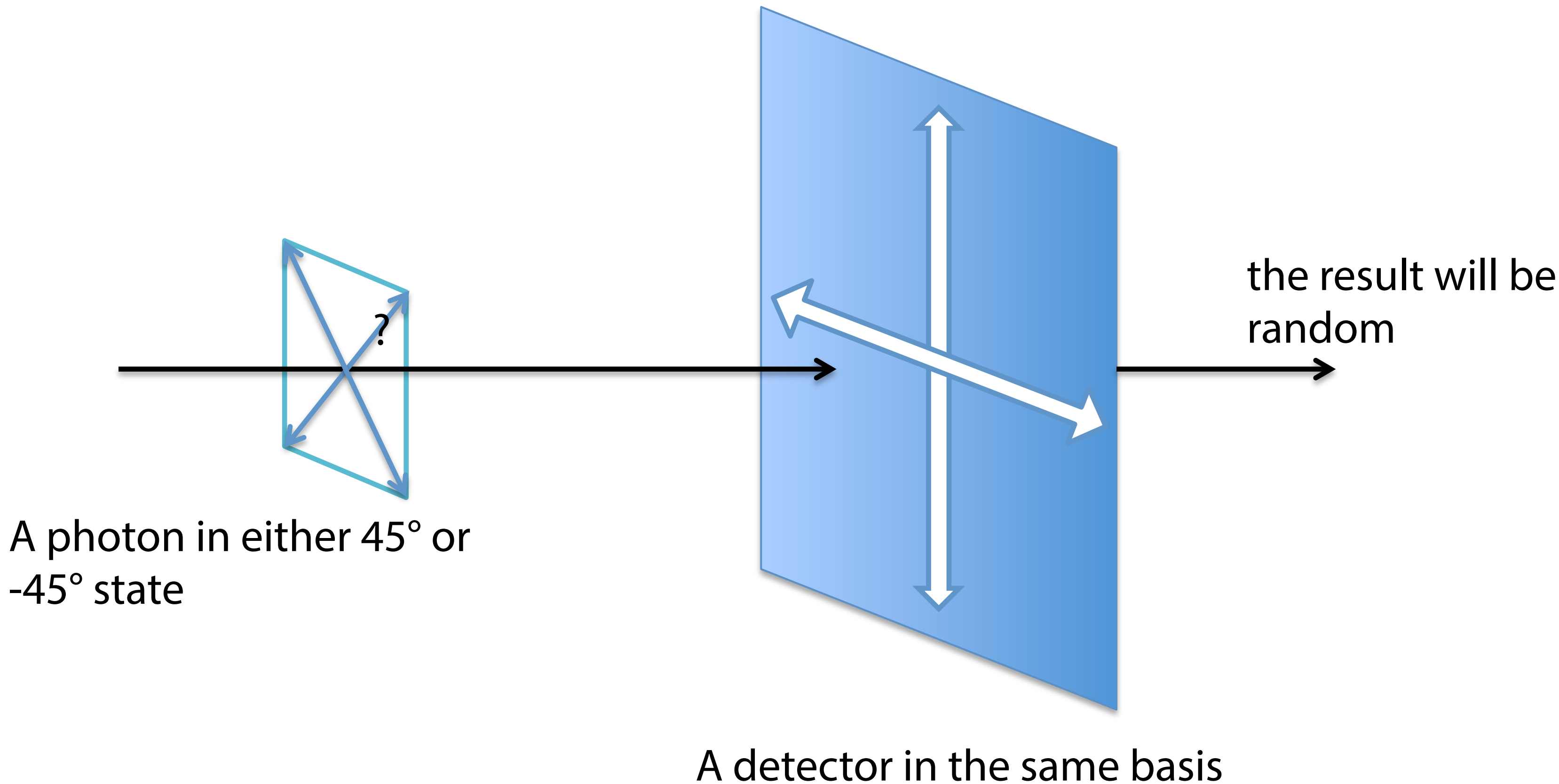
A detector in the same basis yields 100% accurate results



Photons passing a polarizer



Using a wrong basis yields 50% detection rate



Two important properties

In order to correctly identify the status of a photon, the basis must be known

quantum indeterminism

Measuring a photon destroys its state

thus, no-cloning

The BB84 Protocol

The BB84 Protocol

Relies on quantum indeterminism and no-cloning theorem

Can be used between Alice and Bob to “negotiate” a key through a quantum channel + a classical channel

the classical channel doesn’t have to be confidential, but has to be authentic

Key is generated on-the-fly

neither Alice nor Bob knows the key beforehand

The BB84 Protocol's steps

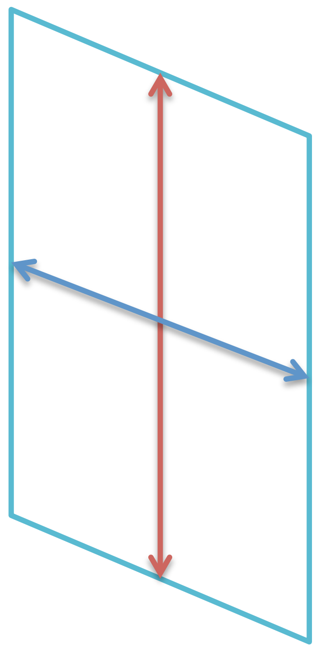
1. Key transmission through the quantum channel
for getting a "raw key"

2. Error correction
for getting a "sifted key"

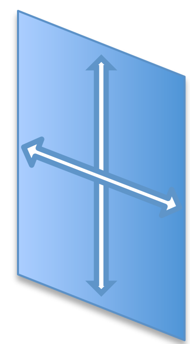
3. Key distillation
to counter man-in-the-middle attack

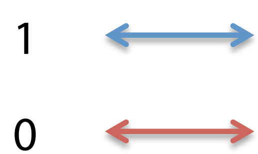
Alice randomly generates a bit randomly and randomly choose a basis to generate a photon

Use these two states



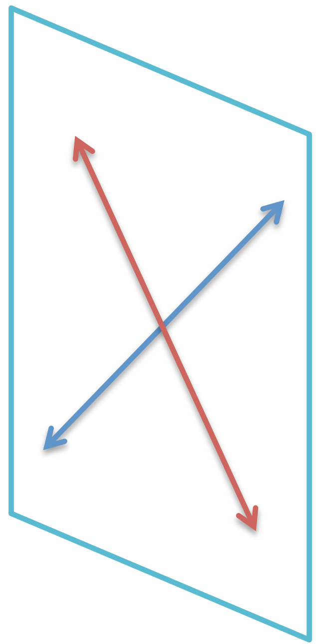
with basis 1



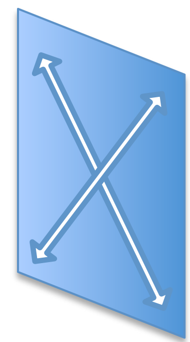


Alice randomly generates a bit randomly and randomly choose a basis to generate a photon

Use these two states

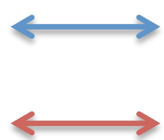


with basis 2

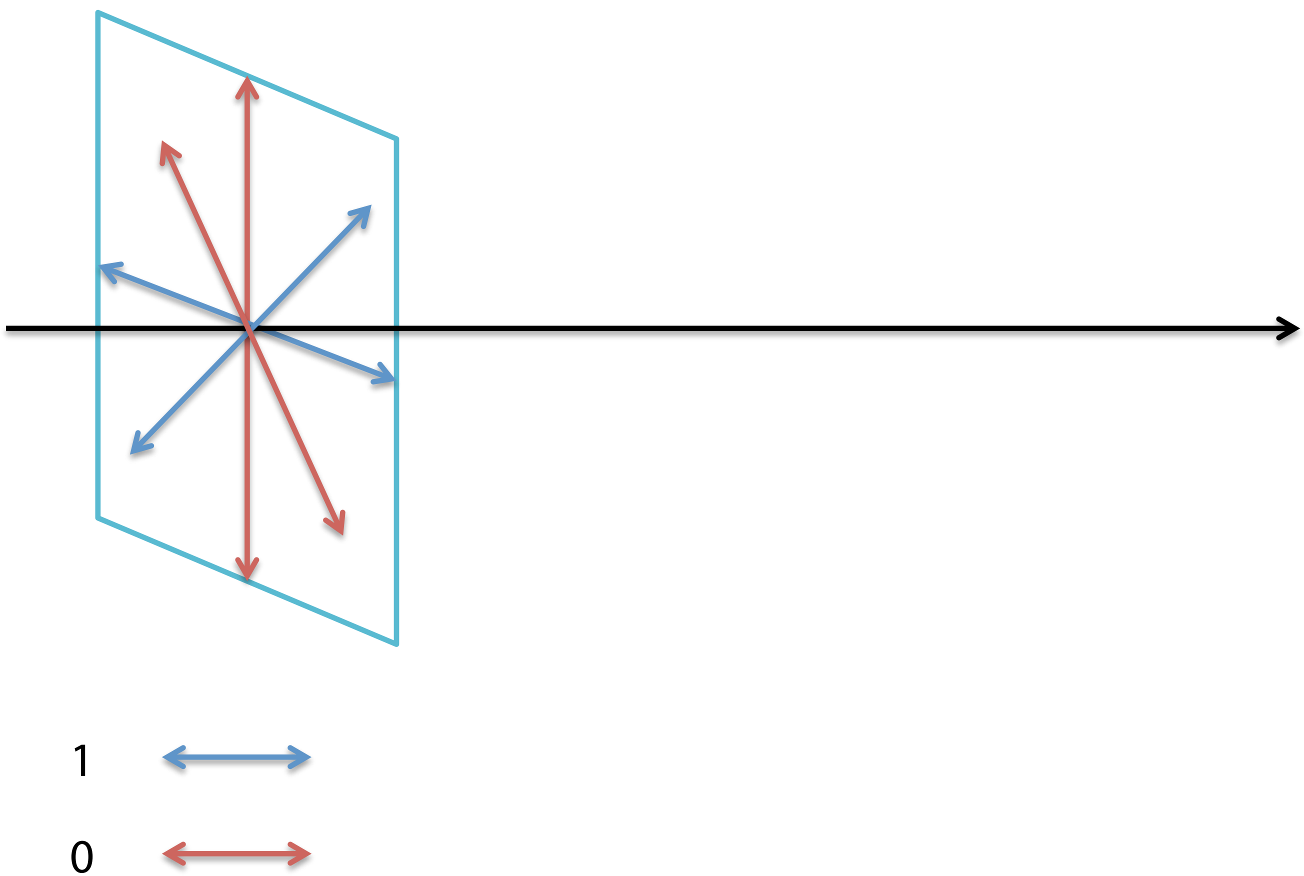


1

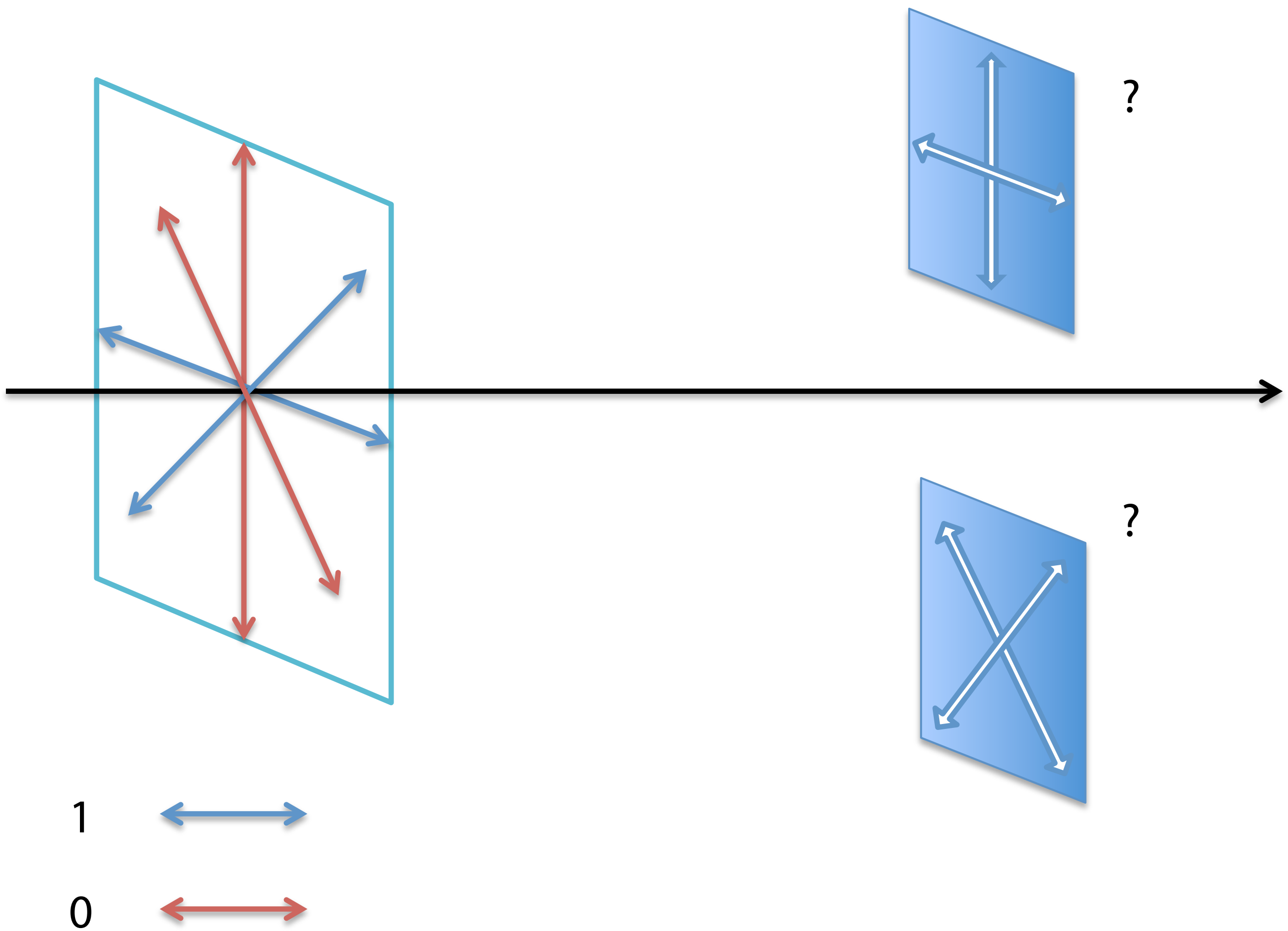
0



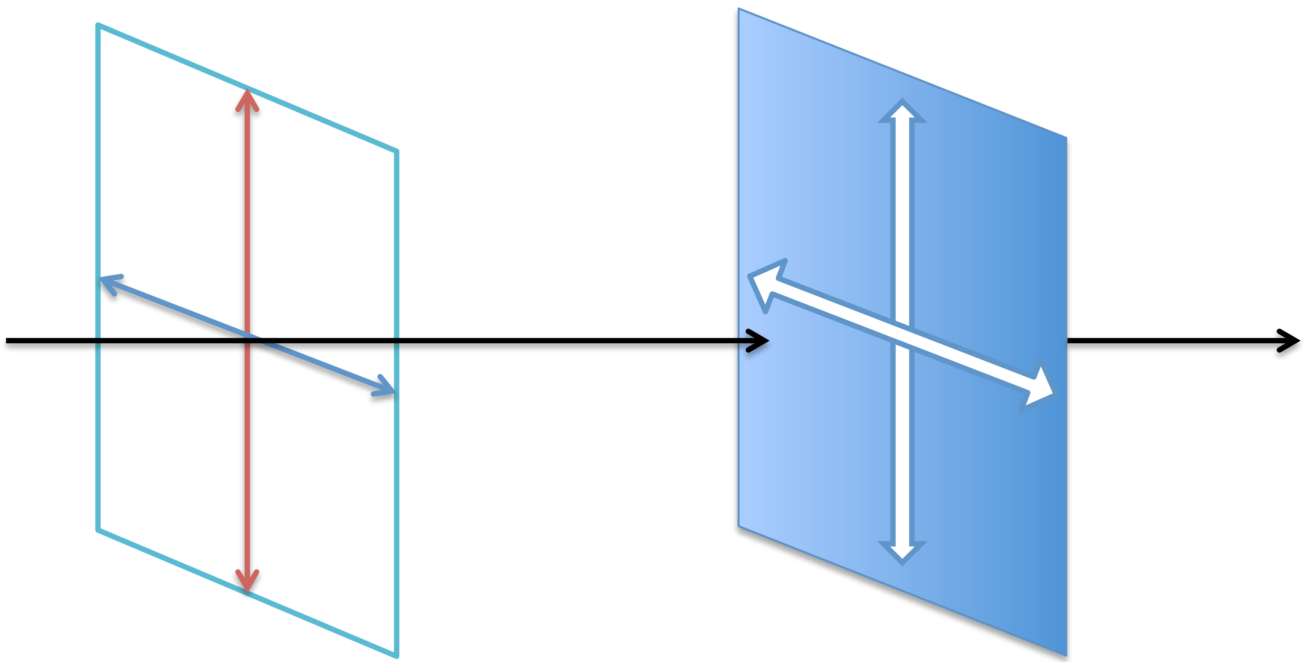
The photon Alice sends out can be in either four states



Bob randomly choose a basis to measure the photon



If Bob chooses the same basis as Alice

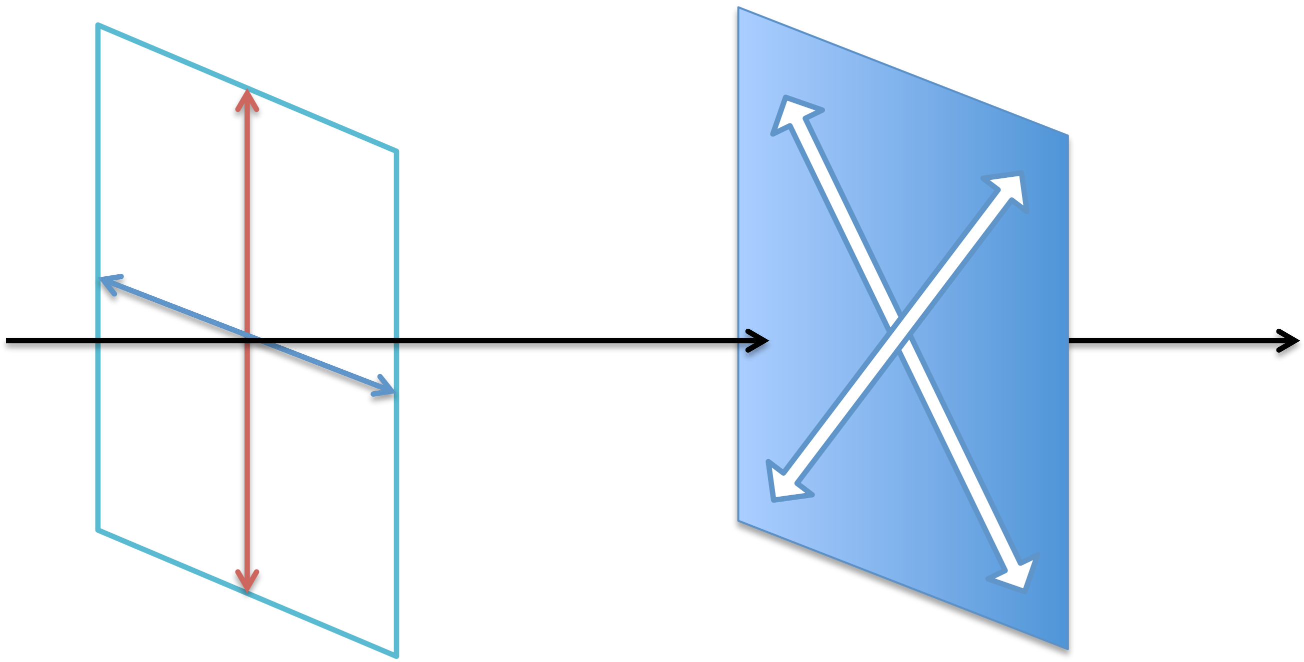


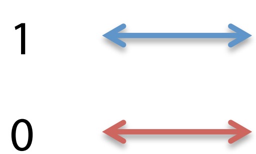
1

0

a correct measure can be got

If Bob chooses the wrong basis





the measure result will have
50% chance to be correct

Over all, Bob got a “raw key” with 25% error rate

… without considering noise and man-in-the-middle attack,

and is too high for traditional error correction coding.

A classical channel is needed for coordinating the quantum communication

to transfer signals, like start, stop, sending a bit, etc., and it has to be authentic.

QBER: Quantum Bit Error Rate

is the error rate of the sifted key

different from BER, which is the error rate of an optical communication channel

can be caused by noise or eavesdropping in the quantum channel,

or imperfection of sending and receiving devices

A straightforward error correction scheme: basis reconciliation

Bob asks Alice whether the basis he used was correct or not

through an unencrypted public classical channel

Bits detected by using a wrong basis are discarded

The result is a more correct "sifted key"

can't be 100% correct due to either noise or man-in-the-middle

Now, introducing the attacker Eve

Eve’s possible attacks

1. Cloning the photon
2. Intercept-resend
3. Intercept the public classical channel
4. Spoofing attack through the public channel

1. Perfect cloning a photon is impossible

Observing a photon irreversibly collapses it and corrupts the information it carries

because a measurement takes energy away from the photon

Mathematically proofed

Wootters-Zurek theorem

Note the “perfect” here, non-perfect cloning is possible

through a process called weak measure

2. Intercept-resend

Eve intercepts the photon, measures it in a random basis, and resent a new photon to Bob

Eve has a 50% chance to steal a bit correctly

in which cases Bob and Alice won't be able to notice

In other cases, Eve guessed the wrong bases and introduces more errors into the quantum channel

thus higher than noise level errors in a channel may indicate a man-in-the-middle attack

3. Intercept the public classical channel
4. Spoofing attack through the public channel

Alice and Bob only exchanges bases information

thus Eve can't get the key directly

After a key has been exchanged, all following communication in the classical channel can be encrypted

However, authentication remains a big issue

Error correction

Error rate in the sifted key can be detected by comparing part of the key through the classical channel

those bits will be discarded

A simple error correction method: Alice randomly chooses pairs of bits and announces their XOR value. Bob replies either "accept" or "reject." They keep the first bit in the first case and discard the two bits in the second case.

How do they know when to stop this process?

Use privacy amplification to reduce the information Eve may possess

Alice announces two random locations, Alice and Bob then replace these two bits by their XOR value

shrinks the key, also the bits Eve may possess

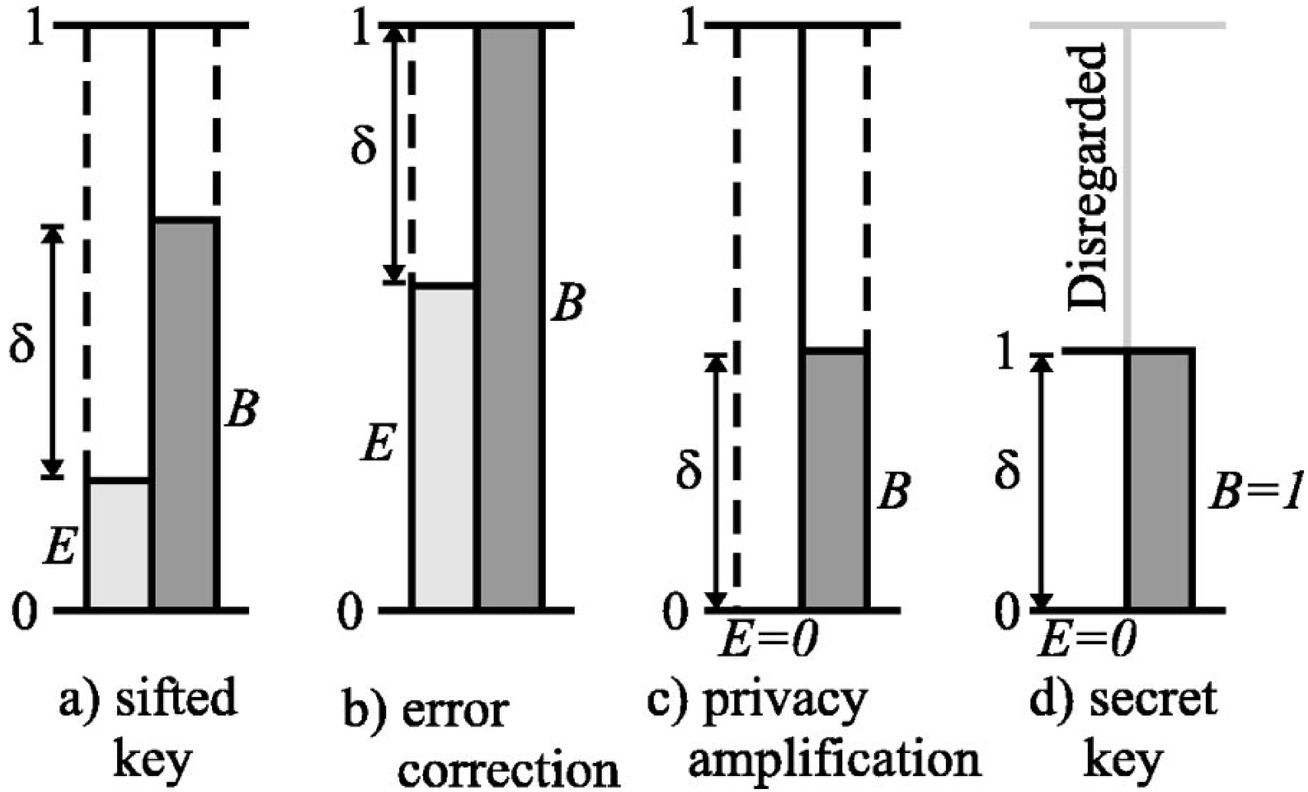
Bob must be possessing more information then Eve does for this algorithm to be useful

Quantum secret growing

Alice and Bob needs to share a (short) secret beforehand for authentication

They can use quantum key exchange to get a longer key, thus "secret growing"

Intuitive illustration of error correction and privacy amplification



Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. 2002

Other weaknesses

Relies on the quality of the random number generators

Relies on the authentication of the classical channel

Recently progress in weak measurement makes directly measuring a photon more efficient

thus Eve may intercept more information without disturbing the photon stream

BB84 Protocol summary

Cool on paper

Somehow succeeded in experiments

Some products are available

Has many shortcomings

needs an authentic classical channel's help

Can be a complement to standard symmetrical cryptosystems

Other protocols

Two-state protocol

Two nonorthogonal states are necessary and enough

But not good in practice

Six-state protocol

Uses three different bases

Simplifies security analysis

Reduces Eve's optimal information gain for a given error rate

The EPR protocol

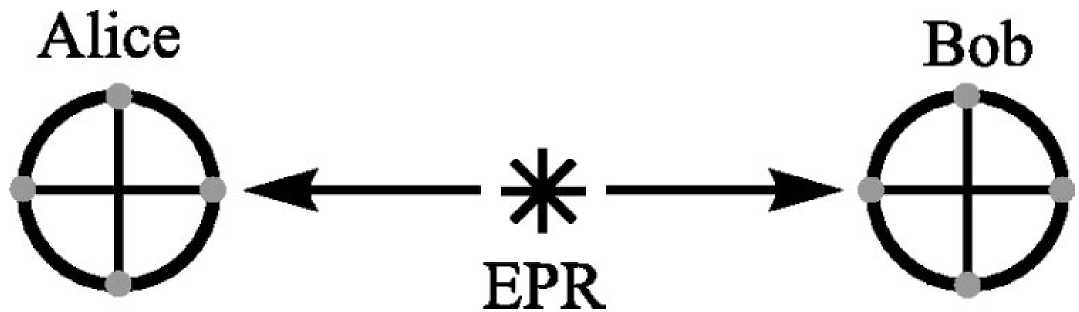


FIG. 3. Einstein-Podolsky-Rosen (EPR) protocol, with the source and a Poincaré representation of the four possible states measured independently by Alice and Bob.

Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. 2002

Quantum teleportation as a “quantum one-time pad”

Qubit

A two-state quantum system, such as the polarization of a photon. It can be in a superposition of both states at the same time.

It can be described in the bra-ket notion:

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

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

Quantum entanglement

Two qubits can be entangled by some physical interact

Two qubits can be spatially separately

Measuring one qubit yields completely random result

But measuring the other bit subsequently yields the same result

Quantum teleportation

Can be used to “teleport” a quantum system

by duplicating its state remotely onto another quantum system

Can be used to duplicate a quantum state

can duplicate the quantum state matrix

Is not cloning

the original quantum system will be destroyed

Quantum teleportation as a secret channel

A number of entangled qubits were distributed to two sides that need to communicate beforehand

Alice is sending *c* to Bob

Alice measures her qubit and gets an *a*, sends *a* XOR *c* to Bob via a public channel

Bob measures his qubit and gets *b*, then *a* XOR *c* XOR *b* generates *c*

Quantum teleportation as a secret channel

Proofed secure

bits in the public channel is like being encrypted by using a one-time pad

Requires pre-deliver a large amount of entangled qubits

Relies on a classical channel too

Technological challenges

Optical amplification

Due to non-clone theory, perfect amplification is not possible

Theoretically, cloning a photon can get at most 5/6 in fidelity

Quantum nondemolition measurements

is a measure that doesn't destroy the photon

possible on orthogonal states when you know the state beforehand

by making the state an eigenstate, however, you can't gain extra information from this process

But it is possible to detect a photon without disturbing it (much)

will increase noise in the system

Transmission media

	Fiber	Free space
Noise level	0.2 ~ 0.35 dB/km	higher
Wavelength	1300 ~ 1550 nm	800 nm
Speed	< 1 M	?
Distance	tens of km	1~2 km
Cost	High	Low

Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. 2002

Photons sources

Faint laser pulses

Photon pairs

Experimental QC with Faint Laser Pulses

General ideas

All implementations rely on photons

QBER increases as distances increases

current technology put the limit at 100 km

Different codings

Polarizing coding: 10 km, high QBER since preserving polarization in fibers is hard

Phase coding: lots of research and experiments, requires phase sync., not a single photon system, lower QBER (~ 1.4%)

Frequency coding: easier to implement than phase coding, but has higher error rate

Free-space line-of-sight applications

By 2000, key exchange over 1.6 km (daylight) and 1.9 km (nighttime) was achieved

Can be used with low-orbit satellites (300 – 1200 km)

Experimental QC with Entangled Photon Pairs

Advantages of photon pairs

Better detection rate

single photon detectors have high dark-count probability

Better against eavesdropping

QC using photon pairs

Polarization entanglement

Energy-time entanglement

Phase coding, phase-time coding

Quantum secret sharing

Alice sends a split secret to Bob and Charlie

Either Bob or Charlie alone doesn’t have any information of the key

Bob and Charlie can work together to get the key

Eavesdropping

An Eve only limited by quantum physics

has unlimited resources

has access to future technologies

Difficulties against an “omnipotent” Eve

Eve can hide in noise

Eve can replace the quantum channel with better instruments of lower noise level

this can make discovering Eve very difficult

Eve also possesses all traditional methods of attacking

like attacking the RNG, tapping or spoofing the traditional channel, or even accessing the local storage of Alice or Bob

Supply chain woes

Eve can be the device suppliers

Or bug the devices while they are in transit

Testing quantum equipment is very hard

Three classes of attacks

Individual attack

Eve attaches one probe to a qubit a time, and measures one a time

Joint attack

Eve processes several qubits collectively

Collective attack

Attach one probe to a qubit a time, but measures several probes coherently

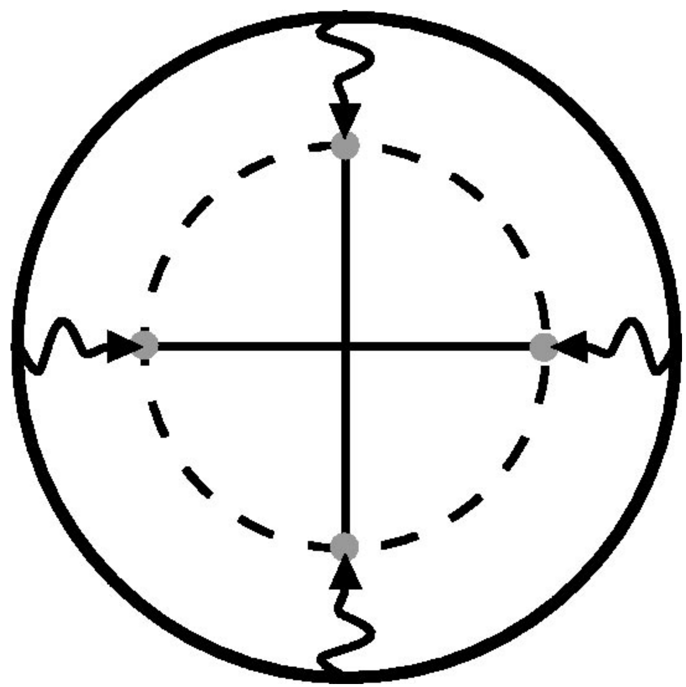
Simple individual attacks

Eve gets 0.5 bits of information per bit in the sifted key

Induced QBER of 25%

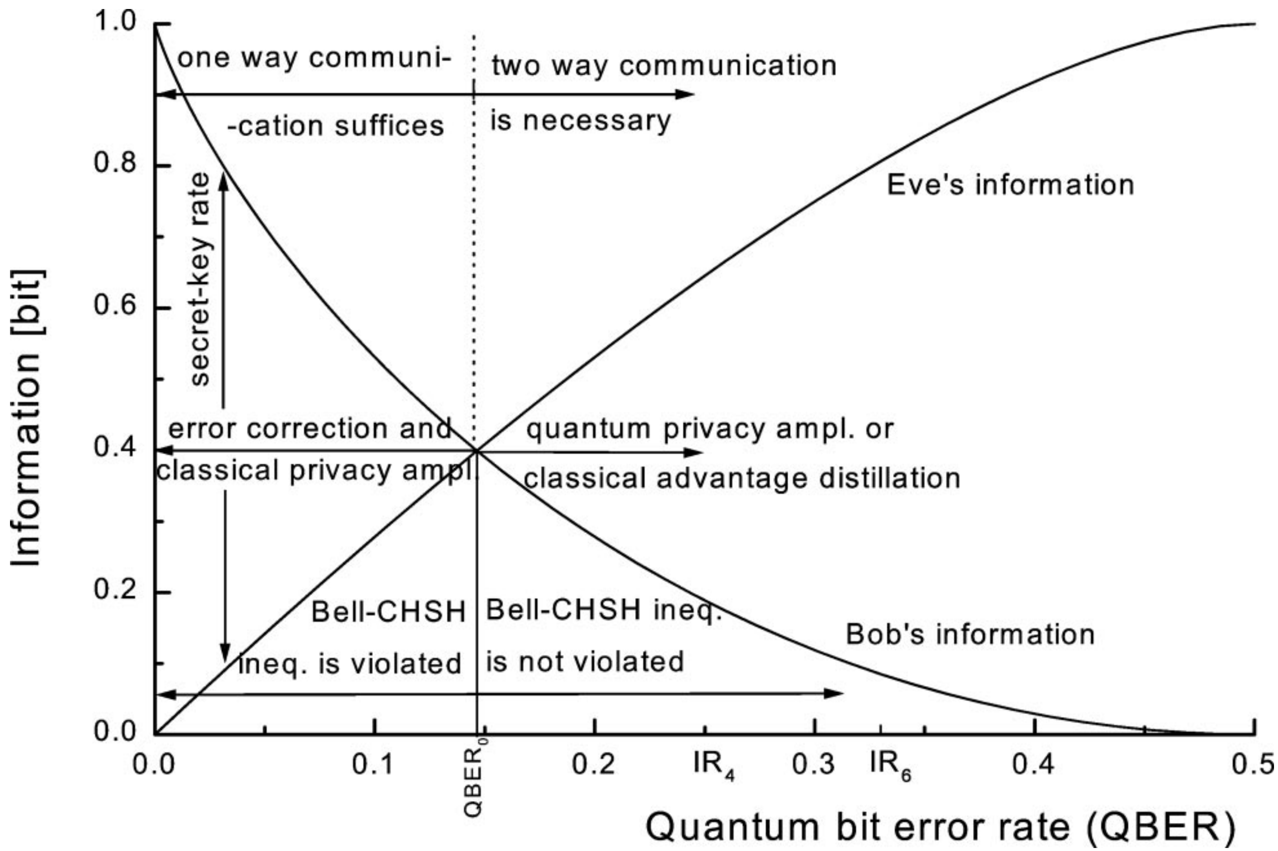
Symmetric individual attacks

Eve probes a qubit, changing the possibility of each four states equally, thus called “symmetric-attack.”



Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. 2002

Eve's info vs Bob's info



Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. 2002

Quantum nondemolition measurement attack

Taking advantage if Alice sends more than one photons with the same information

due to imperfection in devices

But considered impractical

Trojan horse attacks

Eve sends pulses to Alice and Bob to understand their devices' status

May be thwarted technically

Illustrated that analyzing a QC system requires both physical and technical measures

Conclusion of QC

Has some unique and interesting features

Is the cross of quantum mechanics and information theory

Has lots of technological limitations

Is developing rapidly

Some products are on market

Can't significantly improve communication security (yet)

The End

Questions & discussion?