ALL ABOUT EVE

Secret Sharing Using Quantum Effects

Dr. Deborah J. Jackson

Jet Propulsion Laboratory

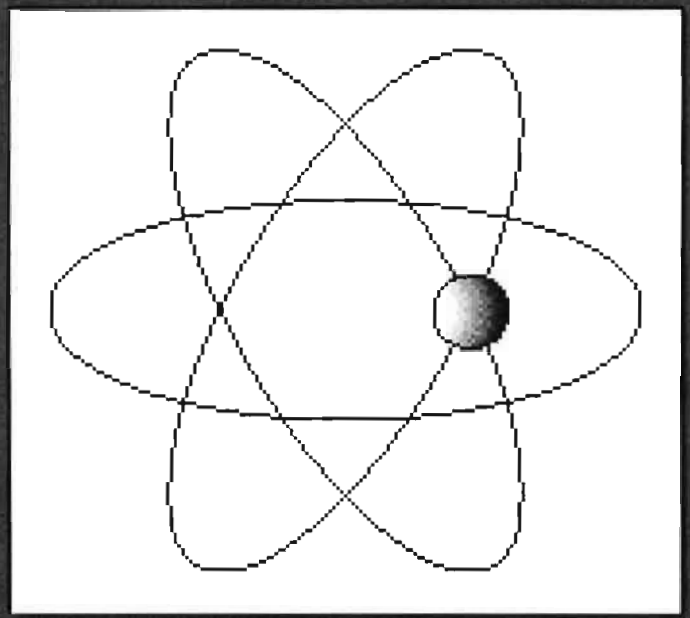
California Institute of Technology

National Science Teachers Association

Shell Lecture

April 2, 2005

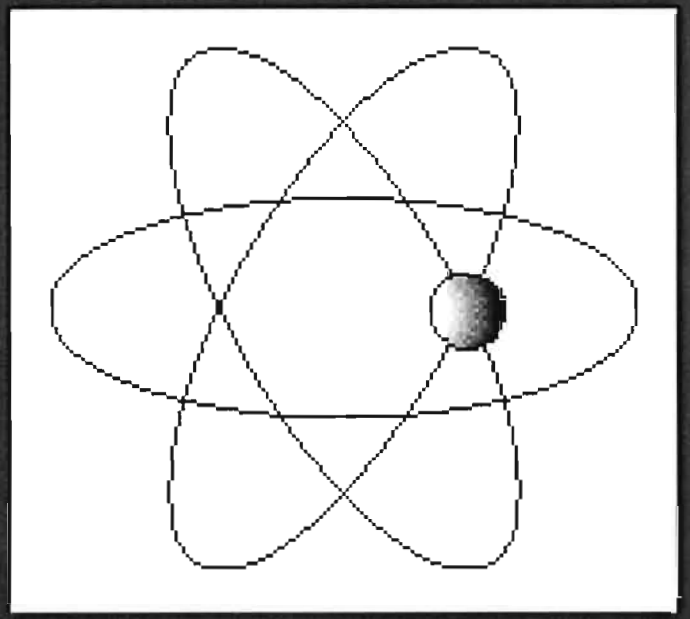
Teaching Old Atoms New Tricks



What does this have to do with Eve?

Teaching Old ~~Atoms~~ New Tricks

Adam



Outline

Buzz Words

- What is the nature of Light?
  - What is classical light?
  - What is a photon? (aka Quantum information)
- Encryption
- Alice's problem (Hint: Evil Eve)
- Quantum Key Distribution (QKD)
- Advanced QKD

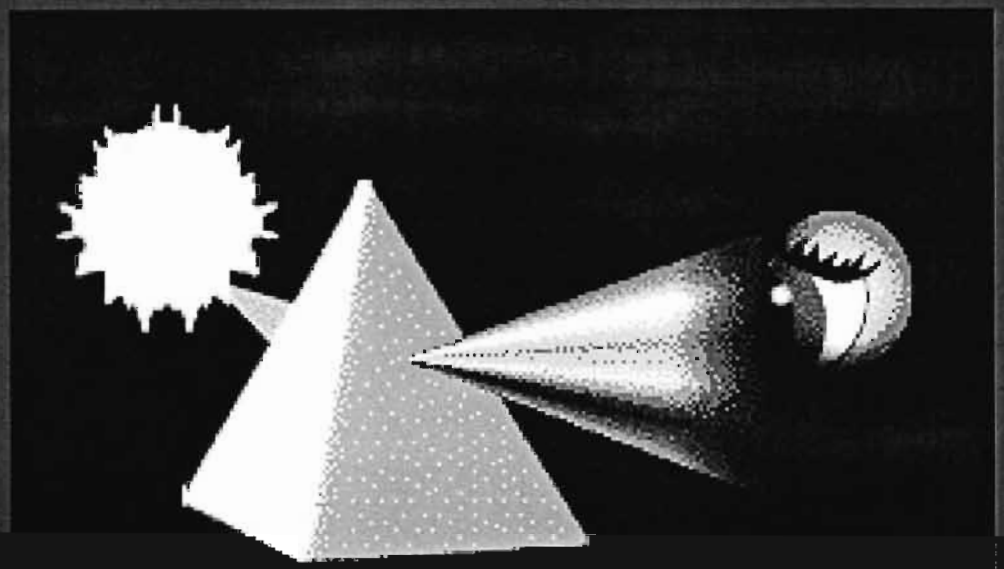
Buzz Words

- Polarization of light
- Beamsplitter
- Photon
- No cloning theorem
- Encryption vs Quantum Key Distribution

Outline

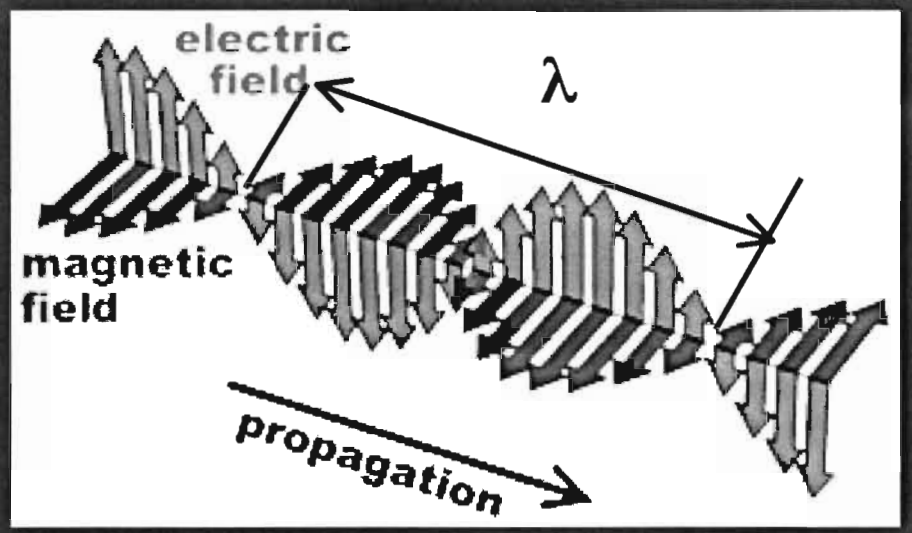
- Buzz Words
- ★ What is the nature of Light?
  - What is classical light?
  - What is a photon? (aka Quantum information)
- Encryption
- Alice's problem (Hint: Evil Eve)
- Quantum Key Distribution (QKD)
- Advanced QKD

Classical light

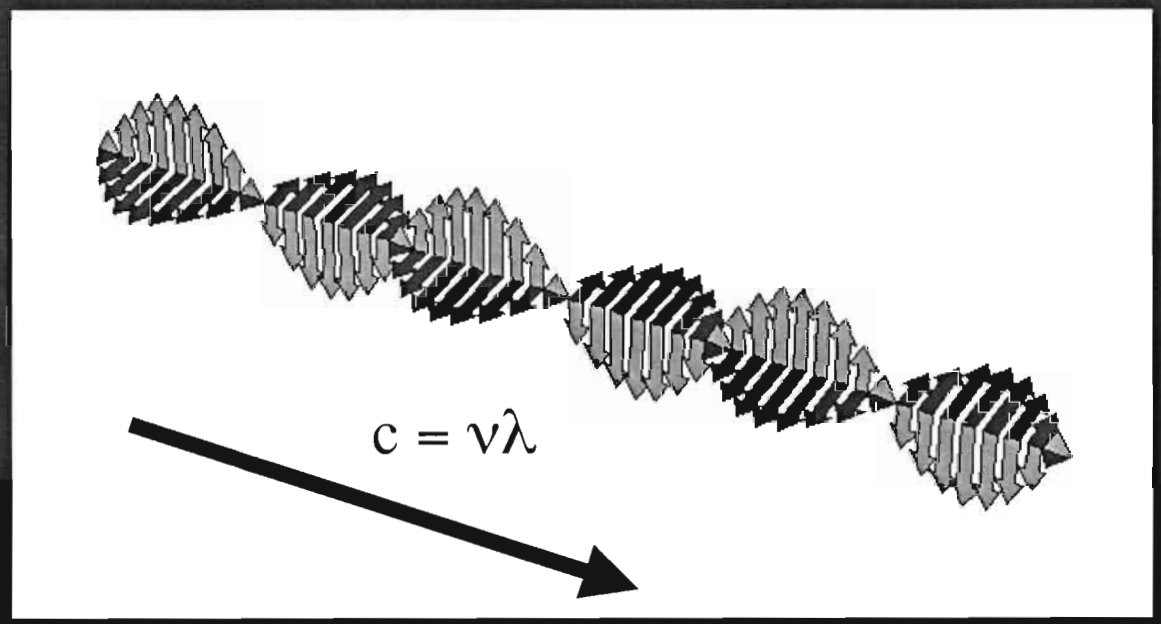


Something that makes vision possible; the stimulation aroused by visual receptors; electromagnetic radiation in the wavelength range including infrared, visible, ultraviolet, x-rays and traveling in vacuum at the speed of light.

Electro-Magnetic wave

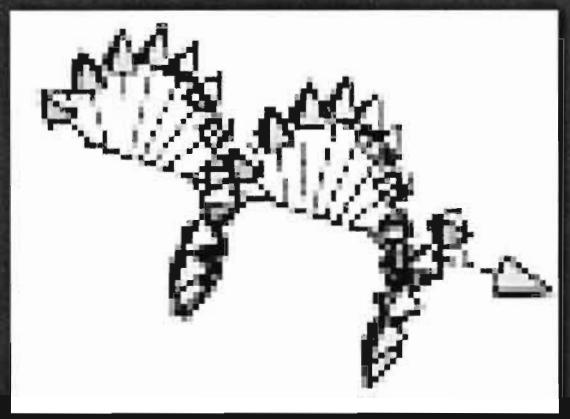


Linearly Polarized Electro-Magnetic Wave



Circular Polarization

s = -1



s = +1

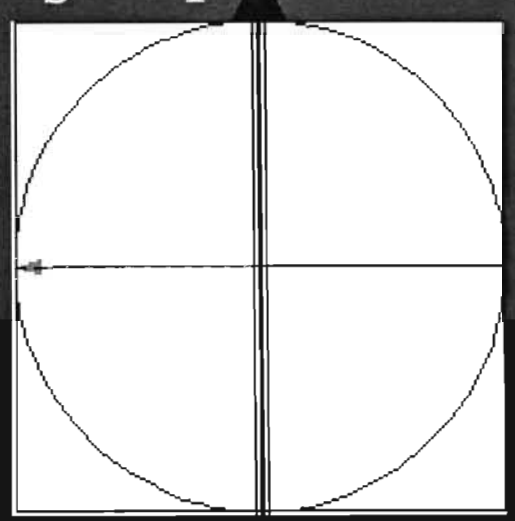
Right-hand circularly polarized

Left-hand circularly polarized

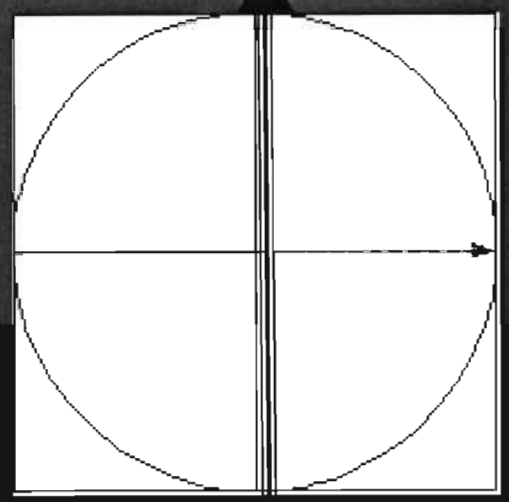
Polarization analyzer

The action or process of affecting radiation, especially light so that the vibrations assume a definite form.

s = -1



s = +1

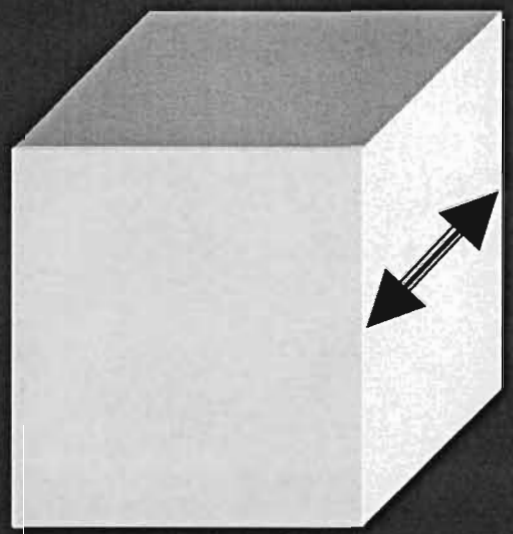


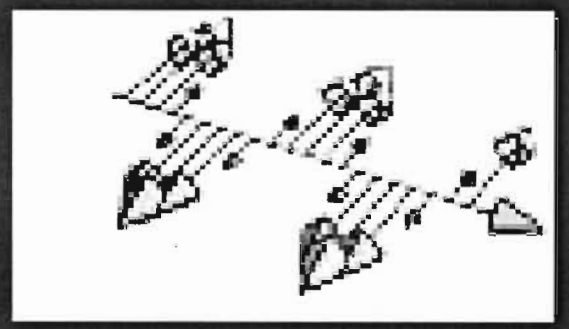
Right-hand circularly polarized

Left-hand circularly polarized

Preparation of Linearly Polarized Light

s = -1



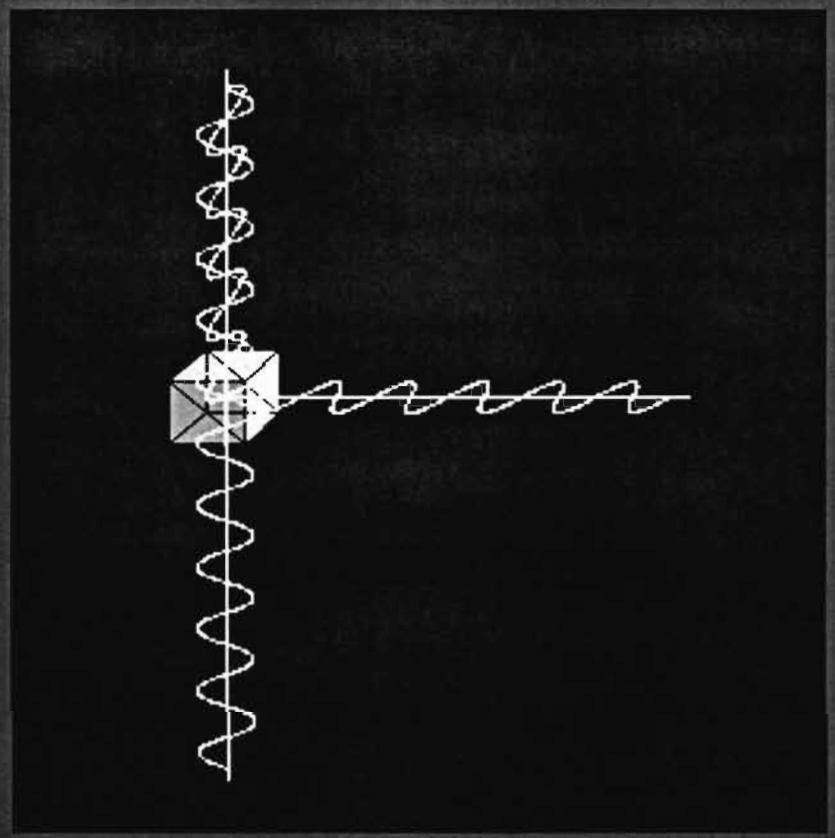


Right-hand circularly polarized

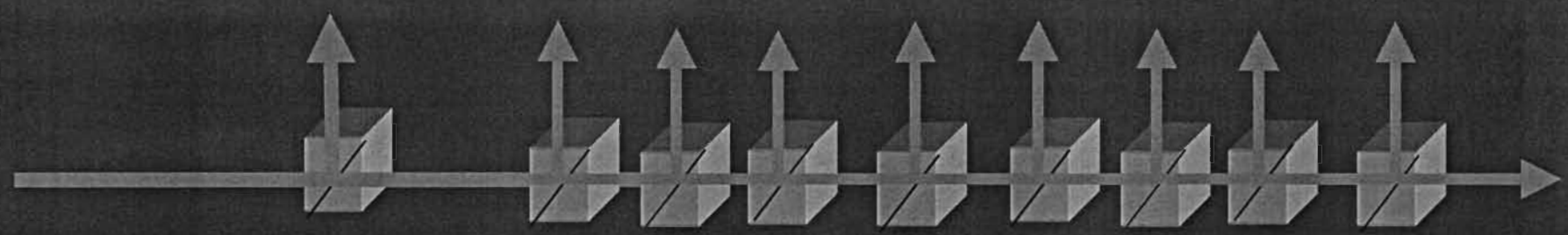
Polarization Analyzer

Linearly polarized

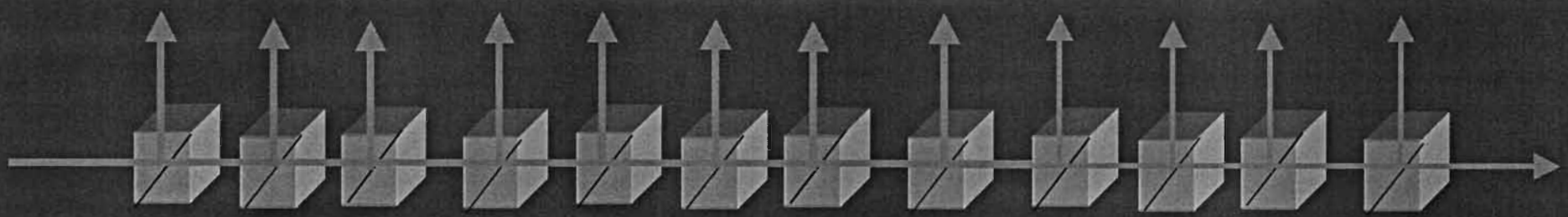
Beam Splitter



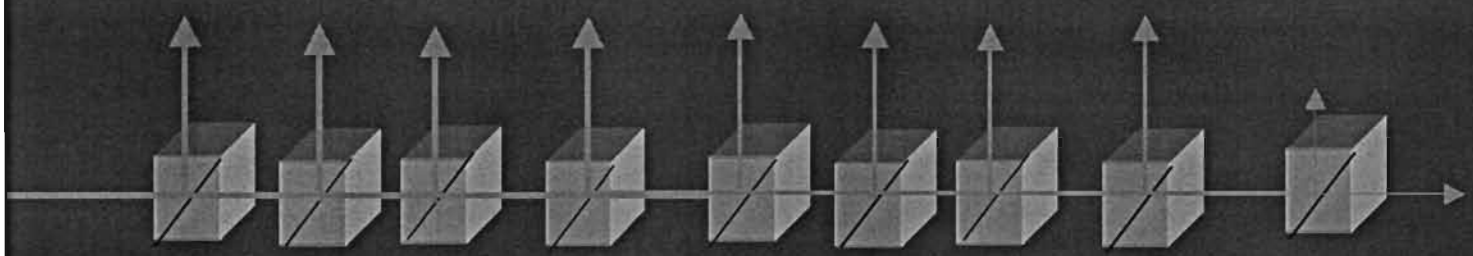
Binary division



Binary Division

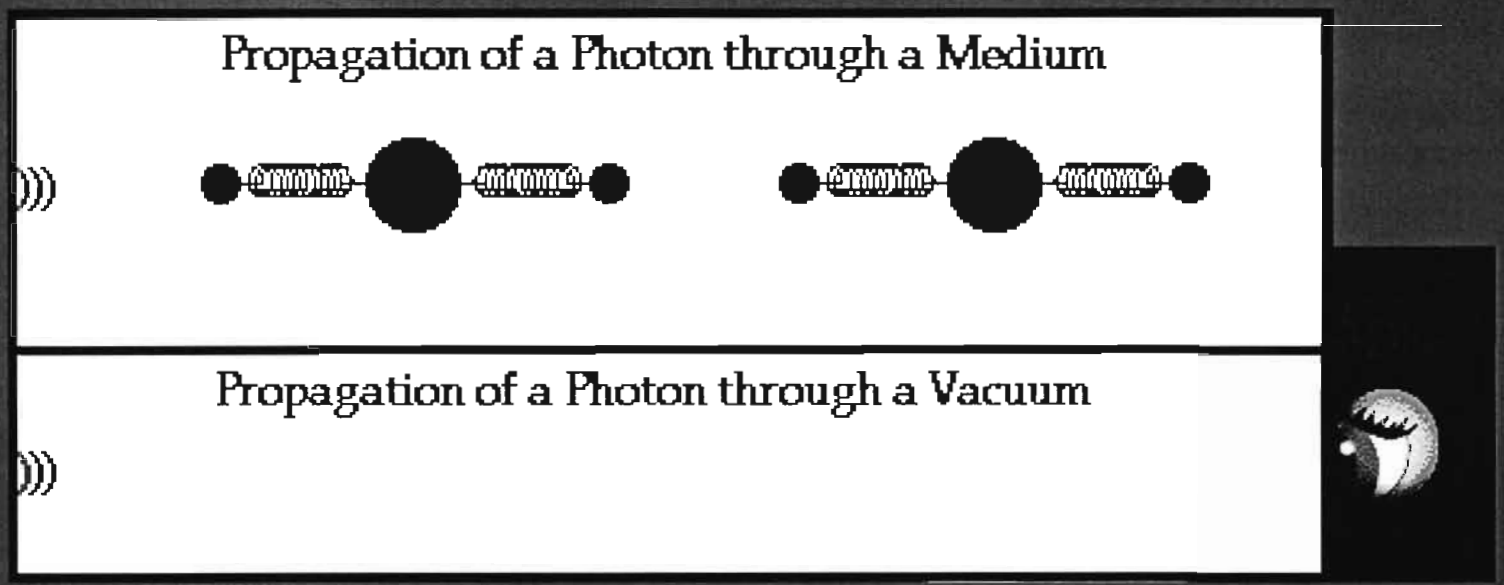


Binary Division



A quantum; the smallest possible subdivision of radiant energy defined as a PHOTON

Single-Photon Propagation



A single-photon

- Is described in terms of a single color/wavelength
- Still interacts with a medium like a beam of light
- Still propagates through vacuum at speed of light
- Unable to see with naked eye

What other properties of light change for single-photons?

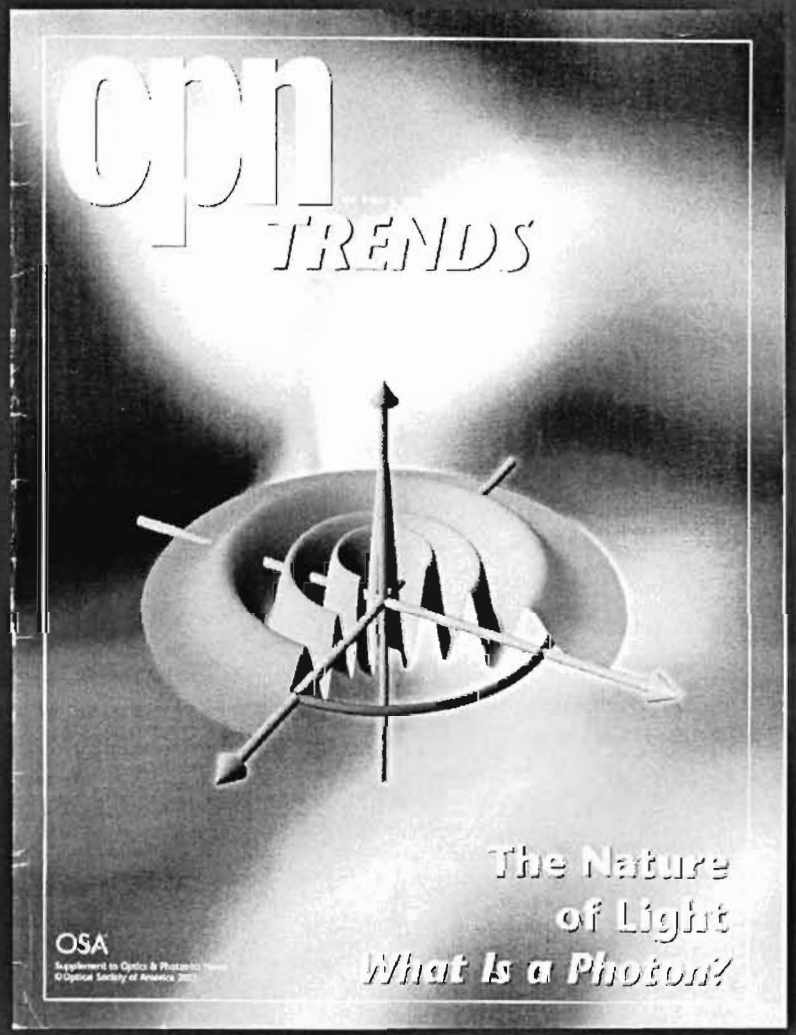
Unique quantum phenomena exploited in quantum information theory

- Interference (also classically observed)
- Superposition
- Entanglement
- Non-determinism
- ✓ Non-clonability

Unknown quantum states cannot be copied exactly.

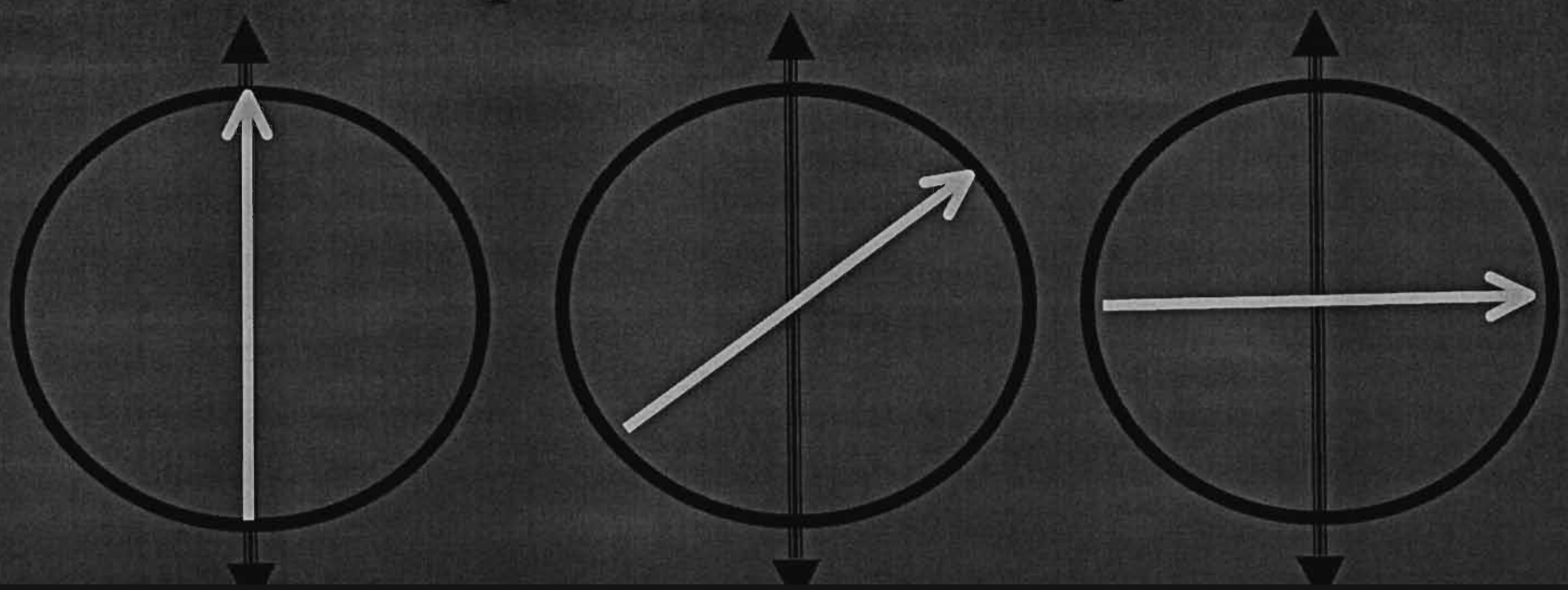
Optics Photonics News

Special Issue - October 2003



The more we know about light, the more we don't' know.

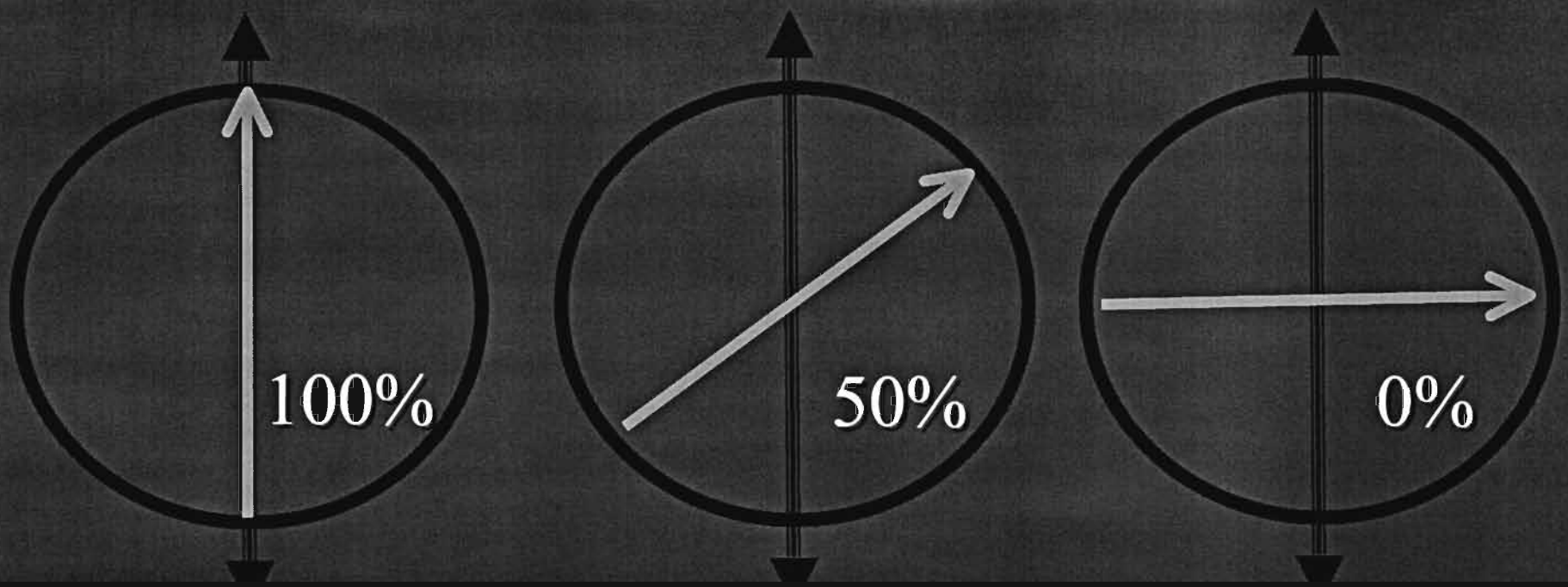
What happens when single photon encounters polarization analyzer?



Analyzer

Polarization orientation

Throughput described in terms of probabilities



Analyzer

Polarization orientation

Outline

- Buzz Words
- What is the nature of Light?
  - What is classical light?
  - What is a photon? (aka Quantum information)
- ★ Encryption
- Alice's problem (Hint: Evil Eve)
- Quantum Key Distribution (QKD)
- Advanced QKD

Example Crypto Code: CAESAR CIPHER (-1)

ABCDEFGHIJKLMN

ZABCDEFGHIJKLM

OPQRSTUVWXYZ

NOPQRSTUVWXY

IBM => HAL

Example Crypto Code:

CAESAR CIPHER (random)

+4 +2 −1

ABCDEFGHIJKLMN

ABCDEFGHIJKLMN

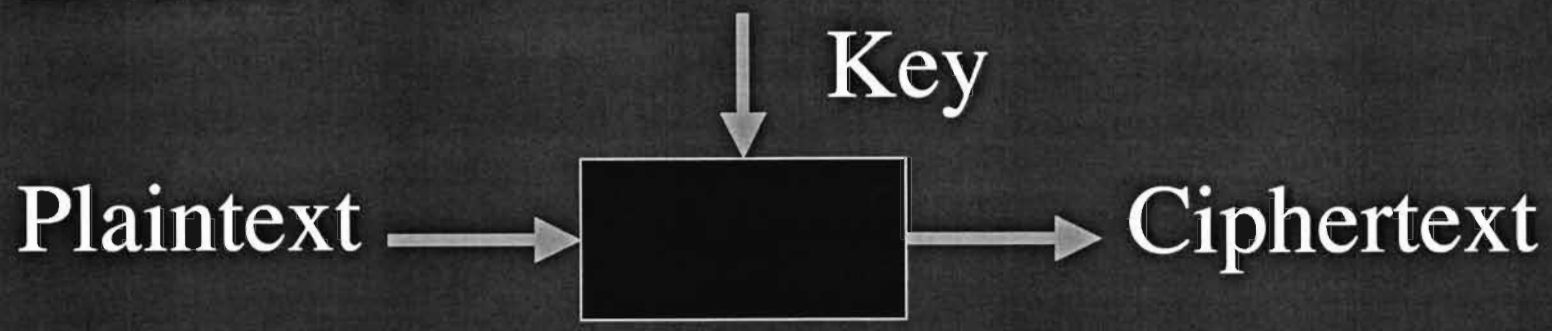
OPQRSTUVWXYZ

OPQRSTUVWXYZ

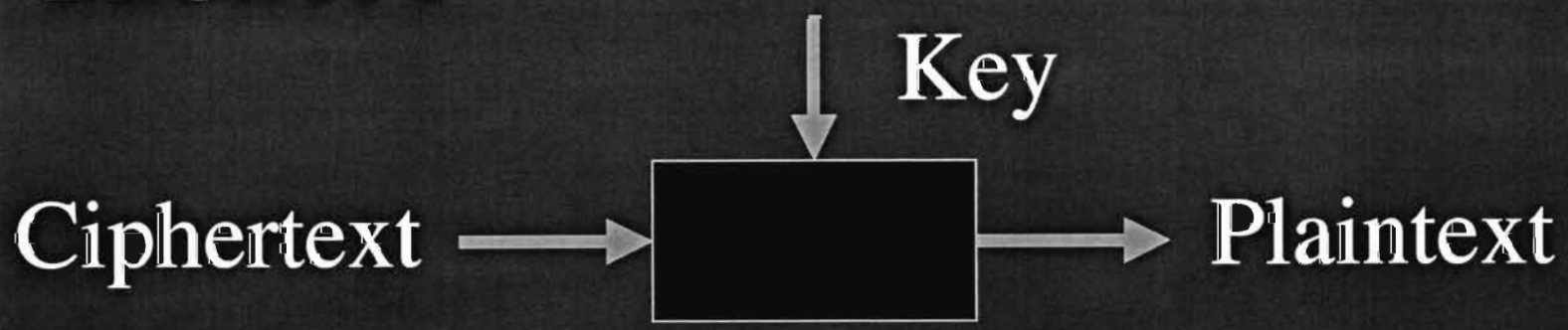
IBM => KFL

Symmetric Crypto Codes

ENCRYPT

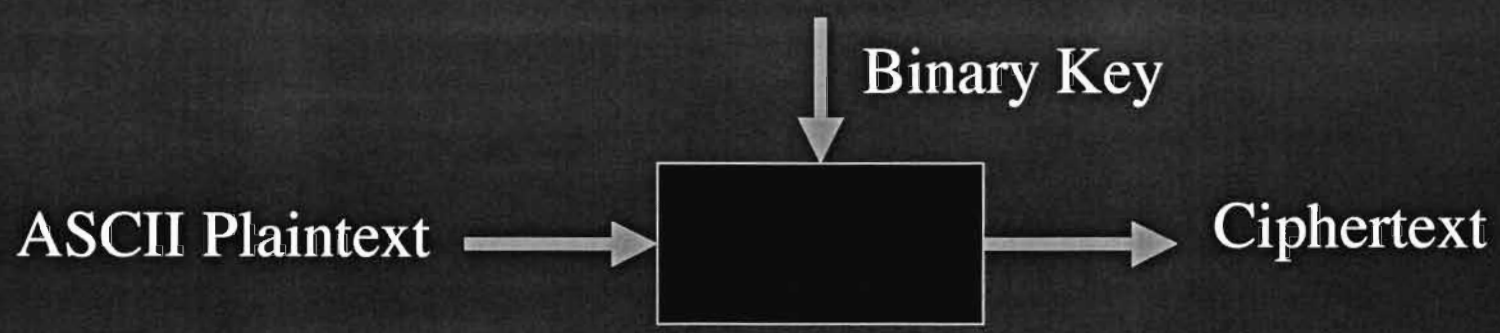


DECRYPT



Drivers for QKD Implementation

- Key exchange weakest part of crypto procedure
- All computerized information is converted to binary symbols in the form of ASCII text.
- Key generation can be a matter of simply generating a random sequence of "1"s and "0"s.



XOR Function

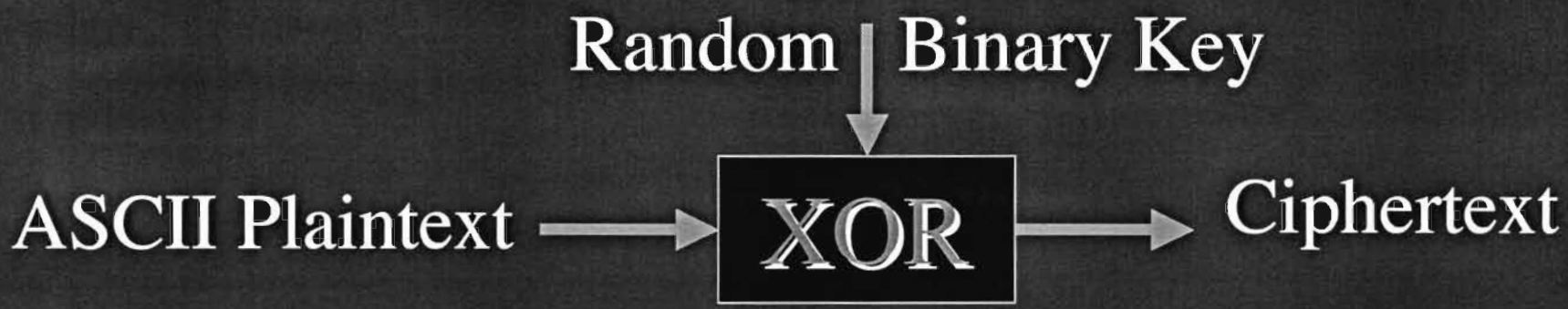
A	B	Output
0	0	0
0	1	1
1	0	1
1	1	0

XOR Property:

If $A \oplus B = C$, *then* ← ENCRYPT

$C \oplus A = B$, *and* $B \oplus C = A$ ← DECRYPT

Vernam Cipher



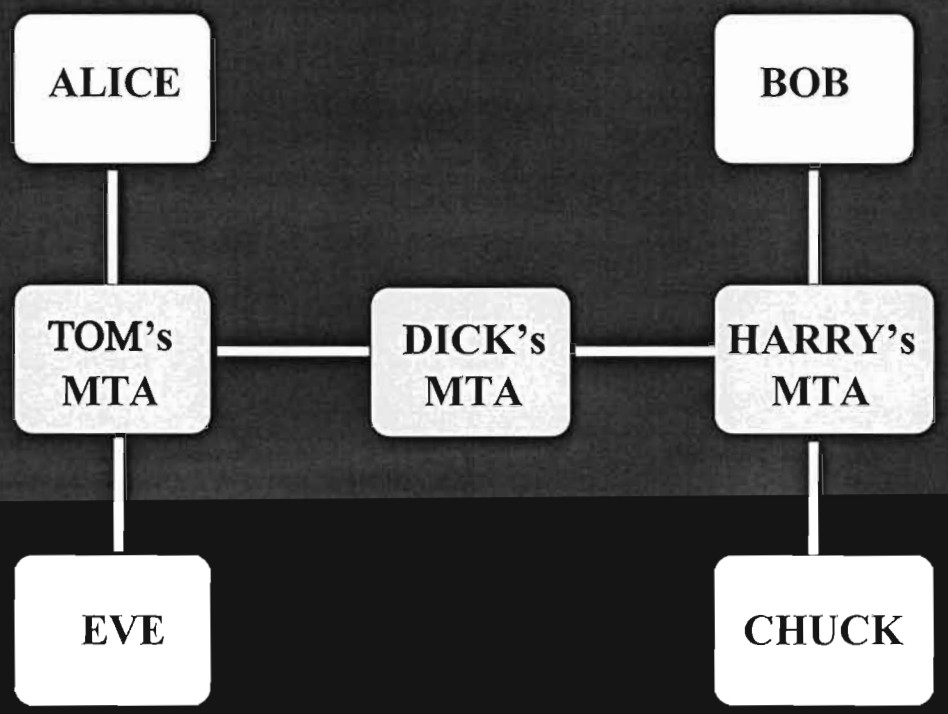
QKD + Vernam Cipher

- "One Time Pad"
- Analytically proven to be unconditionally secure

Outline

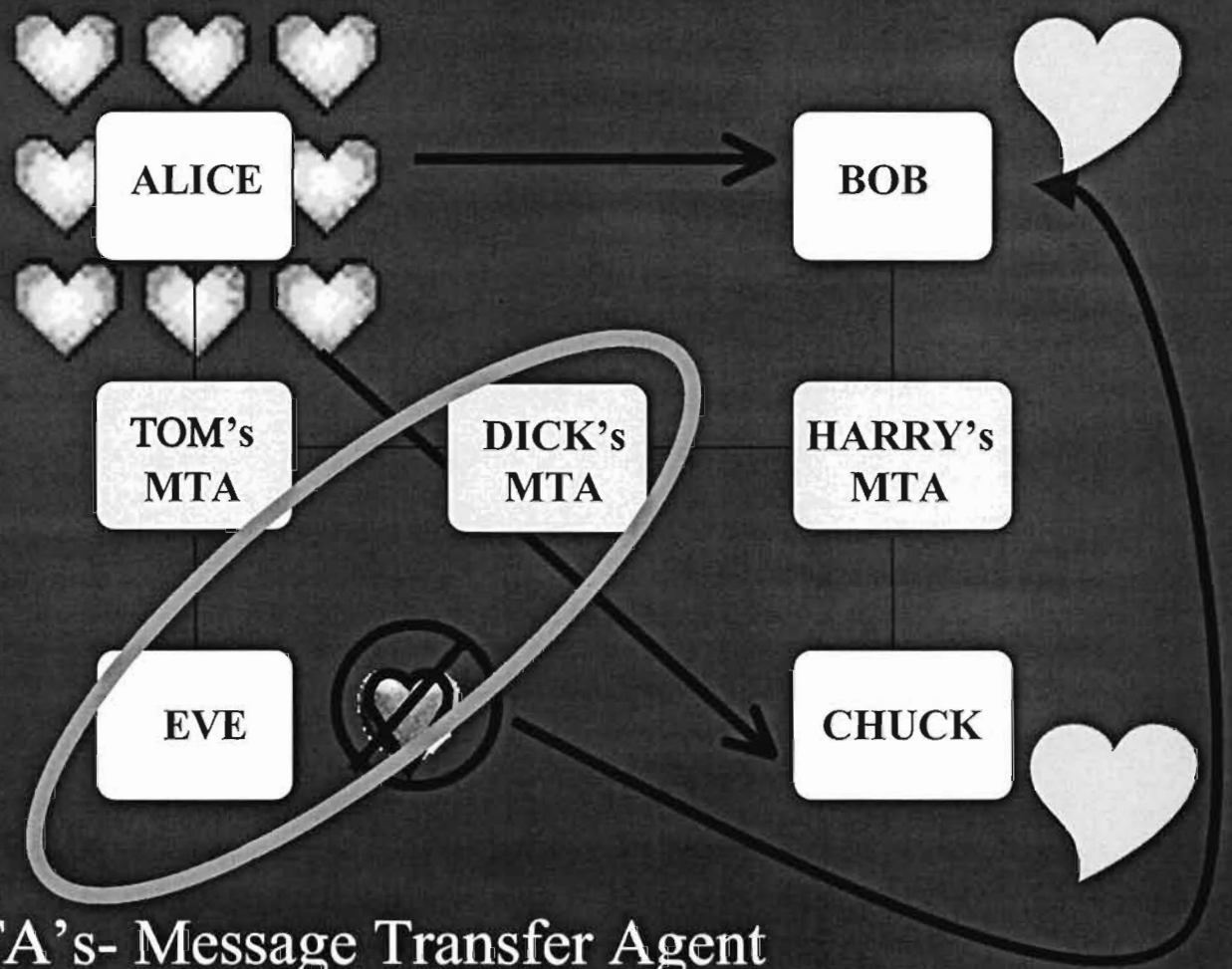
- Buzz Words
- What is the nature of Light?
  - What is classical light?
  - What is a photon? (aka Quantum information)
- Encryption
- ★ Alice's problem (Hint: Evil Eve)
- Quantum Key Distribution (QKD)
- Advanced QKD

WORLD ACCORDING TO ALICE



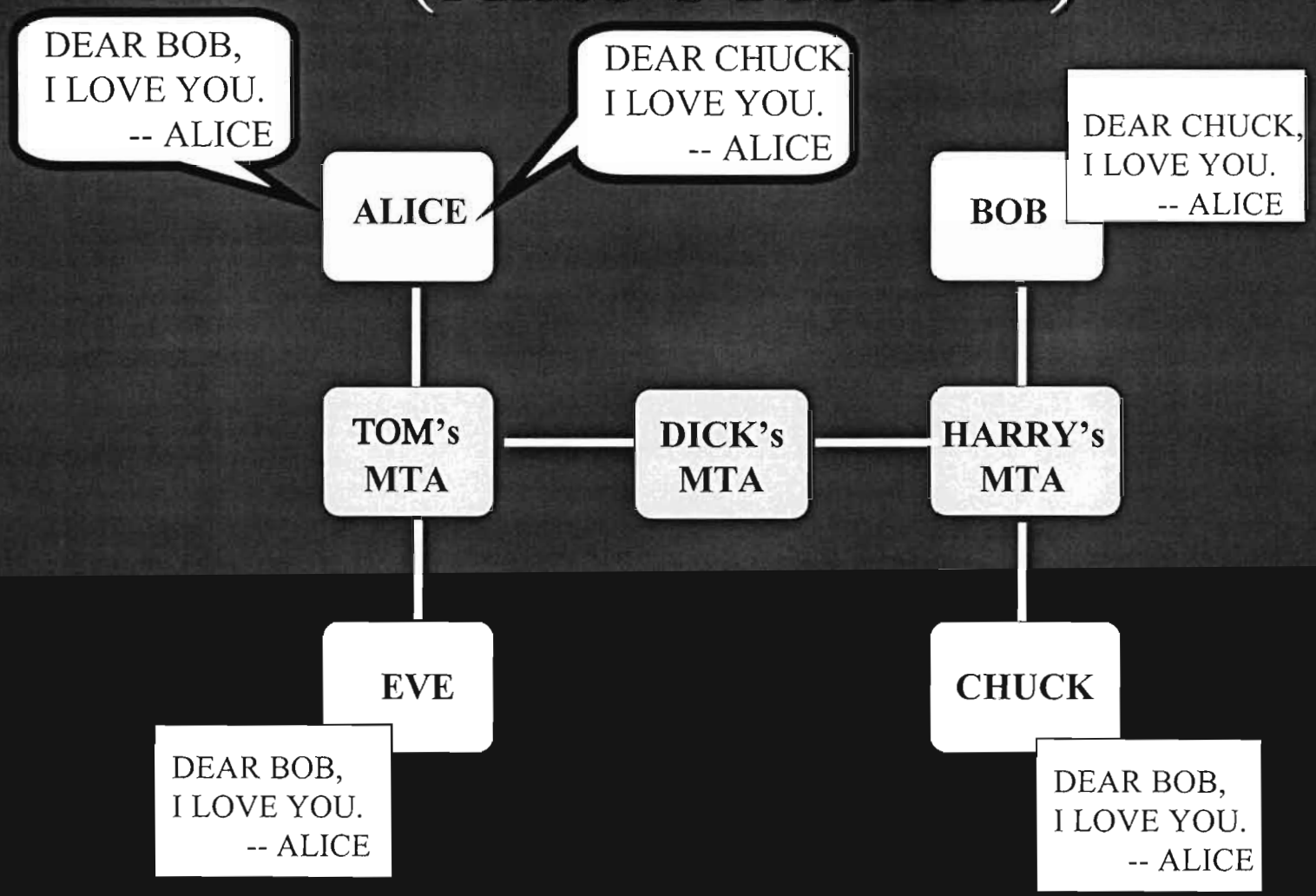
MTA's- Message Transfer Agent

ALICE'S PROBLEM



MTA's- Message Transfer Agent

CONFIDENTIALITY
(Alice's Problem)



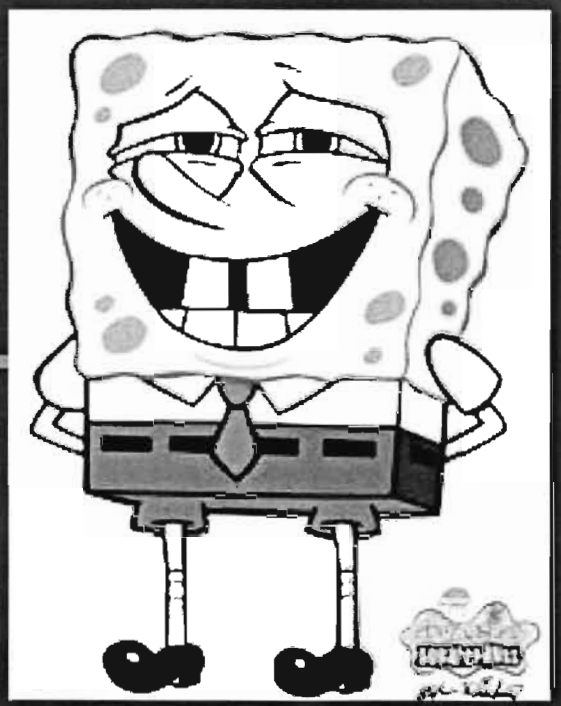
MTA's- Message Transfer Agent

Outline

- Buzz Words
- What is the nature of Light?
  - What is classical light?
  - What is a photon? (aka Quantum information)
- Encryption
- Alice's problem (Hint: Evil Eve)
- ★ Quantum Key Distribution (QKD)
- Advanced QKD

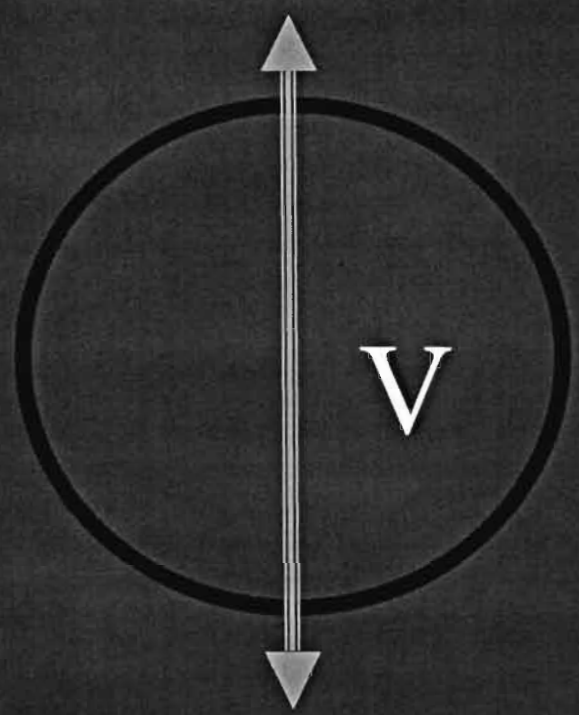
QKD Key Generation Sequence

Key Generation
Link

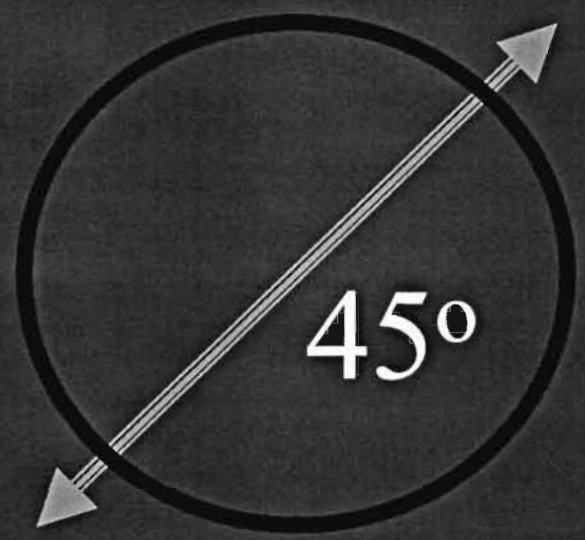


Take advantage of non-cloning theorem
=> Unknown quantum states cannot be copied exactly.

Alice's Base-2 Encoding

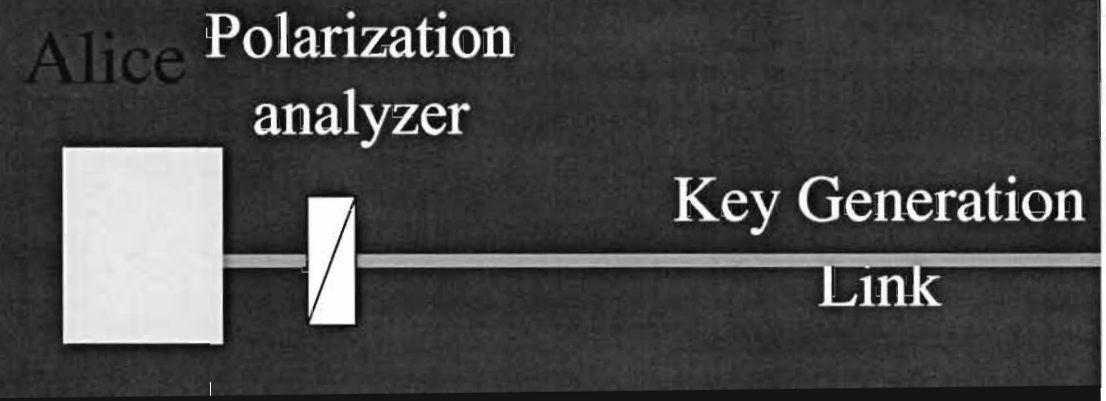


"0"

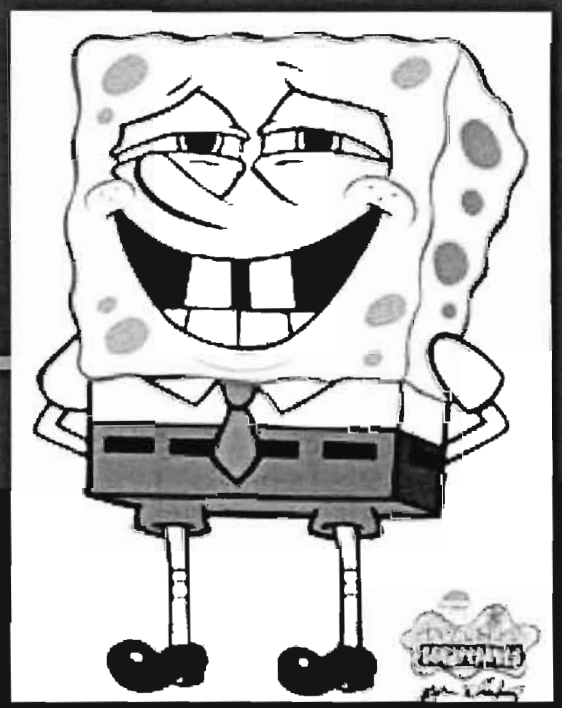


"1"

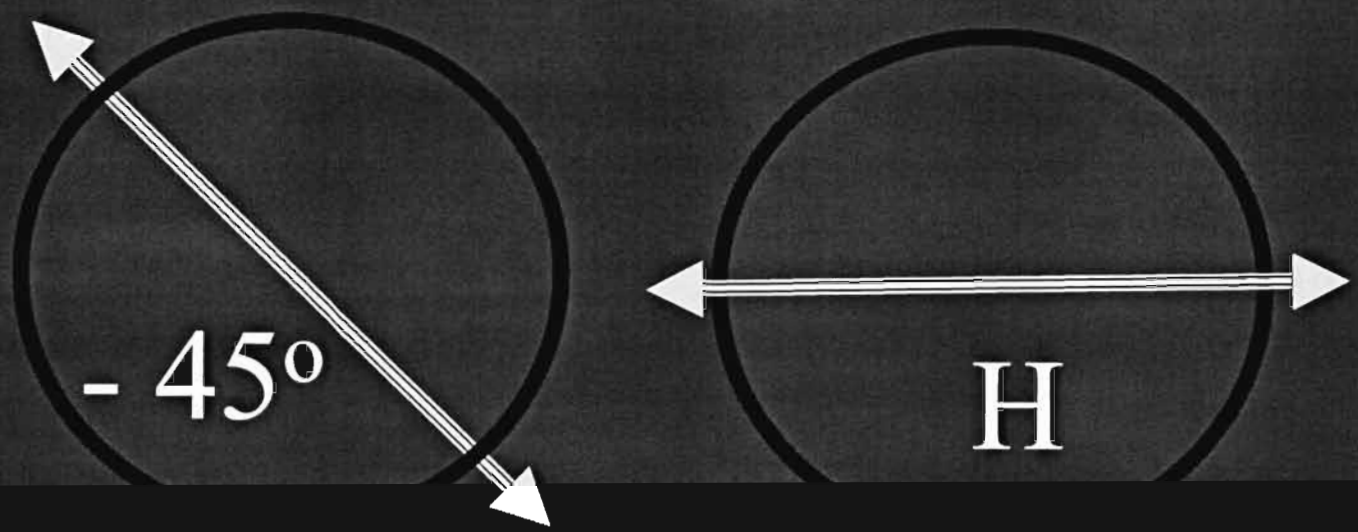
QKD Key Generation Sequence



SOURCE

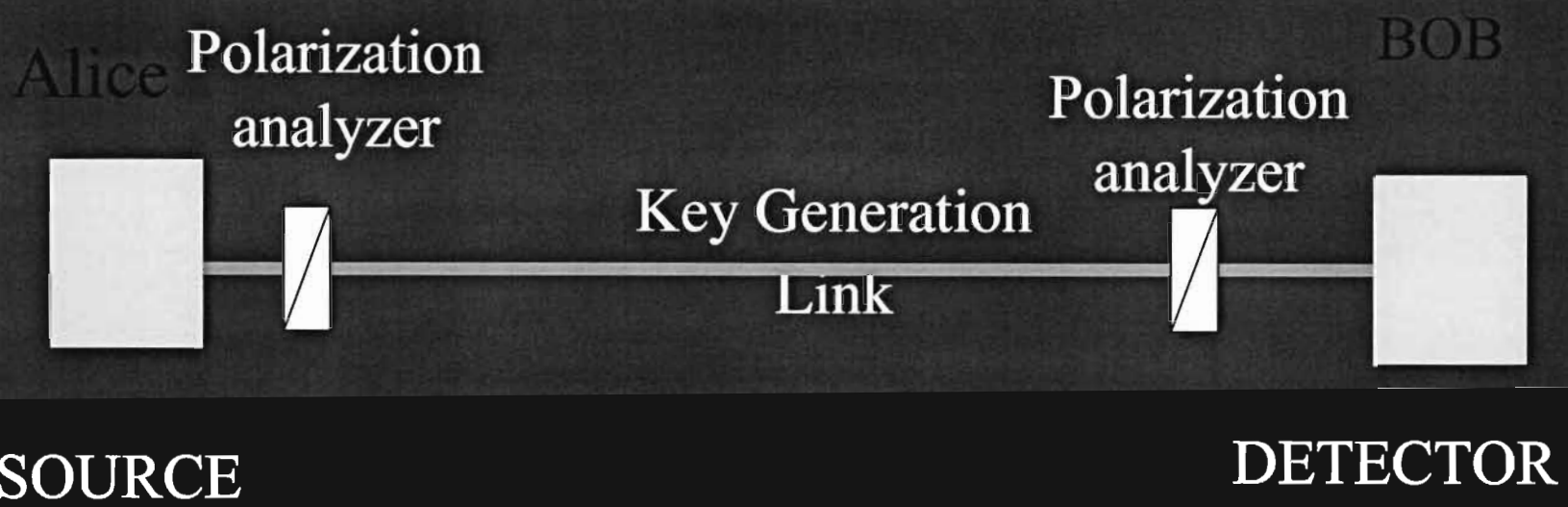


Bob's Base-2 Encoding

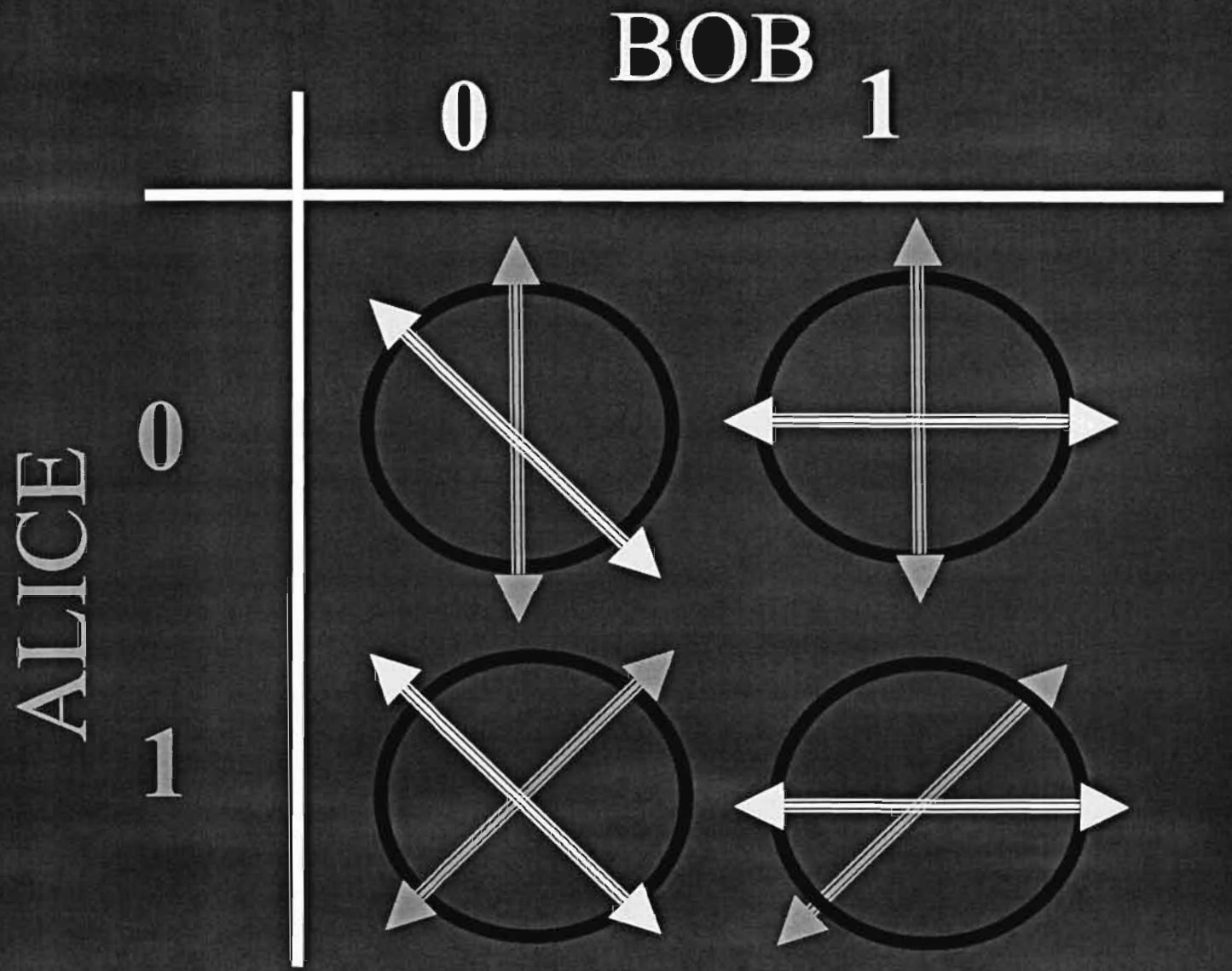


"0" "1"

QKD Key Generation Sequence



Truth Table



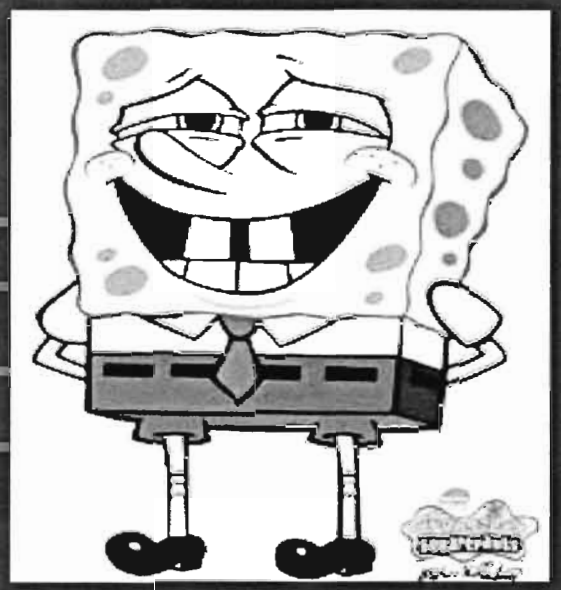
QKD Key Generation Sequence

Receiver Initiation Signal

Timing Pulse

Key Generation Link

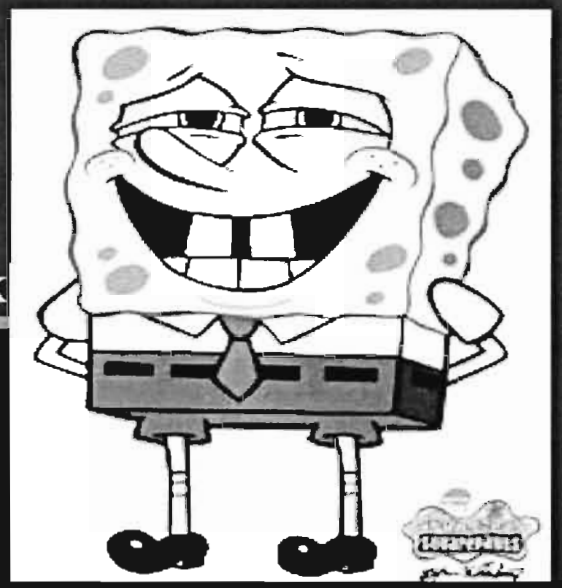
Datalink



- Initiation broadcast from Bob indicates reception availability.
- Timing pulse from Alice provides reference for gated detection of photon.
- Alice generates photons through a random polarization; Bob detects photons with random polarization.
- Alice and Bob compare notes via communications on a data link to mutually establish random keys.

QKD Key Generation Sequence

Key Generation Link

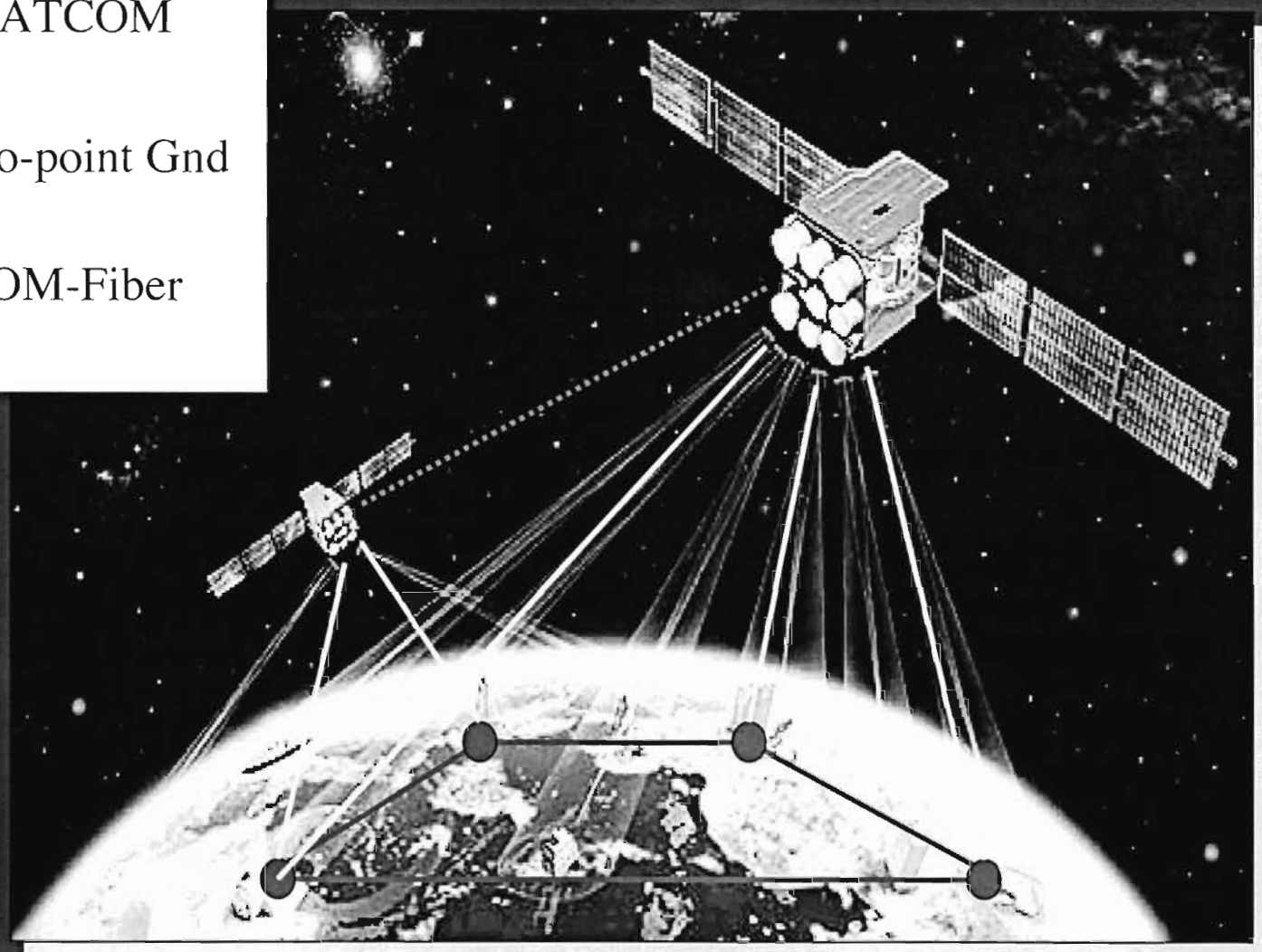


- QKD demonstrated over 49 km of dedicated experimental fiber by LANL.
- British Telecom demonstrated over 30 km of datalink; no degradation of QKD signal.

QKD Network Vision

LEGEND

- ····· •Inter-SATCOM
- —— •Point-to-point Gnd Fiber
- •SATCOM-Fiber node

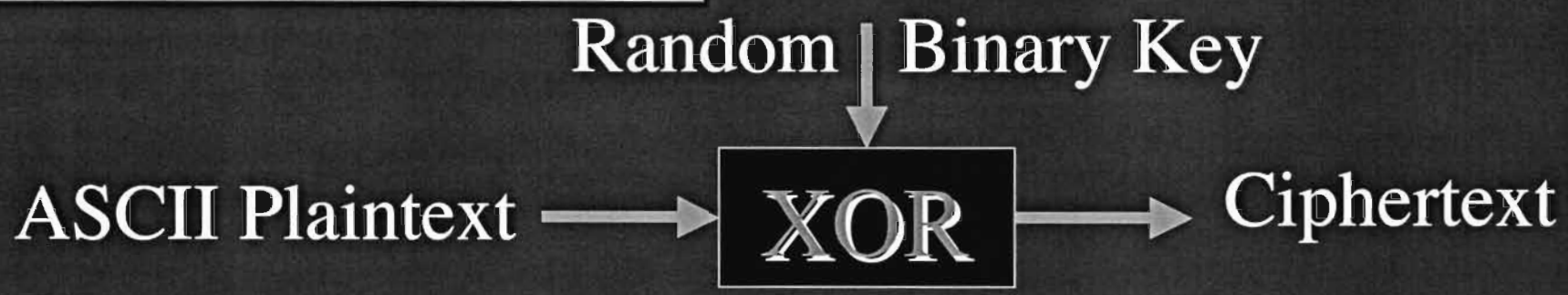


Outline

- Buzz Words
- What is the nature of Light?
  - What is classical light?
  - What is a photon? (aka Quantum information)
- Encryption
- Alice's problem (Hint: Evil Eve)
- Quantum Key Distribution (QKD)
- ★ Advanced QKD

New research focuses on increasing key generation rate

VERNAM CIPHER

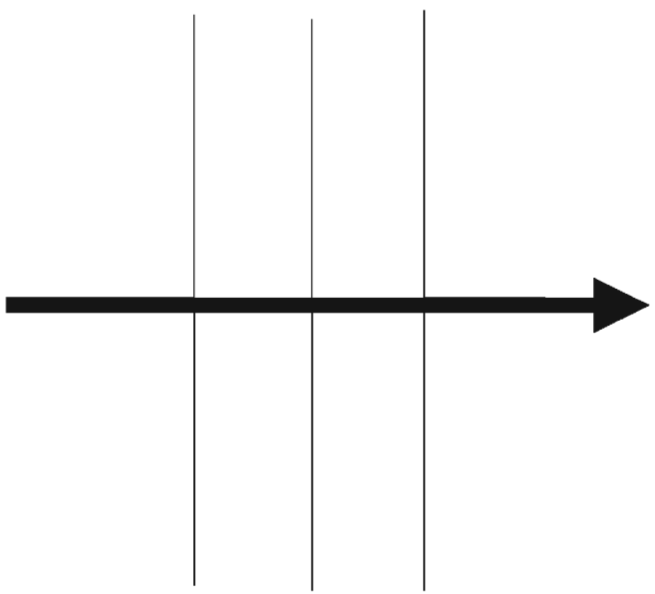


MAJOR DRAWBACK:

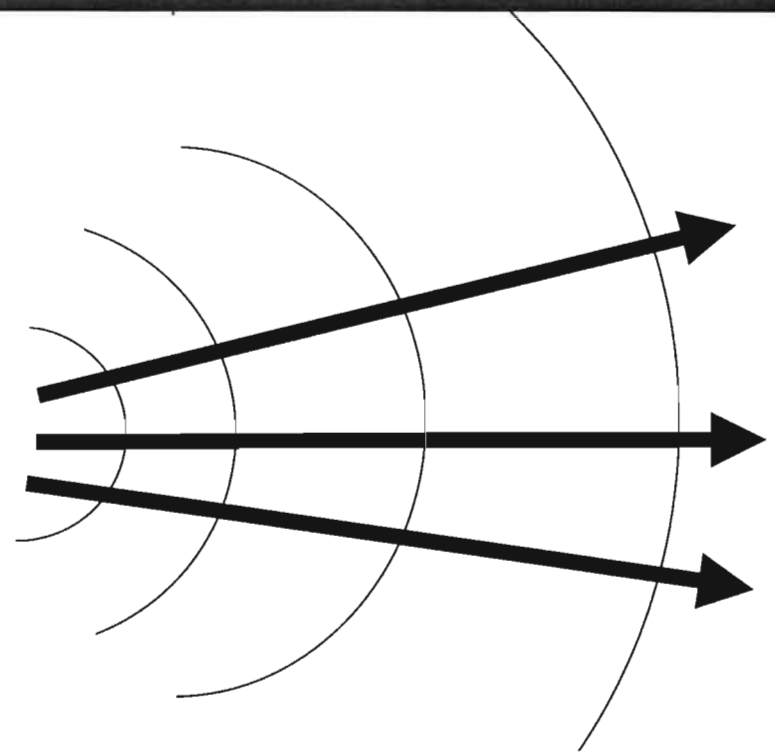
Key length must be as long as the length of plaintext!

=> Motivated to improve key generation efficiency.

Orbital Angular Momentum

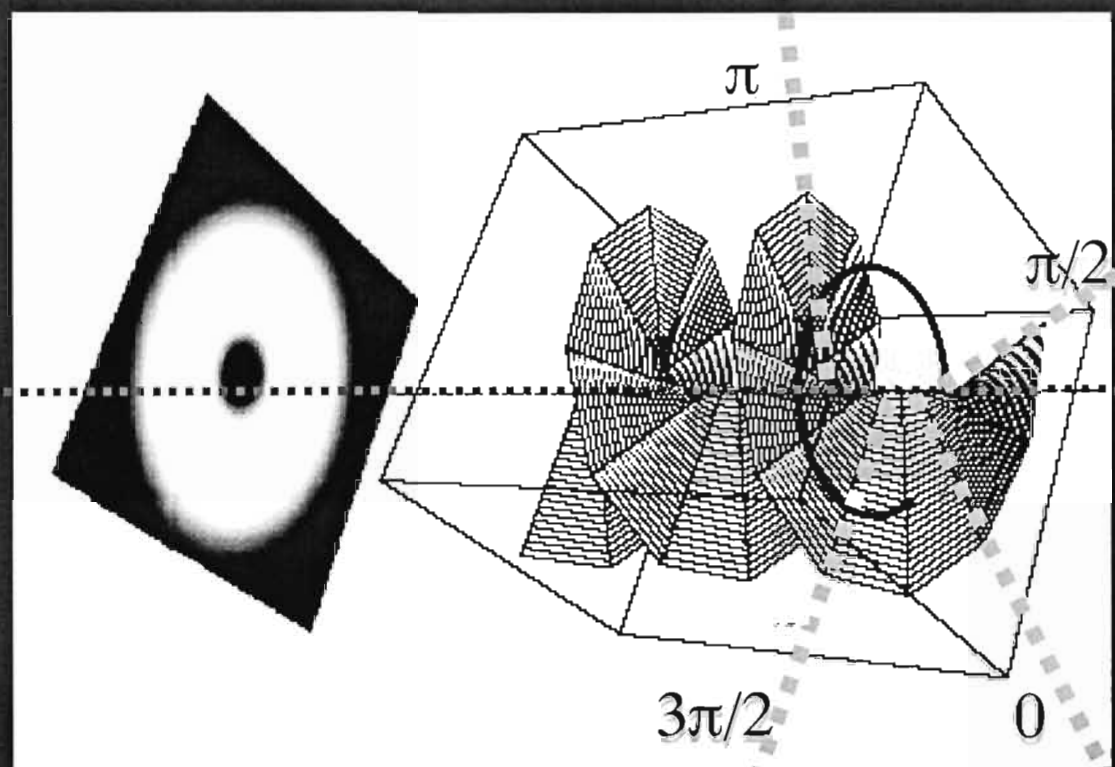


Plane wave propagation

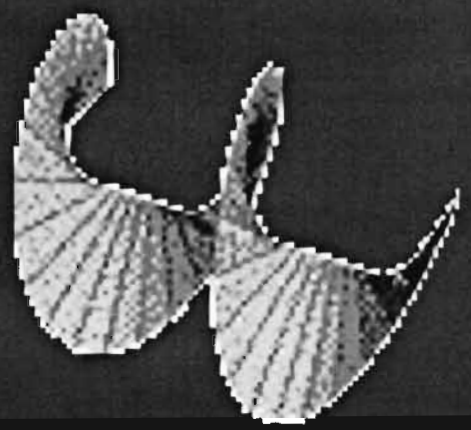


Gaussian wave propagation

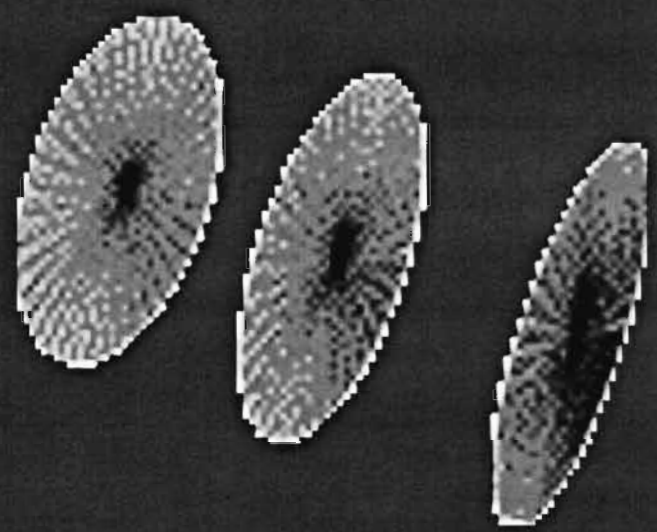
Beam Phase Front Rotates Instead of Individual Photons Spinning



Orbital Angular Momentum, l=-1

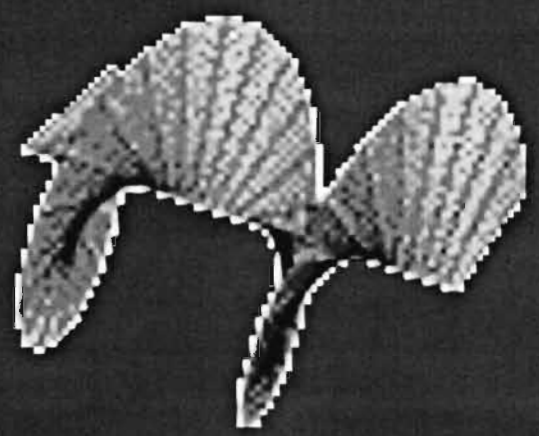


Orbital Angular Momentum, l=0



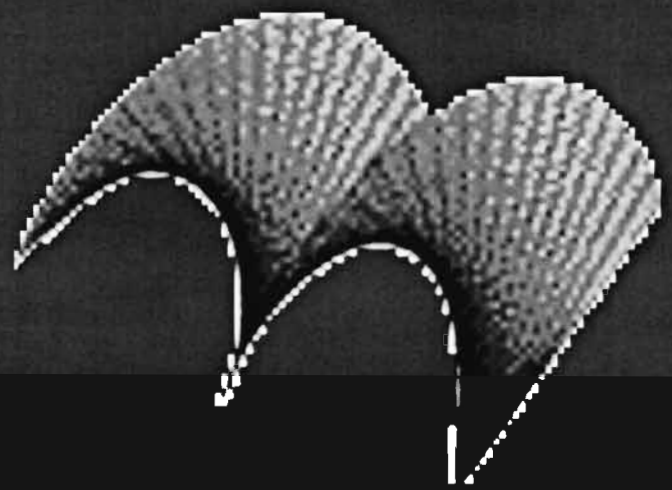
Credit: University of Glasgow Optics Group

Orbital Angular Momentum, l=1

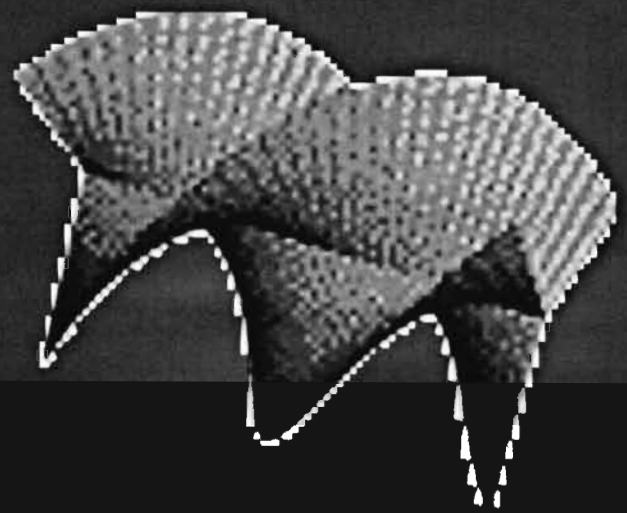


Credit: University of Glasgow Optics Group

Orbital Angular Momentum, l=2



Orbital Angular Momentum, l=3

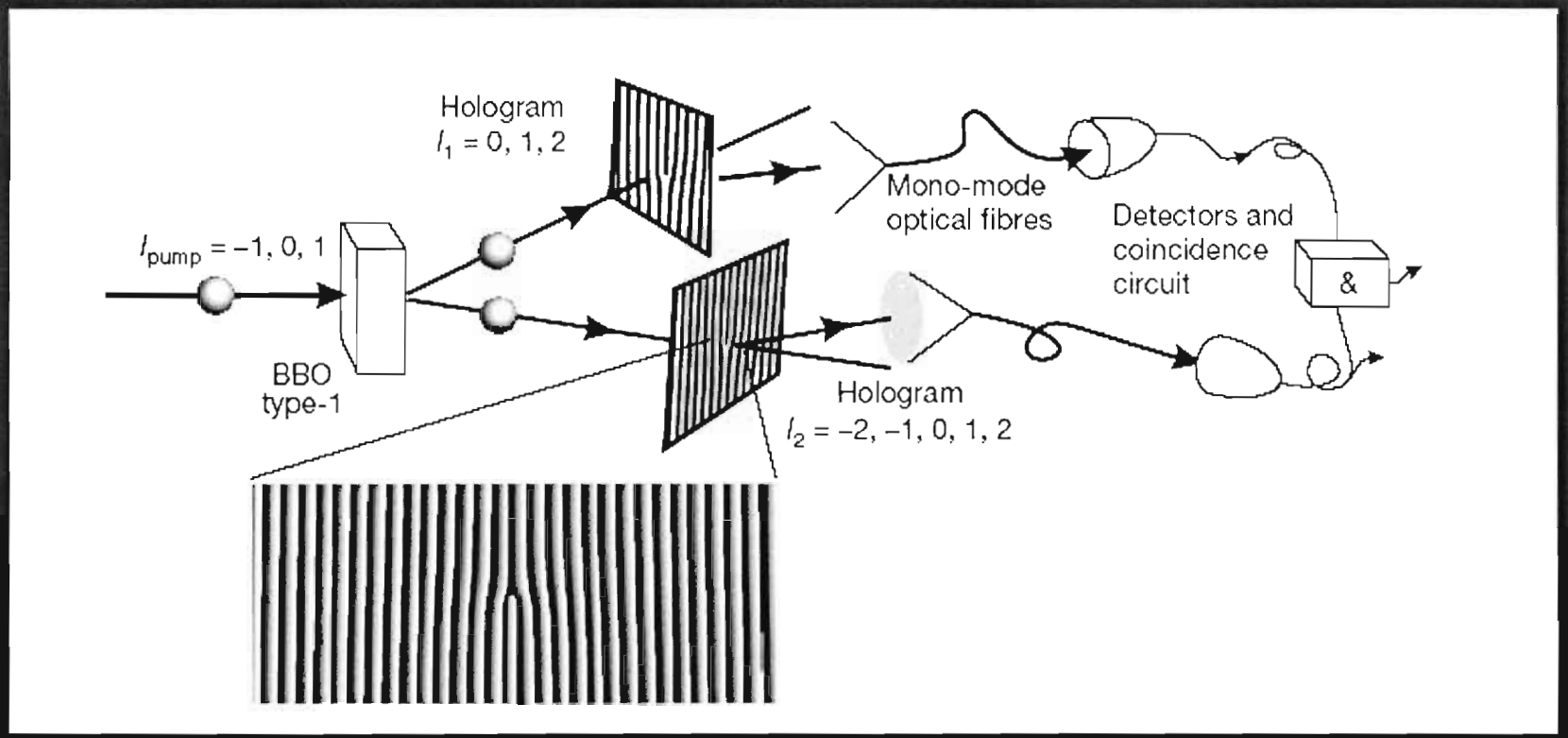


OAM encoding

Orbital Angular Momentum encoding allows a single photon carries more than one bit of information

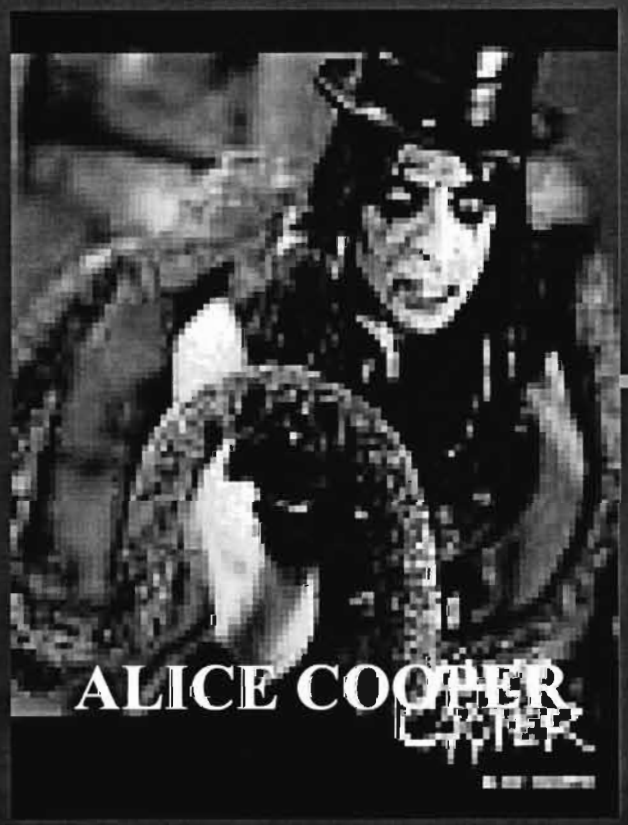
ℓ	Binary bits
–3	000
–2	001
–1	010
0	011
+1	100
+2	101
+3	110

Can a single photon be prepared with orbital angular momentum?

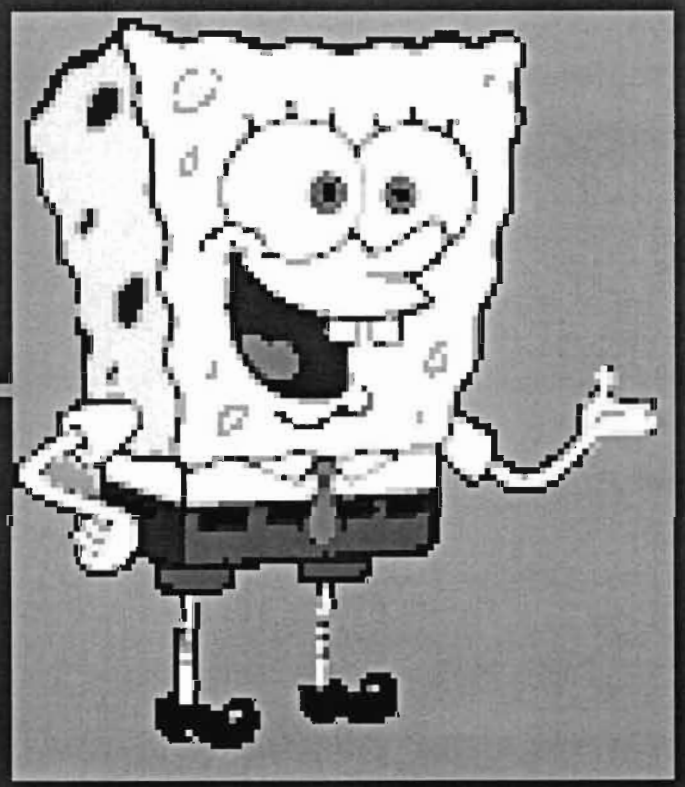


Mair et. al., Nature 412, 313 - 316 (19 July 2001).

OAM QKD Key Generation Sequence



Key Generation Link



CONCLUSIONS

- Quantum Key Distribution offers an unconditionally secure method of exchanging encryption keys.
- Ongoing research focuses on how to increase the key generation rate.

THE END