THE START

Quantum Key Distribution [QKD]

Quantum Keys By Polarization (w/) or (w/o) Entanglement

Pace University

rfrank@pace.edu

1. Table of Contents [1/1]

2. MOTIVATION

All encryption methods fail in one way. The distribution of keys is **insecure**.

All current encryption methods can be broken with enough computing power [which is increasing] except one-time-pads **OTP** (see above).

QKD distribution is secure.
QKD can't be broken (it is a OTP).

3. Encryption – Why Bother With QKD?
&
Current State of QKD
&
Overview of QKD

Why Bother With QKD?
(Current Problems Intro)

A Current State of Network Encryption Usage

B Why should we understand it?

C Potential Weaknesses

D What is The Classical Key Distribution Problem?

E Therefore QKD

A. Current State of Network Encryption Usage

- DES —► AES (Symmetric all)
- PKI (Asymmetric – 2 key)
- IPSEC (Symmetric, AES)
- SSL/TLS (Negotiated – PKI/Symmetric)

B. Why should we understand it?

- PKI & AES
  - Founded on a conjecture
    - Ultimately on computational burden too large for an enemy.
  - BUT Faster Computers Coming
  - BUT Quantum Computers

    Will Break It!

C. Potential Weaknesses

1. **PKI Based on assumptions about factoring large numbers.**

2. **Security of 3rd Party PKI Key Vault**

3. **Security of (P_r) Key**
   - ***Distribution Problem***
   - ***3rd Party Vault Current MO***

D. What is The Classical Key Distribution Problem?

- **One-time-pads (1 key/1 message)**

IT IS SYMMETRIC! [You & Me: Pads ≡]

Key as long as message (|K|~|M|)

Vernam Cipher (K ⊕ M) [XOR]

***ONLY* Unbreakable Code**

(Proved by Shannon)

If done right.

The Key (*PAD*)

Distribution Problem Again

E. WHY QKD? [1/3]

- **Computation capability is increasing non-linearly**

- **Quantum Computers Promise to Completely Negate Efficacy of Current Encryption Technology (i.e., *kill it dead*) (not imminent)**

E. WHY QKD? [2/3]

- **QKD is Based On Physics**
- **Unaffected By Either:**
  - **Current Computer Technology**

    or
  - **QUANTUM COMPUTING CAPABILITY**
- **It is a handshake protocol**
- **It can sense Eve *(Alice, Eve, Bob)***
- **After Key Distribution:**
  - **Use classical**

    or
  - **Q-encryption**

E. WHY QKD? [3/3]

QKD SOLVES THE KEY DISTRIBUTION PROBLEM & IS UNBREAKABLE

Summary: So What?

- More Secure Data Transmission

- QKD Used For:
  - IPSEC (for Internet) (& SSL)
  - Replace PKI, AES
  - It is a Vernam One-Time-Pad (Unbreakable!)
  - Solves the key distribution problem
    - Borming's Dissertation (for Grids)
  - Chinese from a satellite.
  - Chinese national effort to secure networking.

Current QKD State

- **QKD**
  - **There are products that do it (100+ km distances) [MAGIQTECH]**
  - **Open air QE coming to a satellite near you**
  - **BBN Boston Network & Vienna Network**
- **QKD In TCP/IP**
  - **Research progressing**
- **QKD Education**
  - **QE appearing in CS texts [Tanenbaum's Networking]**
- **Cultural Motivation to Learn**
  - **<u>30% GDP derives from QM</u>**

    [Waite, Stephen R., 2002]

OVERVIEW of QKD [1/2]

A Crypto Key

- A key for encryption/decryption is sent using Quantum Mechanical Phenomena.

- The key may be a quantum encryption key or a non-Quantum encryption Key, e. g., a PKI private key.

- The transmission may or may not involve entanglement.

Entanglement

Two (or more) particles created as single coupled complimentary set. A measurement of one determines the complimentary value of the other(s) regardless of separation.

OVERVIEW of QKD [2/2]

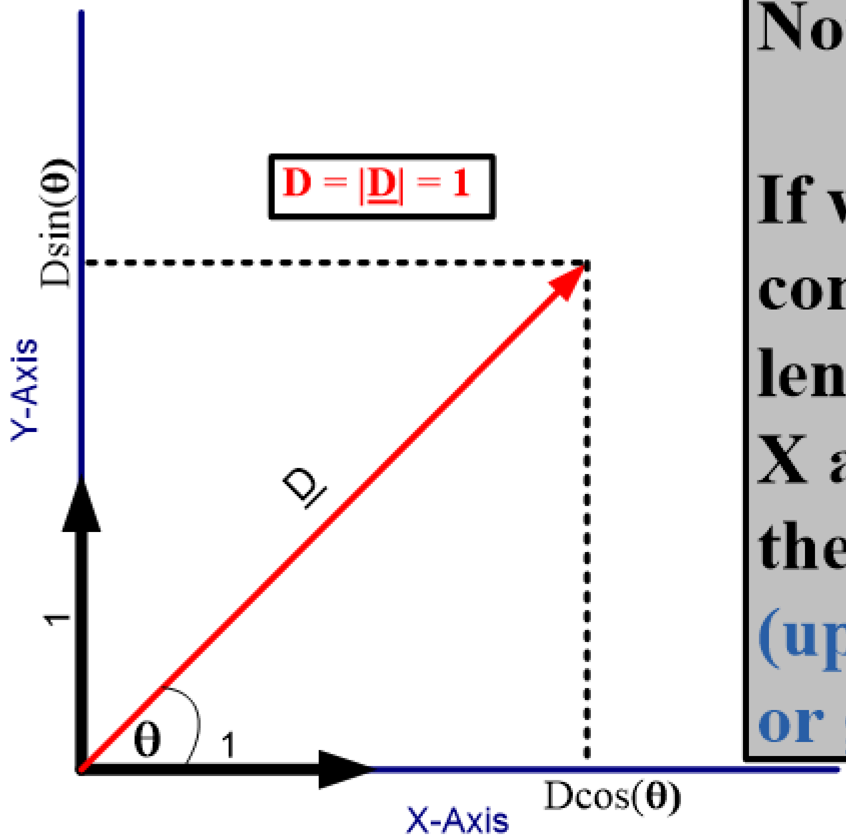
One-time-pads (1TP)

- QKD is to used create a shared key for a 1TP
- The 1TP is used to send an encrypted message
- Only proved unbreakable encryption scheme.
- This is done many time/sec (>100)

4. Vectors & QM

Vectors

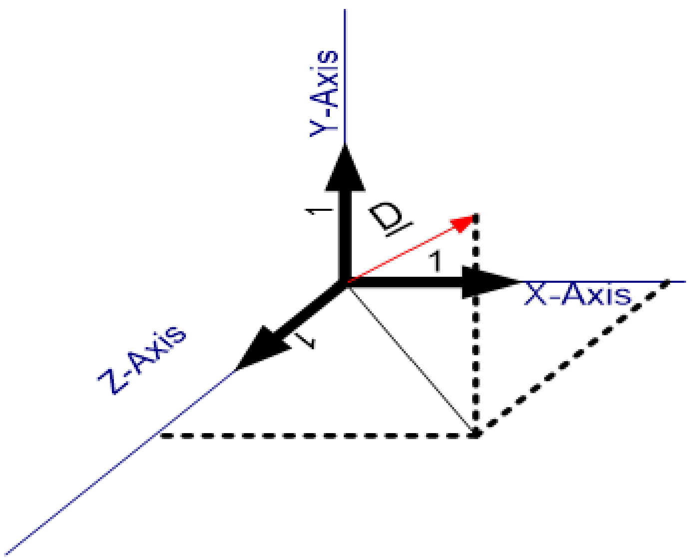
TRICK



Notice: ***2-D Special Case***

If we know the X component of vector D of length = 1, is 0 along the X axis, we know D lies in the Y axis. UNIQENESS (up to ±). Not so in 3-D or greater.

Vectors



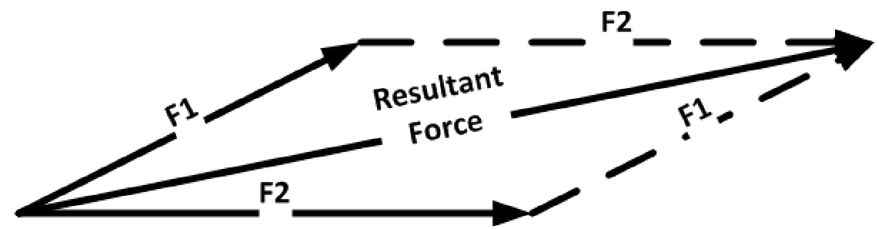
Notice:

If we know the vector |D| = 1 has component of 0 length along the X axis, ALL we know it lies in the Y-Z plane. There are ∞ vectors (or lines) in Y-Z orthogonal to X. NON-UNIQENESS.

Vectors

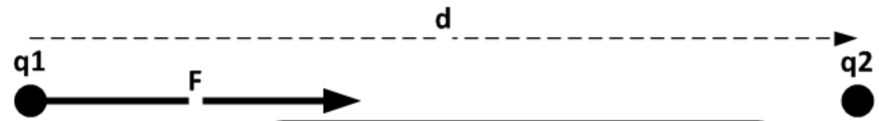
Vector Examples

Mechanical FORCE



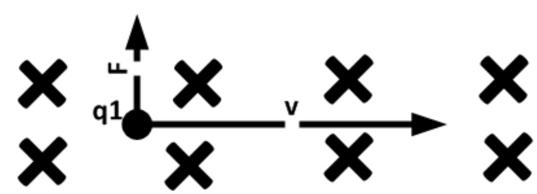
Law: Parallelogram of Forces:
RF = F1 + F2 (Vector Addition)

Electric FORCE



Law: Electrostatic Force: Charges q1 & q2,
$F = (q1*q2)/d^2$: A vector:
q1, q2: [+, -] or [-, +] : Toward q2
q1, q2: [-, -] or [+, +] Away From q2

Magnetic FORCE



Black Hole Vertical Jets

Law: Right Hand Rule:
v is velocity of charge (fingers), B field vectors into paper (fingers curl closed into paper), F is force on q1 in the direction of your thumb.

WHY Vectors (Linear Algebra)?

The world can be effectively modelled by *Objects* that have *Observable States* with *Measureable [real] Values* with known *probabilities* of measurement.

Objects can be effectively modelled by *Hermitian Operators* on *vectors*.

States can be effectively modelled by *vectors* [combination of eigenvectors].

Measureable values of the object can be effectively modelled by *eigenvalues* of the eigenvectors of the object. Hermitian => real.

WHY Vectors (Linear Algebra)?

The probability of finding the initial [before measurement] system in the final eigenstate vector [i] with measured eigenvalue [λ] after measurement , can be effectively modelled as the *__square__* of the *__projection__* of the initial [before measurement] system vector onto the eigenvector [i] found as the result of the measurement.

Example (Continued):

$$\boxed{H = \lambda \underline{v}}$$

$$\boxed{H = \sum_{i=1}^{i=N} \lambda_i (\underline{v}_i \underline{v}_i^T) == \sum_{i=1}^{i=N} \lambda_i P[\underline{v}_i]}$$

Hermitian operators have a spanning set of eigenvectors with all eigenvalues <u>real</u>.

https://en.wikipedia.org/wiki/Spectral_theorem

<u>For convenience we take the eigenvectors & other state vectors to be of unit length.</u>

If the operator is real symmetric this is the principle components theorem.

https://en.wikipedia.org/wiki/Principal_component_analysis

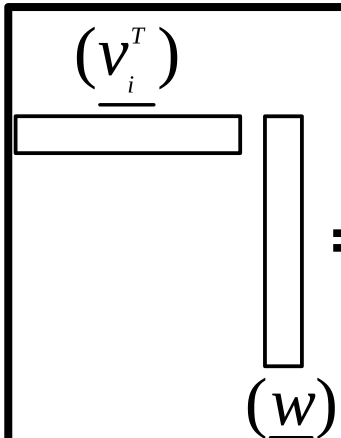
$$\boxed{\left[A = X^T X\right] \Rightarrow A^T = \left(X^T X\right)^T = X^T X = A}$$

Example (Continued):

Projector on the eigenvector.

$$(\underline{v}_i\,\underline{v}_i^T)\underline{w} = \underline{v}_i(\underline{v}_i^T\,\underline{w}) = P[\underline{v}_i]\underline{w} = \underline{v}_i k_i$$

$$H\underline{w} = \sum_{i=1}^{i=N}\lambda_i(\underline{v}_i\,\underline{v}_i^T)\ \underline{w} = \sum_{i=1}^{i=N}\lambda_i P[\underline{v}_i]\ \underline{w} = \sum_{i=1}^{i=N}\lambda_i\underline{v}_i k_i$$

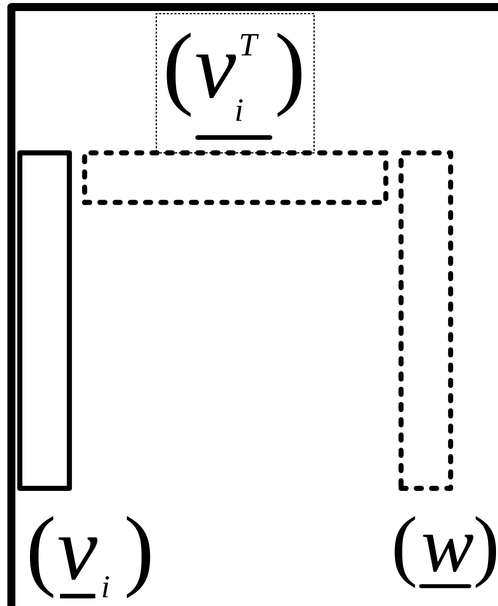


Measurement chooses ONE i

$= |(\underline{v}_i^T)|\,|(\underline{w})|$ **Cos(θ) = constant k_i**

$$p(\lambda_i\underline{v}_i) = (k_i)^2$$

Probability of λ_i



Example (Continued):

$$\boxed{\sum_{i=1}^{i=N} \lambda_i \underline{v}_i \left(\underline{v}_i^T \underline{w}\right) = \sum_{i=1}^{i=N} \left[\lambda_i (k_i)\right] \underline{v}_i}$$

$$(k_i)^2: \quad \left[\left\{ |w| = 1 \right\} \Rightarrow \left\{ \sum_{j=1}^{j=N} (k_j)^2 = 1 \right\} \Rightarrow (k_i)^2 < 1 \right]$$

$$\left[\left\{ \sum_{j=1}^{j=N} (k_j)^2 = 1 \right\} \& \, (k_i)^2 < 1 \right] \Rightarrow$$

$(k_i)^2$ has the properites of a probability.

Example:

The energy of a particle can be effectively modelled by a Hermitian Operator.

The location and velocity states of the particle can be effectively modelled by sets of eigenvectors of the Hermitian operator.

The value of the particle's energy when in one of the states can be effectively modelled by the eigenvalue corresponding to that state.

The Heisenberg Uncertainty Principle says we can't simultaneously measure the location state/value and the velocity state/value from the 2 sets.

Vectors & QM

Quantum Mechanics is "just" modeling a physical system by "the right" Hermitian vector space.

Measurable Quantity $\xleftrightarrow{H^* = H}$ **Hermitian Operator**

$$H\underline{\mathrm{v}} = \lambda\underline{\mathrm{v}}$$

Measured __Value__ $\longleftrightarrow$ **Eigen__value__**

[All states = length 1, all eigenvalues real]

[Sometimes we don't care about the values!]

$$H\left(-\underline{\mathrm{v}}\right) = \lambda\left(-\underline{\mathrm{v}}\right)$$

Measured State ["Pure"] $\longleftrightarrow$ **Eigenvector**

[Sometimes we know the eigenvectors so we don't need the operator!]

[Most times we care only about the line, not the +- direction!]

Gen. System States $\longleftrightarrow$ **Eigenvector Combination**

Probability of __Value__ $\longleftrightarrow$ **(Length)^2 of projection on resultant eigenvector [<=1]**

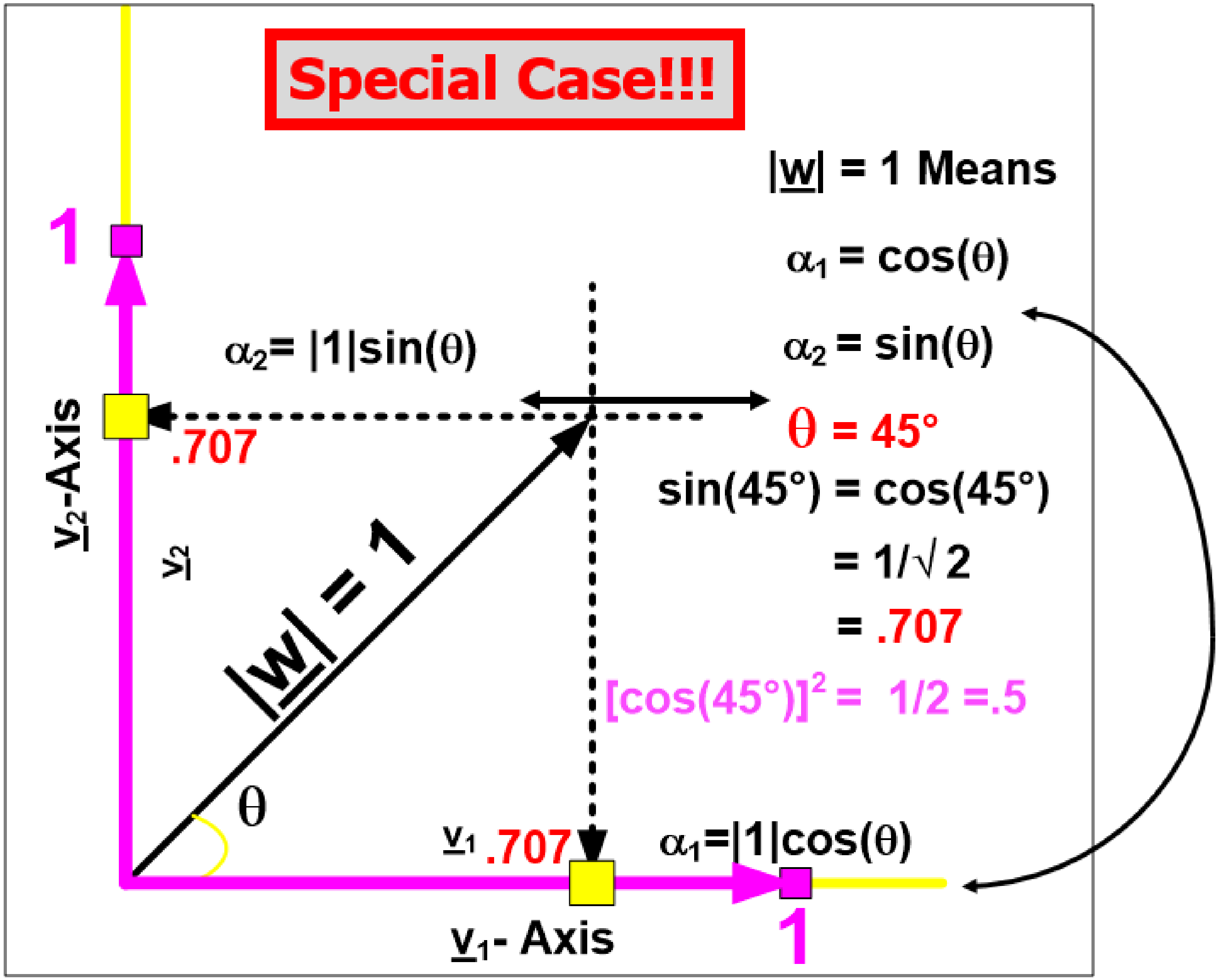
Vectors & QM

1. **A Quantum System in a physical state is represented by a corresponding UNIT vector in some ~~abstract~~ Hermitian vector space.**
2. **A Measurement puts the Quantum System into a unique physical state called a "Pure State" represented by a vector along a UNIT Basis Vector in that ~~abstract~~ vector space.**
3. **Before any measurement, the system is in an <u>unknown</u> mixture of pure states, called a "Mixed State".**
4. **A measurement corresponds to a projection of a UNIT mixed vector onto ONE of the UNIT basis vectors of the ~~abstract~~ space.**

Vectors & QM

5. **The $(\text{length})^2 < 1$ of the projected unit mixed state vector is the PROBABILITY of finding that Pure State in any given measurement.**
6. **All Basis Vectors are actually eigenvectors of the operator representing the measured quantity.**
7. **The value of the eigenvalue corresponding to the pure state is the measured VALUE in that pure state.**
8. **A measurement corresponds to a meter reading of a physical system in an unknown state yielding a known state with a known metered value.**

Components as Projections



Basis Vectors

5. Physical Background of The QKD Algorithm

Background (2-D Polarization, & Probability)

1. 2-D Vector Uses
   - Components as Projections
2. Polarization of Light
   - Polarized Photons
   - Filtered Photons Have P=1
3. Discrete Probability (Definition)

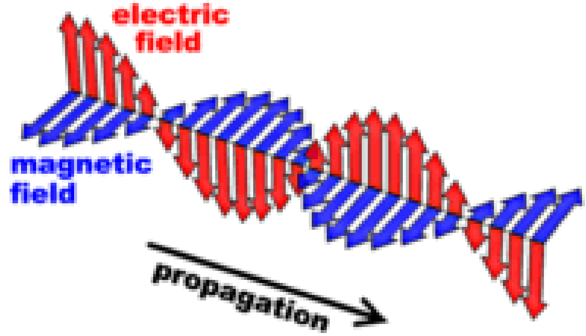
   Addition ("OR")

   Multiplication ("AND")

Physics of QKD

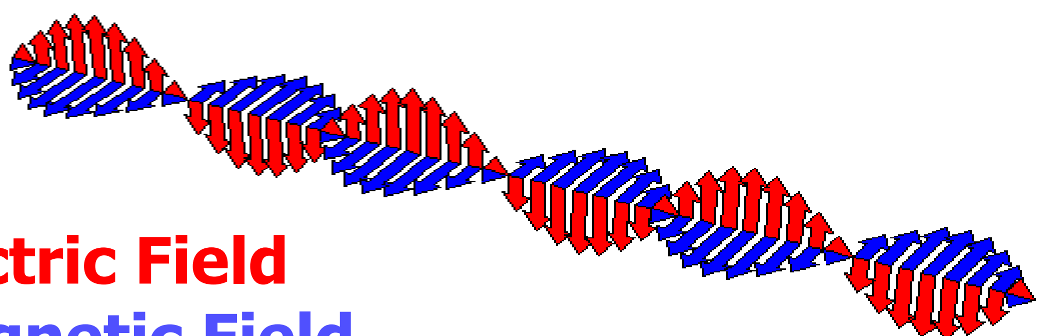
Propagating Electromagnetic Field

Rotates Around Direction of Propagation



IF Fixed Plane THEN "Polarized"

<u>2, 3-component Fields = 6 components</u>



<u>E</u>(t) = Electric Field
<u>H</u>(t) = Magnetic Field

Polarization of Light

- **A photon is a “particle” of light**
- **A photon can be polarized along a direction**

  In the 2-D space perpendicular to the propagation direction.
- **A photon can be polarized by a filter**
- **Once polarized by a filter *(QM Think)***
  - **it passes through <u>that</u> filter: p= 100%**
  - **it is blocked by a filter at 90°: p = 0 %**

    [2-D TRICK]
  - **it passes a (45°) filter BUT**
    - **it becomes (45°) polarized**
      - **there is a 50% chance of being one**
      - **there is a 50% chance of being other**

2x(2-D Vector) Bases

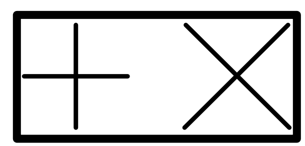
- **A photon state is a unit ‘vector’ ↕ , ↔ , ⤡, or ⤢.**
  [We use only the ray (line) not the direction]

- **{ ↕ & ↔ } are a basis of the 2-D space**

  The 2-D space is perpendicular to the propagation direction.

- **{ ⤡ & ⤢ } are also a basis of the 2-D space**

- **These are also the 4 filters (*directions*) we use as**
  2 pairs +, & X,



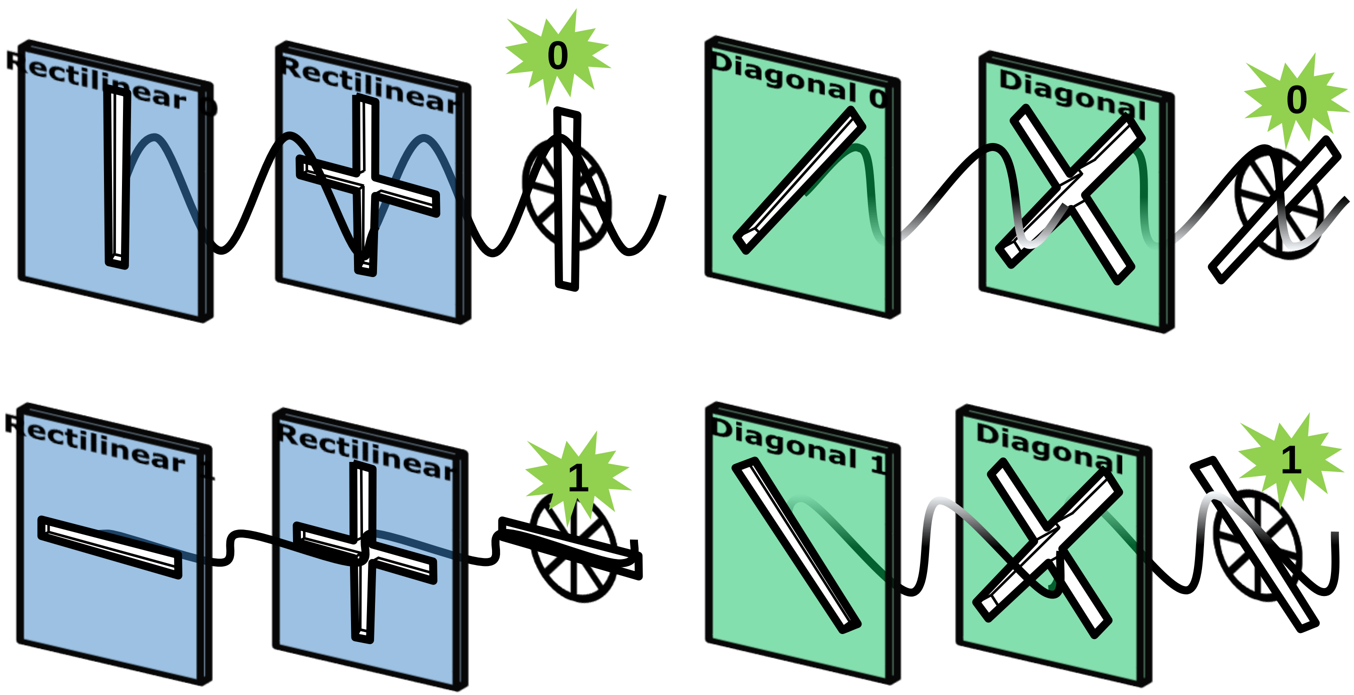
- **A photon in a state in one basis is represented**
  - **as a sum in the other basis**
  - **with projected <u>lengths</u> = 1cos(45°)=1/√2**
  - **giving [1cos(45°)]^{2}= .5 as probabilities**

Polarized Photons

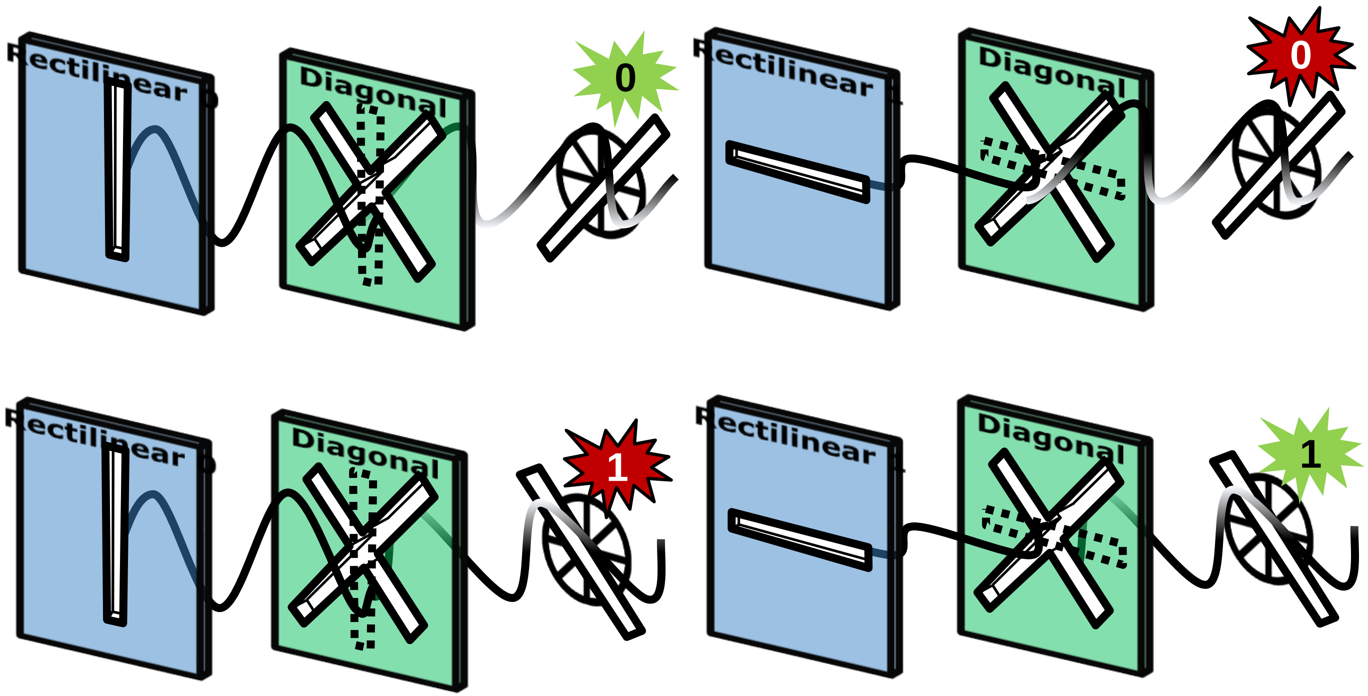
A UNIT basis vector represented in a Second, 45° rotated basis has $(\text{projection})^2 = .5$ on EITHER second-basis direction.

I.e., we have p=.5 (I.e., EQUAL) probabilities of getting either second-basis vector as a measurement state result.

Polarization, correctly aligned filter correctly detects the bit sent

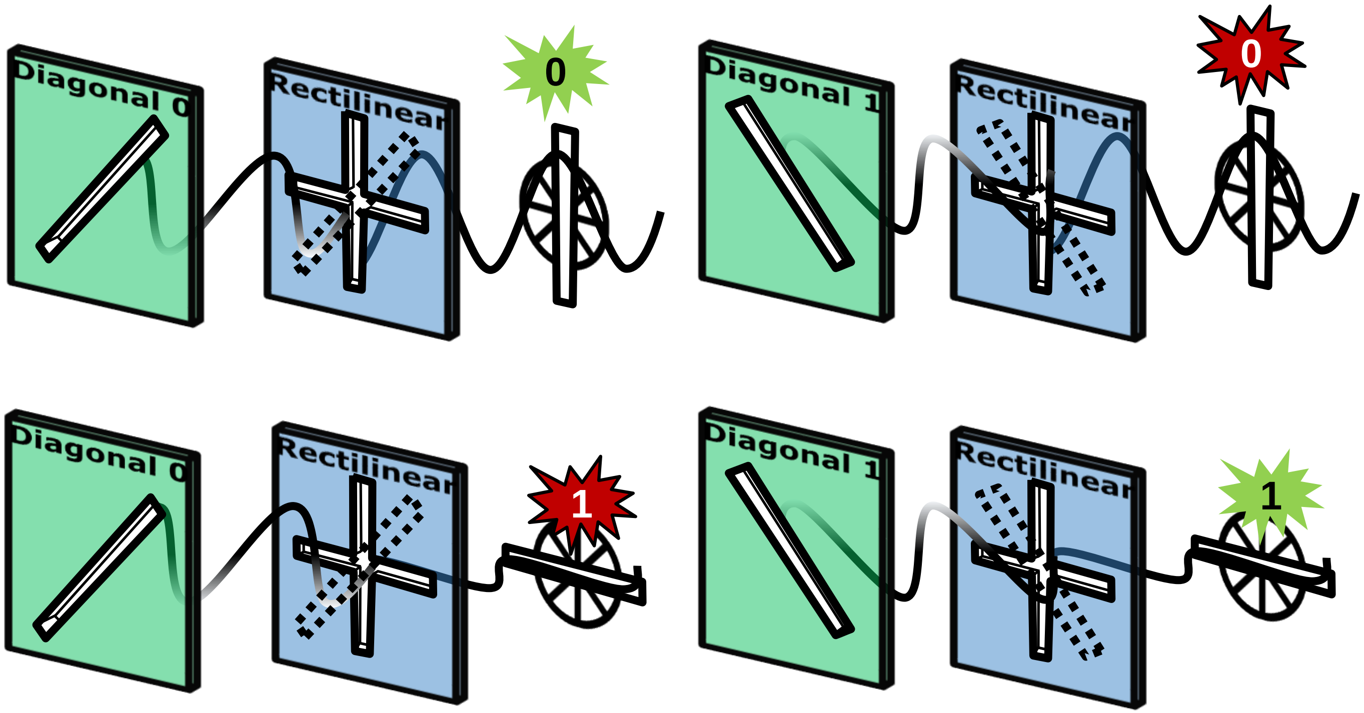


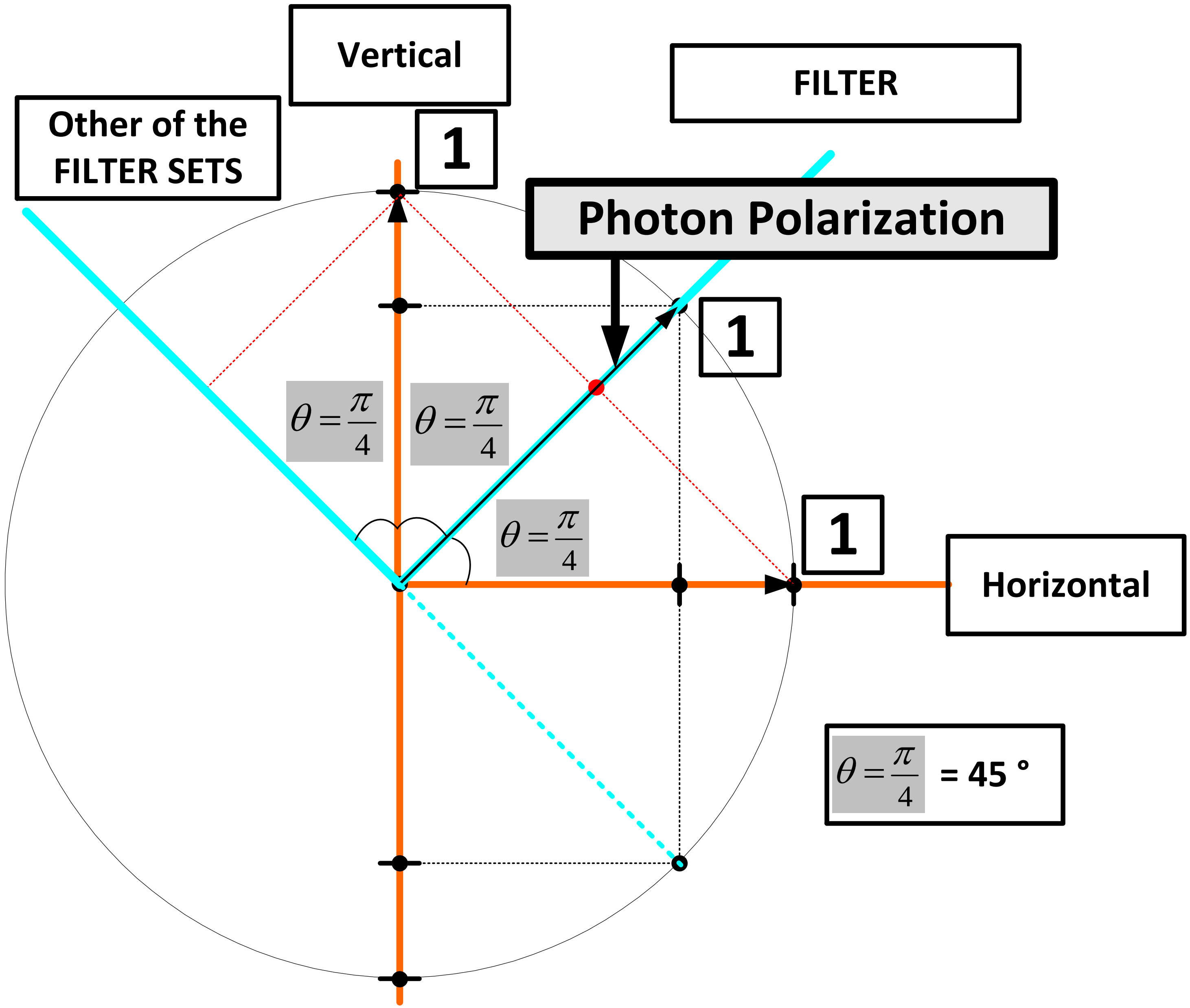
Rectilinear polarization, *diagonal* filter, quantum effect yields either bit



Photon has all possible states until detection, at which time it must choose a state based on the sending and detecting polarity filters

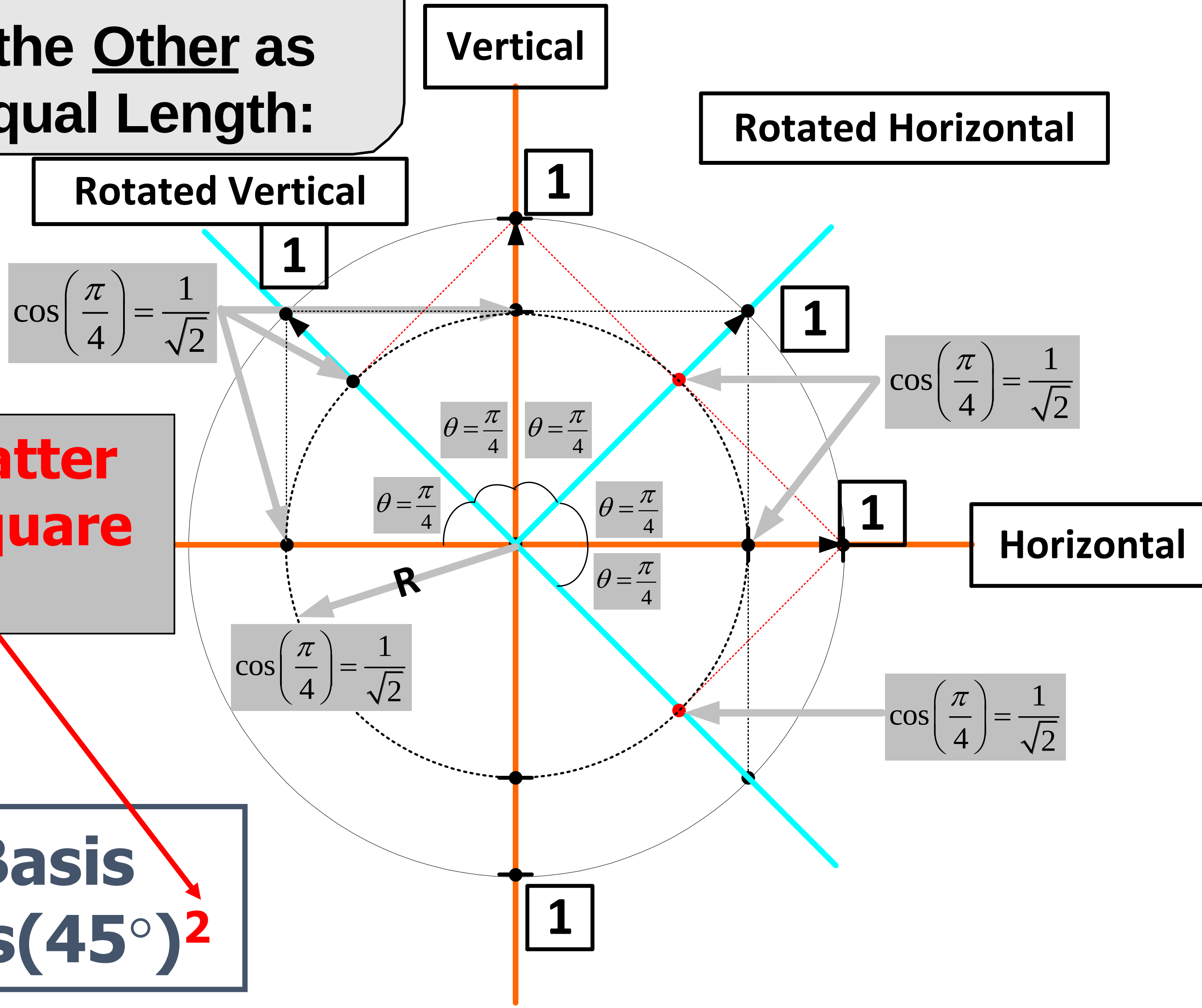
Diagonal polarization, *rectilinear* filter, quantum effect yields either bit




Vertical
FILTER
Other of the FILTER SETS
1
Photon Polarization
1
$\theta = \frac{\pi}{4}$
$\theta = \frac{\pi}{4}$
$\theta = \frac{\pi}{4}$
1
Horizontal
$\theta = \frac{\pi}{4}$ = 45 °

Two Axes Rotated 45 Degrees Relative to Each Other

The Unit Axis Vectors of Each Project onto the Other as Vectors of Equal Length:



Signs don't matter because we square lengths.

Rotated Basis

$$p=.5=1^2\cos(45^\circ)^2$$

Filtered Photons Have P=1
Of passing same filter again.

They lie along the filter direction

so: $\cos(0°)^2 = 1^2 = 1 = P.$

OR

$\cos(180°)^2 = (-1)^2 = 1 = P.$

So we care only about the line not the (+ or -) direction of the vector.

Discrete Probability

- $0 \leq p_i \leq 1$ for all cases i
- i discrete & finite
- {Sum of p_i over all cases i} = 1
- Probability of case j AND case k =

  $p_j \, p_k$
- Probability of case j OR case k =

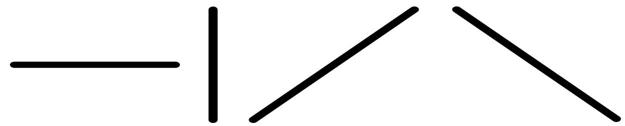
  $p_j + p_k$

QKD Algorithm Background [1/3]

1. **The whole purpose of the QKD algorithm is to find a secure 1TP (Key) for encryption**

2. **A polarized photon is a particle of light that has a known [i.e., measured] electric field orientation orthogonal to propagation**
   - **PASSING LIGHT THRU A POLARIZATION FILTER IS MEASURING ITS FIELD ORIENTATION**
   - **We use two filter SETS called + X because that is what they look like.**
   - **They are rotated relative to each other by 45° TRICK!!! TRICK!!! TRICK!!!**

QKD Algorithm Background [2/3]

- **We use 4 filters.** 
- **We can call them horizontal, vertical, right 45 and left 45 (since the last two are at 45 degrees to the vertical).**

- **<u>Polarized Photon State Vectors</u>**
  - **A state of vertical polarization is notated** $|\updownarrow\rangle$
  - **A state of horizontal polarization is notated** $|\leftrightarrow\rangle$

  - **A state of 45° right polarization is notated** $|\swarrow\!\!\!\!\!\!\nearrow\rangle$
  - **A state of 45° left polarization is notated** $|\nwarrow\!\!\!\!\!\!\searrow\rangle$

    [We really want only the ray not the direction since signs don't count because we square lengths]

QKD Algorithm Background [1/3]

We chose one state from <u>each basis pair</u> to represent a 1 bit
(the other of the pair is the 0 bit) TRICK

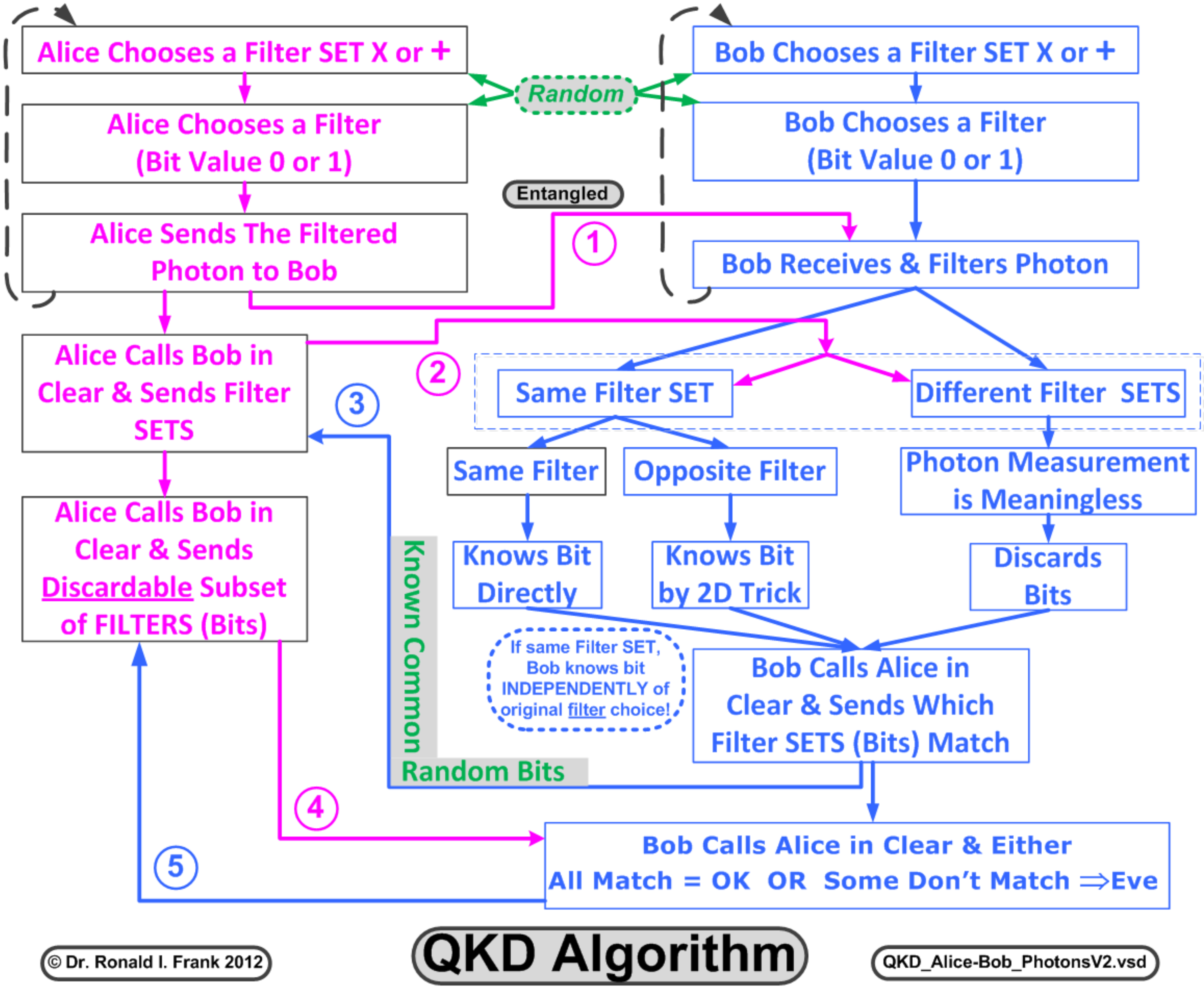
[Arbitrary choice of rep]

$$\boxed{\begin{array}{l} |\updownarrow\rangle \triangleq 1, \Rightarrow |\leftrightarrow\rangle \triangleq 0 \\ |\swarrow\!\!\!\nearrow\rangle \triangleq 1, \Rightarrow |\nwarrow\!\!\!\searrow\rangle \triangleq 0 \end{array}}$$

6. Quantum Key Distribution The Algorithm

What QKD IS
(The Details)

See the Bibliography for sources.


Alice Chooses a Filter SET X or +
Alice Chooses a Filter (Bit Value 0 or 1)
Alice Sends The Filtered Photon to Bob
Random
Entangled
Bob Chooses a Filter SET X or +
Bob Chooses a Filter (Bit Value 0 or 1)
Bob Receives & Filters Photon
1
2
3
Alice Calls Bob in Clear & Sends Filter SETS
Same Filter SET
Different Filter SETS
Same Filter
Opposite Filter
Photon Measurement is Meaningless
Alice Calls Bob in Clear & Sends Discardable Subset of FILTERS (Bits)
Known Common
Knows Bit Directly
Knows Bit by 2D Trick
Discards Bits
If same Filter SET, Bob knows bit INDEPENDENTLY of original filter choice!
Bob Calls Alice in Clear & Sends Which Filter SETS (Bits) Match
Random Bits
4
5
Bob Calls Alice in Clear & Either
All Match = OK OR Some Don't Match ⇒Eve
© Dr. Ronald I. Frank 2012
QKD Algorithm
QKD_Alice-Bob_PhotonsV2.vsd

Quantum Key Distribution Algorithm

Alice sends N random bits (photons) using a random choice of N filters. Alice knows her bits (filters) & sets.

Entaglement Goes Here

1. **Bob uses a random choice of receiving filters**
   - **Bob knows his measured bits (filters) & sets.**
   - **Some are errors because he chose the wrong set**
   - **A bad set gives a bit error 50% of the time**
   - **A good set gives a correct bit 100% of the time**
2. **Alice calls Bob in the open and tells him HER Filter SETS**
3. **Bob tells Alice which of HIS SETS agree (M bits)**
   - **This determines a secret set of *M known bit values***
   - **This is a key (after 4) for encryption - if no Eve**
4. **Alice calls Bob and reads to him a discardable subset of HER actual FILTERS (i.e., BITS). If they agree there has been no Eve. Otherwise, there has been an Eve. DISCARD ALL!**

Singh, Simon. *The Code Book.* Anchor Books NY. ISBN 0-385-49532-3 (1999) PP. 339-344

Discussion [1/6]

Any measured (filtered) Photon is in a pure state

- **If measured again by the same filter get same state.**

- **If measured by the other filter of the same SET (90°) see NOTHING so know bit (2-D TRICK).**

- **If measured by the OTHER SET, get one of them with p = .5 by QM rep in other basis.**

Notice neither Bob or EVE knows Alice's filters when they have to choose their own.

Discussion [2/6]

Bob's random choice of a filter set matching Alice's is equi-probable (p = .5).

Either choice of bit (particular filter), given a matching pair will give correct info (actual bit or NOTHING, which implies the other bit 2-D TRICK!!!).

A choice of picking correct filter set (½).

The chance of picking N matching filters to Alice's hidden choices is $(½)^N$ [the AND case]. $(½)^N$ is $1/(2^N) \sim 10^{(-N/3.3)}$ For N = 128 $\sim 10^{(-36)}$

Doing it 100 times a second for one second $\sim 10^{(-36)100}$ $\sim 10^{(-3600)}$

$\sim 10^{(-3600)}$ qualifies as the definition of impossible.

Discussion [3/6]

Individual Photon Polarization Measurement is a Quantum Process

Knowing that the wrong basis gives either result with p = .5 (therefore no knowledge) is a quantum result.

Knowing that p = .5 because of the probability law of mixed state projections in 45° is a quantum result.

Knowing that a result of NO PHOTON means the complimentary pure state (therefore full knowledge - in 2-D ONLY) is a quantum result. 2-D, IS A TRICK - AGAIN.

Discussion [4/6]

The No Cloning Theorem

Any attempt to measure (read) an unknown (mixed) state MUST modify (Project) that state.

What we know is only the outcome state of the measurement, not the input state.

So – we can't copy (clone) a state.

The No Cloning Theorem

Discussion [5/6]

Quantum Key Distribution EVE Eavesdropping

Any attempt to read an unknown (mixed) photon and pass it on will introduce a probabilistic error.

There is a No Cloning Theorem.

In this case, cloning involves reading a photon.

Reading means applying a filter.

Eve can only pick a random choice of filter & SET which introduces a random change to an incoming photon – sometimes - and sometimes not.
She never knows which!

Discussion [6/6]

Quantum Key Distribution EVE Eavesdropping

Only if her filter SET happens to match the filter SET used by Alice to send the photon is there no error;

- **Eve can't know if there is a match.**
- **A possible basis change causes ambiguity in her resultant measurement knowledge.**
- **No Cloning causes her to almost always pass on some changed photons.**
  - **[She can be detected.]**

Algorithm Diagrams

- UML Swim Lanes w/o Eve
- UML Swim Lanes w/ Eve
- Text Formulation
- Flowchart (Again)

The Following Diagram: QKD Algorithm Overview

W/O Eve 1 of 2

W/O Eve 2 of 2

The The Following Diagram: QKD Algorithm Overview

W/ Eve 1 of 2

W/ Eve 2 of 2

Quantum Key Distribution Algorithm Summary

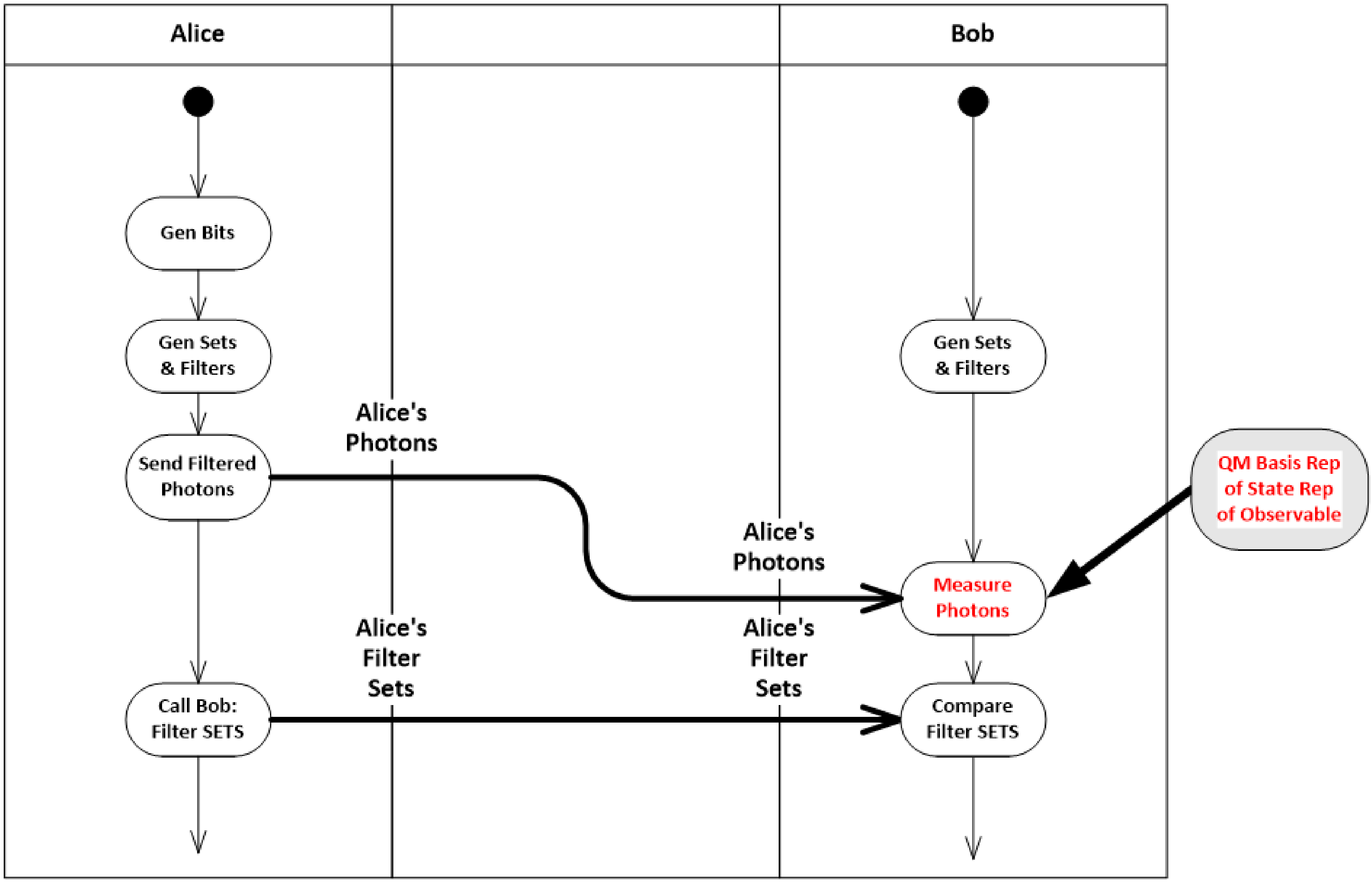
Quantum Key Distribution Results

Quantum Key Distribution One Time Pad

SUMMARY of Algorithm

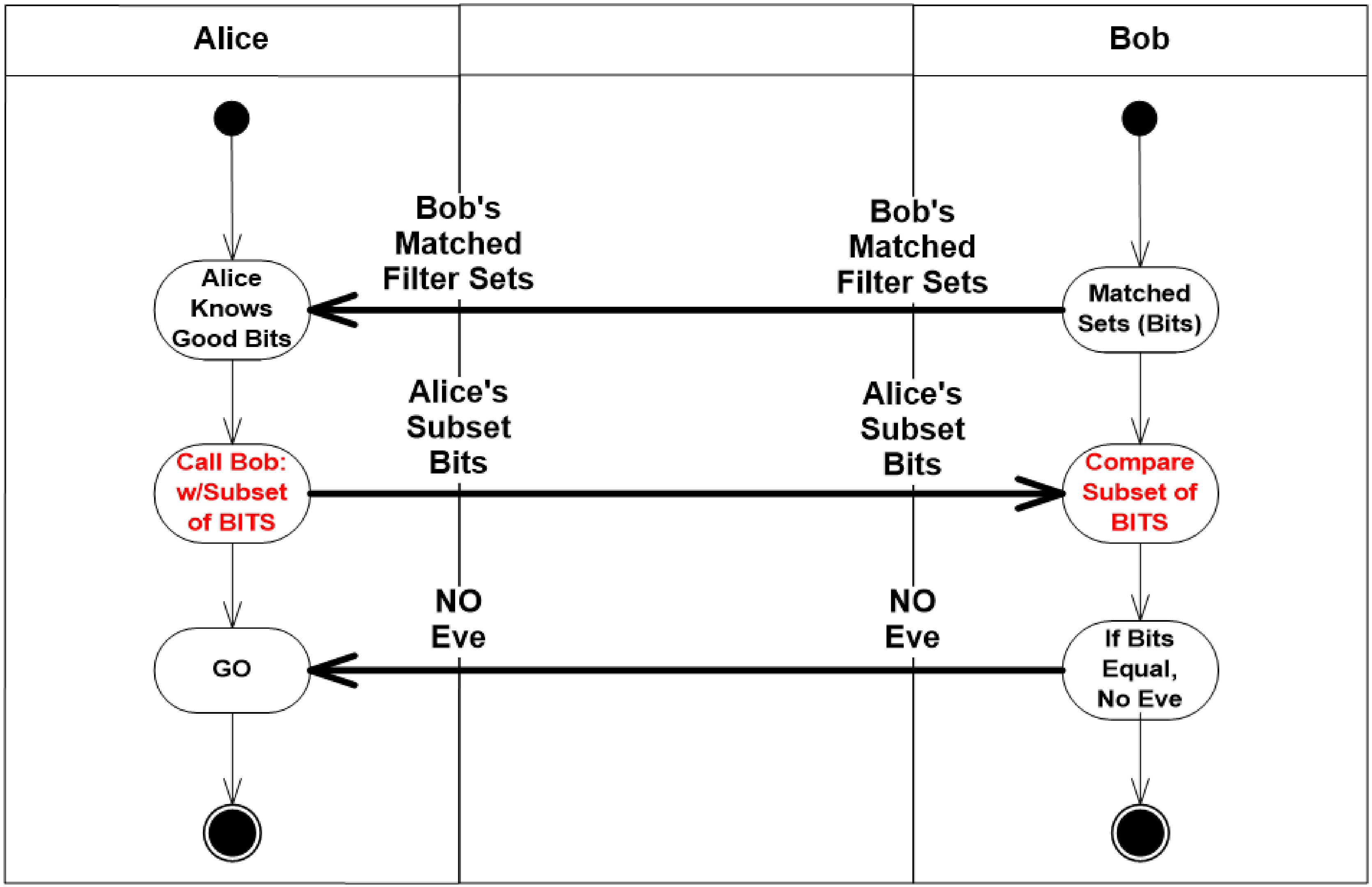
- **We can securely transmit an unbreakable one time pad (Symmetric Key) of any desired length.**
- **We can ALWAYS detect EVE eavesdropping.**

W/O Eve 1 of 2

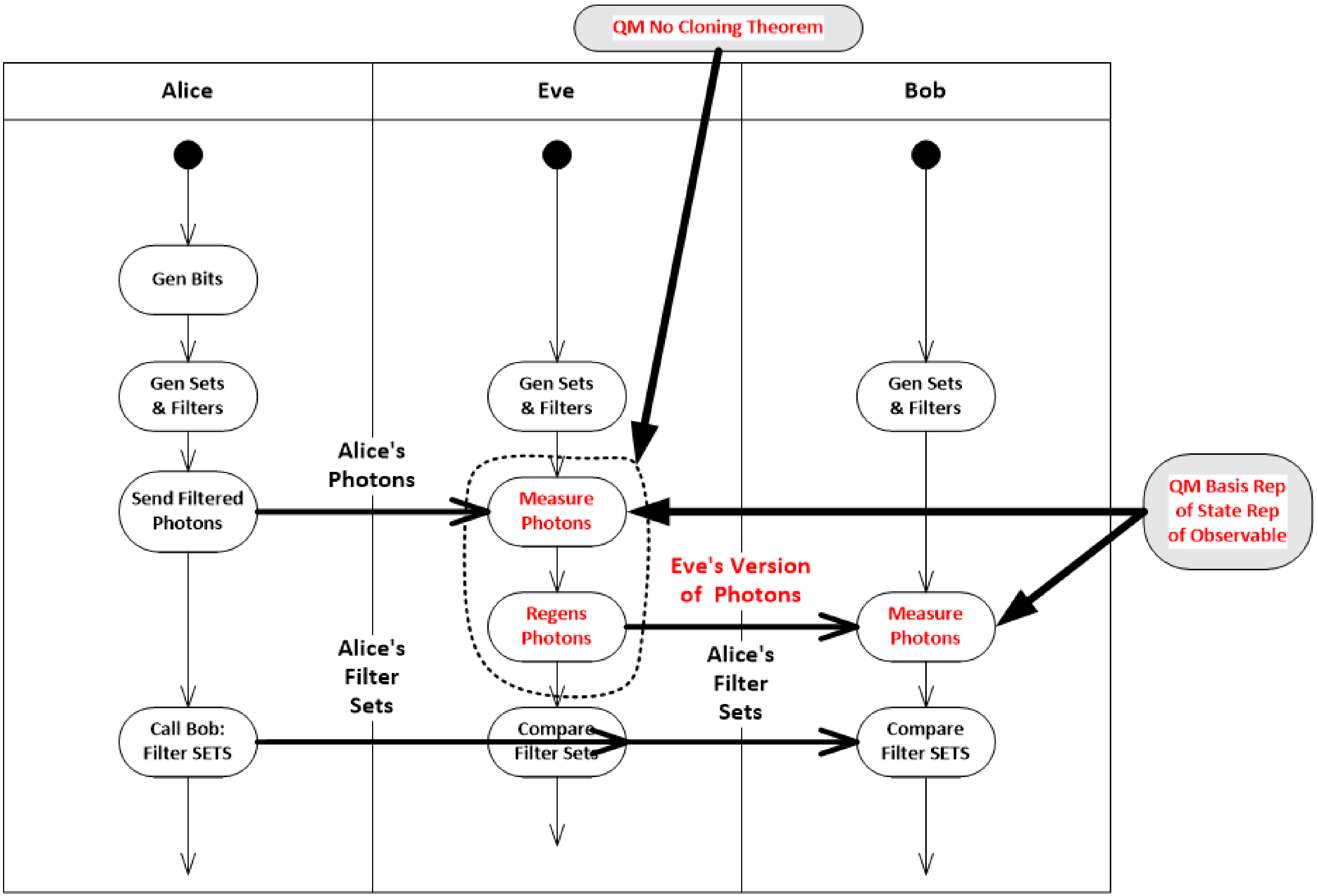

Alice
Bob
Gen Bits
Gen Sets & Filters
Send Filtered Photons
Call Bob: Filter SETS
Alice's Photons
Alice's Photons
Alice's Filter Sets
Alice's Filter Sets
Gen Sets & Filters
Measure Photons
Compare Filter SETS
QM Basis Rep of State Rep of Observable

10.

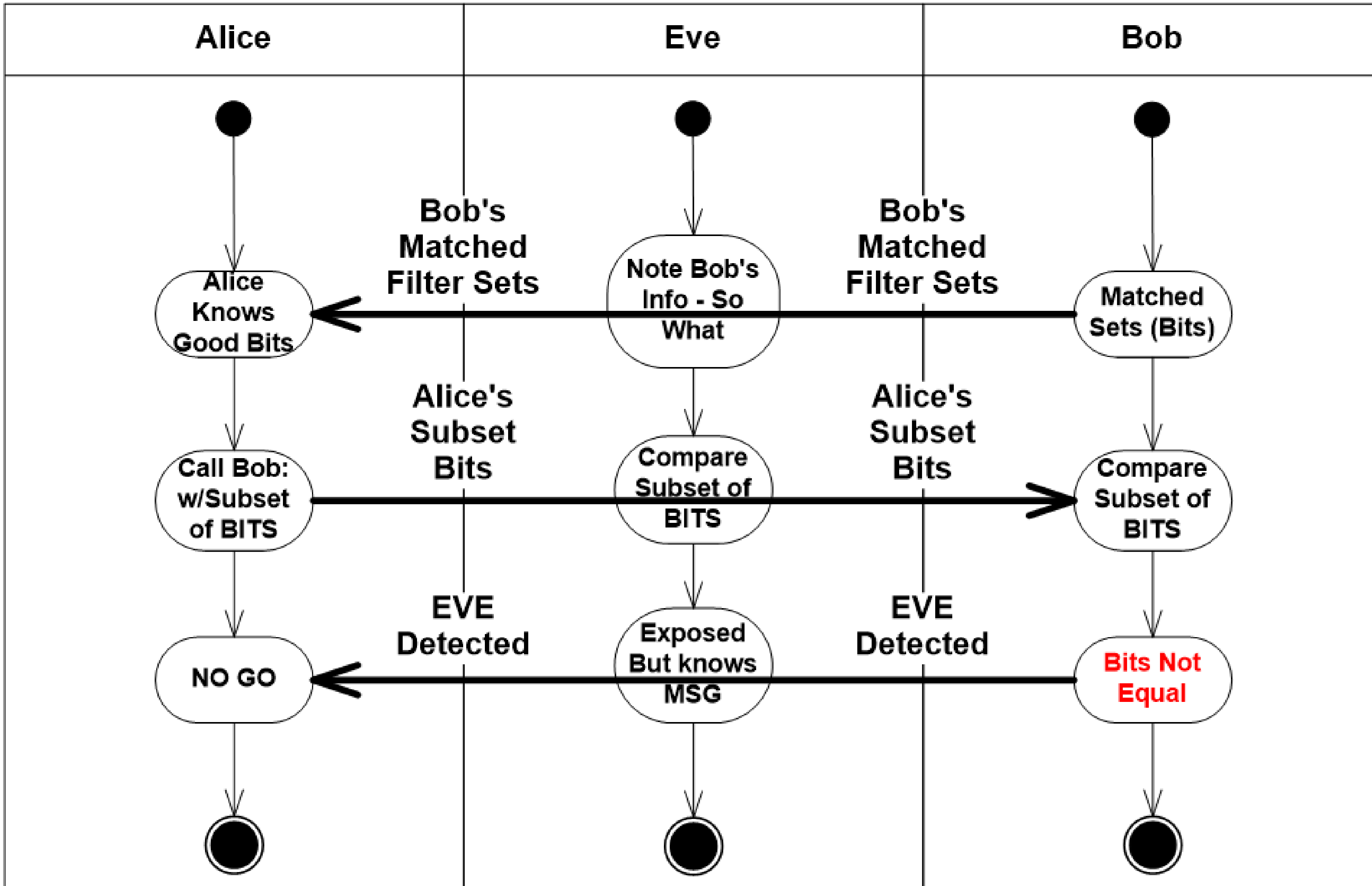
W/O Eve 2 of 2



W/Eve 1 of 2


QM No Cloning Theorem
Alice
Eve
Bob
Gen Bits
Gen Sets & Filters
Gen Sets & Filters
Gen Sets & Filters
Alice's Photons
Send Filtered Photons
Measure Photons
QM Basis Rep of State Rep of Observable
Eve's Version of Photons
Regens Photons
Measure Photons
Alice's Filter Sets
Alice's Filter Sets
Call Bob: Filter SETS
Compare Filter Sets
Compare Filter SETS

W/Eve 2 of 2


Alice
Eve
Bob
Bob's Matched Filter Sets
Bob's Matched Filter Sets
Alice Knows Good Bits
Note Bob's Info - So What
Matched Sets (Bits)
Alice's Subset Bits
Alice's Subset Bits
Call Bob: w/Subset of BITS
Compare Subset of BITS
Compare Subset of BITS
EVE Detected
EVE Detected
NO GO
Exposed But knows MSG
Bits Not Equal

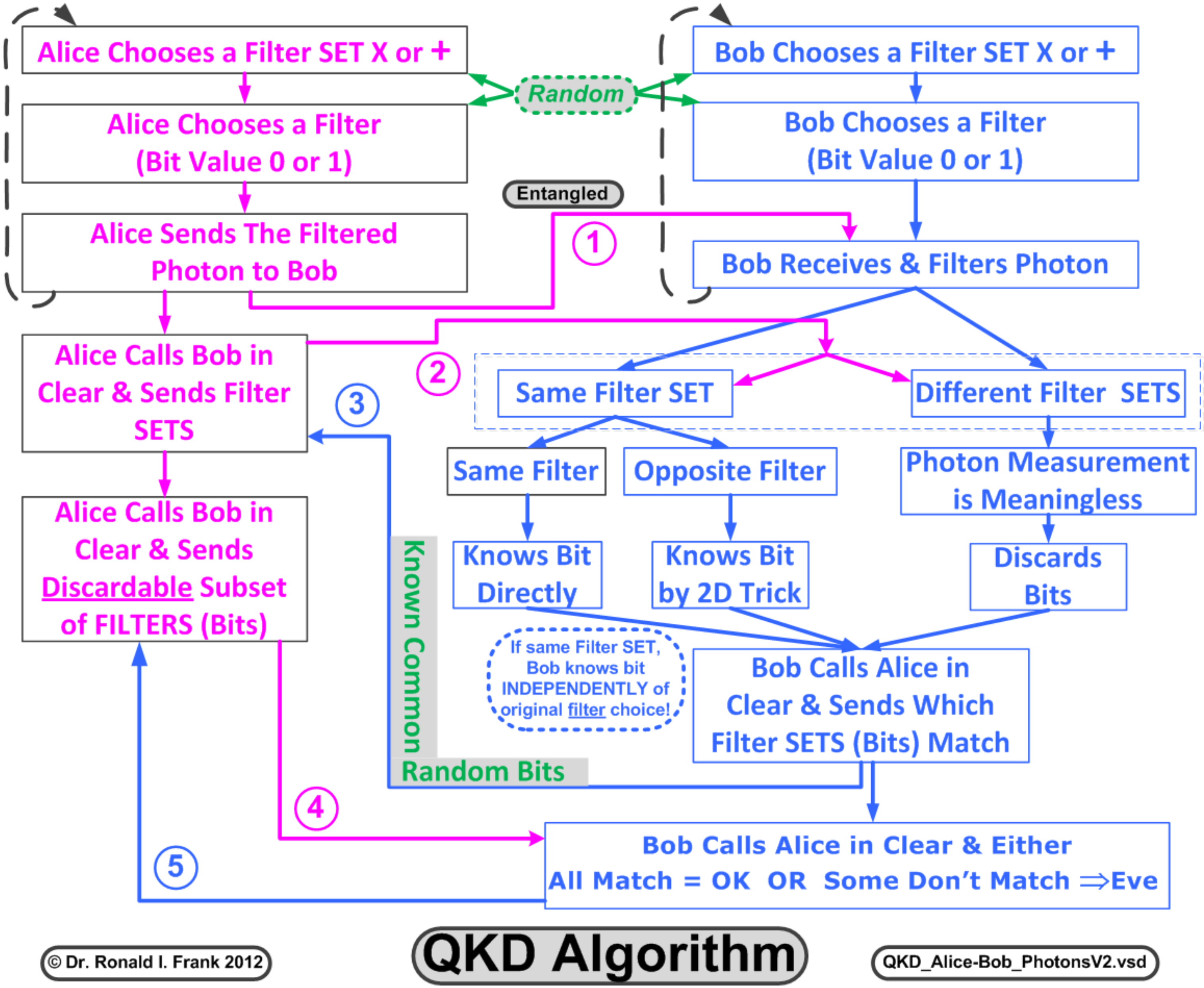
Quantum Key Distribution Algorithm

Alice sends N random bits (photons) using a random choice of N filters. Alice knows her bits and filters.

Entaglement Goes Here

1. **Bob uses a random choice of receiving filters**
   - **Bob knows his measured bits and filters**
   - **Some are errors because he chose the wrong filter**
   - **A bad filter gives a bit error 50% of the time**
   - **A good filter gives a correct bit 100% of the time**
2. **Alice calls Bob in the open and tells him HER Filter SETS**
3. **Bob tells Alice which of HIS SETS agree (M)**
   - **This determines a secret set of *M known bit values***
   - **This is a key for encryption - if no Eve**
5. **Alice calls Bob and reads to him a discardable subset of HER actual FILTERS (bits). If they agree there has been no Eve. Otherwise, there has been an Eve. DISCARD ALL!**

Singh, Simon. *The Code Book*.Anchor Books NY. ISBN 0-385-49532-3 (1999) PP. 339-344



Alice Chooses a Filter SET X or +
Alice Chooses a Filter (Bit Value 0 or 1)
Alice Sends The Filtered Photon to Bob
Random
Entangled
Bob Chooses a Filter SET X or +
Bob Chooses a Filter (Bit Value 0 or 1)
Bob Receives & Filters Photon
1
2
3
4
5
Alice Calls Bob in Clear & Sends Filter SETS
Same Filter SET
Different Filter SETS
Same Filter
Opposite Filter
Photon Measurement is Meaningless
Knows Bit Directly
Knows Bit by 2D Trick
Discards Bits
Alice Calls Bob in Clear & Sends Discardable Subset of FILTERS (Bits)
Known Common
Random Bits
If same Filter SET, Bob knows bit INDEPENDENTLY of original filter choice!
Bob Calls Alice in Clear & Sends Which Filter SETS (Bits) Match
Bob Calls Alice in Clear & Either
All Match = OK OR Some Don't Match ⇒Eve
© Dr. Ronald I. Frank 2012
QKD Algorithm
QKD_Alice-Bob_PhotonsV2.vsd

Quantum Key Distribution Results

1. **This leaves both with a long random bit string which is secret and has not been read by an Eve (P~1).**

2. **This bit string is used as a secure symmetric key for a one-time-pad.**

3. **The Navajo box generates new keys every 10 ms (100/sec).**

Quantum Key Distribution 1TP

One-time-pads are (classically) known (i.e., proven) Unbreakable (By Shannon).

Algorithm Results

We can securely transmit an unbreakable one time pad (Symmetric Key) of any desired length.

We can ALWAYS detect EVE eavesdropping.

Algorithm Uses [1/2]

We can use the quantum key to distribute secure encrypted messages.

We can use the quantum key to distribute classical Private Keys (as messages).

BORMING's Dissertation

Algorithm Uses [2/2]

We can use the quantum key to distribute classical messages with a secure digital signature

[Open text with encrypted hash of long message].

7. Quantum Key Distribution Bibliographies

Bibliographies

1. Quantum Economy
2. Quantum Computing
3. Polarization Demo Materials
4. QKD
   1/2
   2/2
5. IPSEC
6. RIF

Bibliography
(1. Quantum Economy)

Waite, Stephen R., 2002,
Quantum Investing. Thomson Texere.
ISBN 1-587-99140-3

(2. Quantum Computing)

Millburn, Gerard J., 1998, The Feynman Processor. Helix Books (Perseus Basic Books). ISBN 0-7382-0173-1.

{Layperson’s introduction to Quantum Entanglement & Quantum Computing/Computers. Also introduces the difference between classical probability and quantum probability – which defines the quantum domain.}

Bibliography
(2. Quantum Computing)

Gudder, Stan "Quantum Computation." The American Mathematical Monthly March 2003 # 110 pp. 181 – 201.

{Intro to QC for the mathematically prepared under grad.}

Johnson, George, 2003, A Short Cut Through Time. Alfred A. Knoph Pubs. ISBN 0-375-41193-3.

{Layperson's introduction to QC & QE. My choice for selected topic readings in QC in IS courses.}

Bibliography
(3. Polarization Demo Materials)

B & H, http://www.bhphotovideo.com/ 2004

{Search Binoculars & Scopes, 93608. ($29.95). This is a Celestron Polarizing Lens Filter Set containing two rotating polarizing lenses in a threaded lens housing.}

Edmund Industrial Optics, http://www.edmundoptics.com/ 2004

{Search KIT, then OPTICS DISCOVERY KIT ($17.95). This is an American Optical Society of America classroom experiments kit – ages 10 – adult.}

Edmund Scientifics, http://scientificsonline.com/ 2004

{Search 3038490, then POLARIZER EXPERIMENTERS KIT ($19.95)}

Bibliography (4. QKD) [1/2]

Nielsen, Michael A. and Isaac L. Chuang, 2000, Quantum Computation and Quantum Information. Cambridge University Press. ISBN 0-521-63503-9

{The definitive text on QE, QC and QI.}

{Possibly the most widely referenced textbook in QC, QI, and QE (encryption). It contains a review of QM for information people, the no cloning theorem, and the BB84 QKD protocol on which this presentation is based. }

Singh, Simon, 2002, The Code Book.
Anchor Books ISBN 0-385-49532-3

{Includes a layperson's chapter on modern QKD.
My choice for selected topic readings in QKD in IS courses.}

Bibliography (4. QKD) [2/2]

Tanenbaum, Andrew S. 2003, Computer Networks. Prentice Hall PTR. ISBN 0-13-066102-3
{Pp. 731 –734 Under One-Time Pads, Under Network Security}

Products for QKD

http://www.idquantique.com/ 2004, 2010

http://magiqtech.com/ 2004, 2010

http://www.quantiki.org/ 2010

Quantum Entanglement

The Age of Entanglement: When Quantum Physics Was Reborn, by Louisa Gilder. Knopf; 1 edition (11- 11-2008) ISBN-10: 1400044170 ISBN-13: 978-1400044177
{Lay historical discussion of personalities, events, and ideas. A super read.}

Bibliography (5. IPSEC)

- **IP Security Protocol (ipsec) [Home page]**
  http://www.ietf.org/html.charters/ipsec-charter.html

- **IPSEC Security Document Roadmap [1998]**
  http://www.ietf.org/rfc/rfc2411.txt

- **Security Architecture for the Internet Protocol [1998]**
  http://www.ietf.org/rfc/rfc2401.txt

- ***Internetworking with TCP/IP*** **by Douglas E. Comer. Vol. 1. 4th Ed. Prentice Hall (2000) ISBN 0-13-018380-6**

- **SSL is a Netscape de facto standard.**
  http://wp.netscape.com/eng/ssl3/

Bibliography (6. RIF)

- **Frank, R. I. (2003).**
  The Quantum Computing (QC), Quantum Encryption (QE), and Quantum Information (QI) Curriculum (Why? Now? Never?) ***Information Systems Education Journal, 1*** **(46). http://isedj.org/1/46/. ISSN: 1545-679X. (Also appears in *The Proceedings of ISECON 2003: §2132.* ISSN: 1542-7382.)**
  [Argument for 3 topics inclusion in the IS curriculum]

- **Frank, R. I. (2004).**
  An Outline of the Prerequisite Topics and Module for a Quantum Encryption (QE) Module in an IS Course. **Proceedings Americas Conference on Information Systems (AMCIS August 2004) (Security track) http://aisel.isworld.org/article_by_author.asp?Author_ID=5578 [Outline of an undergrad IS course component & prerequisites.]**

Bibliography (6. <u>RIF</u>)

- **Frank, R. I. (2005).**
  An IS Undergraduate Course Module on Quantum Key Distribution. *Information Systems Education Journal, 3* (33). http://isedj.org/3/33/. ISSN: 1545-679X. (Also appears in *The Proceedings of ISECON 2004: §2243.* ISSN: 1542-7382.)

  [Detail of an undergrad IS course component on QKD only.]

8. Appendix on Vector Algebra And Hermitian Inner product Spaces

WHY Vectors (Linear Algebra)?

The world can be effectively modelled by ***Objects*** that have ***Observable States*** with ***Measureable Values with given probability.***

States can be effectively modelled by ***vectors***.

Objects can be effectively modelled by ***Operators*** on ***vectors***.

Measureable values of the object can be effectively modelled by ***eigenvalues*** of the eigenvectors of the object.

WHY Vectors (Linear Algebra)?

He probability of finding the initial (before measurement) system in the final eigenstate i with measured eigenvalue i after measurement , can be effectively modelled as the square of the projection of the initial (before measurement) system vector onto the eigenvector i (found as the result of the measurement).

Vectors

Vectors

A set of thingies that ADD, and scalars (numbers) can multiply them. {Vector: +, • and Scalar: +,-,*,/}

Component Model $(x_1, y_1, z_1) \Rightarrow$ 3D

$(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_3, y_3, z_3) \Rightarrow$ component-wise addition

$s(x_1, y_1, z_1) = (sx_2, sy_2, sz_2) \Rightarrow$ component-wise scalar multiplication

Inner Product $(x_1, y_1, z_1) \bullet (x_2, y_2, z_2)$ = a scalar

vector/vector multiplication=$[x_1\, x_2, + y_1\, y_2, + z_1\, z_2]$

ADD (component-wise component multiplication)

Length $\{(x_1, y_1, z_1) \bullet (x_1, y_1, z_1)\}^{.5}$ = a scalar >=0

$\{x_1\, x_2, + y_1\, y_2, + z_1\, z_2\}^{.5}$ >=0

Vectors

1. A vector space is a collection of thingies that add ($\underline{u}=\underline{v}+\underline{w}$), associate $\underline{u}+(\underline{w}+\underline{z})=(\underline{u}+\underline{w})+\underline{z}$, have an identity ($\underline{u}+\underline{0} =\underline{u}$), an additive inverse ($-\underline{u}+\underline{u}=\underline{0}$), and commute (+) ($\underline{w}+\underline{z}$)=($\underline{z}+\underline{w}$).

2. There is also a field of scalars that multiply them: s$\underline{u}$. This is scalar multiplication. Scalars in QM are <u>complex #s</u>.

3. In addition to this scalar multiplication, there is a (vector • vector) multiplication called the <u>scalar product</u> (= the inner product = the dot product). It yields a <u>scalar</u> and is notated ($\underline{u}\cdot\underline{v}$) [“$\underline{u}$ dot $\underline{v}$”] or <u, y>.

Vectors

1. **A Basis of an (n-D) vector space is a set of n vectors which are:**
   a. **Linearly independent (Can't sum to one of them)**
      &
   b. **Span (generate) all vectors of the space**

2. **We can always find an orthonormal basis which are:**
   a. **Of length 1**
   b. **Mutually orthogonal.**

Vectors

"Hermitian" Inner Product.

1. $<-, ->$ [maps vectors to a scalar (COMPLEX NUMBER)]
2. $<\underline{u}+\underline{v}, \underline{w}> = <\underline{u}, \underline{w}> + <\underline{v}, \underline{w}>$ [$\underline{u}$, $\underline{v}$, $\underline{w}$ are vectors]
3. $<\underline{u}, \underline{v}+\underline{w}> = <\underline{u}, \underline{v}> + <\underline{u}, \underline{w}>$ Bi-Linear
4. $<s\underline{u}, \underline{v}> = s<\underline{u}, \underline{v}>$ [s is a COMPLEX NUMBER]
5. $<\underline{u}, s\underline{v}> = s^*<\underline{u}, \underline{v}>$ [* is COMPLEX CONJUGATION]
6. $<\underline{u}, \underline{v}> = <\underline{v}, \underline{u}>^*$ [Conjugate Symmetric]
7. $<\underline{u}, \underline{u}> = |\underline{u}|^2 \geq 0$ [= 0 iff $\underline{u} = \underline{0}$]

$<H\underline{u}, \underline{v}> = <\underline{u}, H^*\underline{v}> = <\underline{u}, H\underline{v}>$ [Hermitian Definition]

[Eric W. Weisstein et al. "Hermitian Inner Product." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/HermitianInnerProduct.html]

If $\underline{u}$ and $\underline{v}$ are real: $<\underline{u}, \underline{v}> = <\underline{v}, \underline{u}> = \text{def } (\underline{u}\cdot\underline{v})$

$\underline{u}\cdot\underline{v} = |\underline{u}|\,|\underline{v}|\cos(\text{angle between them})$.

Vectors

- $|\underline{u}| = (\underline{u} \cdot \underline{u}^*)^{.5}$ is a real number. "Length"
- **Hermitian** operators [H=H*] (* is conjugate transpose) map vectors to vectors in the vector space. $H\underline{u} = \underline{v}$.
- **Eigenvectors** ("ownvectors") of an operator H are those vectors that H maps into multiples of themselves. $H\underline{u}=\lambda\underline{u}$. If $|\underline{u}| =1$, λ is an **eigenvalue** of H associated with $\underline{u}$ [there can be more than one $\underline{u}$ for a given λ].
- *An Hermitian operator's eigenvalues are real.*
- An Hermitian operator's eigenvectors form a **basis** of the entire [Hermitian Vector] space.
- In a real inner product space the symmetric operators ($A=A^t$) are the Hermitian operators.

9. Appendix on Sin & Cos

Sin(nx) & Cos (nx) Form an Orthonormal Basis of an Infinite Dimensional Space (all n) and are the Eigenvectors of the Second Derivative Operator

$$\boxed{\frac{d^2(\ )}{dx^2}}$$

Mixed (n, m) sin(nx) / cos(mx) are orthogonal
Same (n = m) sin(nx) / cos(nx) are orthogonal

$$\boxed{\int_{-\pi}^{\pi} \cos(nx)\sin(mx)dx = 0}$$

Mixed (n, m) Sin(nx) / sin(mx) are orthogonal
Same (n = m) Sin(nx) / sin(nx) are normalizable

$$\int_{-\pi}^{\pi} \sin(nx)\sin(mx)dx = \pi\delta_{mn} \quad [m, n \geq 1]$$

$$i.e. \int_{-\pi}^{\pi} \sin^2(nx)dx = \pi \qquad [n \geq 1]$$

$$i.e. \int_{-\pi}^{\pi} \sin(nx)\sin(mx)dx = 0 \quad [m \neq n]$$

Mixed cos(nx) / cos(mx) are orthogonal Same cos(nx) / cos(nx) are normalizable

$$\int_{-\pi}^{\pi} \cos(nx)\cos(mx)dx = \pi\delta_{mn} \quad [m, n \geq 1]$$

$$i.e. \int_{-\pi}^{\pi} \cos^2(nx)dx = \pi \qquad [n \geq 1]$$

$$i.e. \int_{-\pi}^{\pi} \cos(nx)\cos(mx)dx = 0 \quad [m \neq n \ \& \ \geq 1]$$

cos(nx) & sin(nx) are Orthogonal to a constant (1).

$$\boxed{\int_{-\pi}^{\pi} (1)\sin(mx)dx = 0}$$

$$\boxed{\int_{-\pi}^{\pi} (1)\cos(nx)dx = 0}$$

<u>So What?</u>

Any

- **Continuous function f(x) on [-π, π]**
- **With only a <u>finite number</u>**
- **of**
- **<u>Finite</u> jump discontinuities**

Equals the infinite sum

$$\boxed{f(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos(nx) + \sum_{n=1}^{\infty} b_n \sin(nx)}$$

where

$$a_0 = \left(\frac{1}{\pi}\right)\int_{-\pi}^{\pi} f(x)dx = 0 \qquad P_1\left[f(x)\right] \qquad = \left\langle 1, f(x)\right\rangle$$

$$a_n = \left(\frac{1}{\pi}\right)\int_{-\pi}^{\pi} f(x)\cos(nx)dx = 0 \qquad P_{\cos(nx)}\left[f(x)\right] \qquad = \left\langle \cos(nx), f(x)\right\rangle$$

$$b_n = \left(\frac{1}{\pi}\right)\int_{-\pi}^{\pi} f(x)\sin(nx)dx = 0 \qquad P_{\sin(nx)}\left[f(x)\right] \qquad = \left\langle \sin(nx), f(x)\right\rangle$$

$$\boxed{\begin{array}{l}\sin(nx) = -\sin(-x) \Rightarrow \dfrac{d(\sin(nx))}{dx} = n\cos(nx) \Rightarrow \dfrac{d^2(\sin(nx))}{dx^2} = -n^2\sin(nx) \\ \cos(nx) = \cos(-nx) \Rightarrow \dfrac{d(\cos(nx))}{dx} = -n\sin(nx) \Rightarrow \dfrac{d^2(\cos(nx))}{dx^2} = -n^2\cos(nx)\end{array}}$$

$$\boxed{H(\bullet) \approx \frac{d^2(\bullet)}{dx^2} \Leftrightarrow H\begin{bmatrix}\sin(nx)\\ \cos(nx)\end{bmatrix} = \begin{bmatrix}-n^2\sin(nx)\\ -n^2\cos(nx)\end{bmatrix}}$$

Therefore sin & cos are the Eigenvectors of the Second Derivative Operator

----------------- o -----------------