"I need someone well versed in the art of torture—do you know PowerPoint?"

NYT 9/29/03 PG 97
Non Sequitur By Wiley Miller

AH-HA! THERE IT IS!!

HOW TO TELL YOUR POWERPOINT PRESENTATION NEEDS WORK

(C) Ronald I. Frank 2004, 2005
(V.9.)
QKD
Quantum Key Distribution
[Quantum Cryptography]

Dr. Ronald I. Frank      Pace University
rfrank@pace.edu

December 2005
(C) Ronald I. Frank 2004, 2005
(V.9.)
Outline - 1/2

0. TOC (Outline) [5-6]
1. Why Bother? (Current Problems) [7-8]
2. Why should we understand it? [9-15]
   • Where & Why is it used?
   • Who will use it?
3. QKD Current State [16]
4. Background (QM) [17-23]
5. Background (OTP, Vectors, Polarization, & Probability) [24-34]
Outline – 2/2

6. Background (QKD) [35-37]
7. Polarization Demo? [38]
8. What is QKD? [39-53]
9. Algorithm Results [54]
10. Algorithm Uses [55-56]
11. Simulator hands on? [57]
12. Q. & A. [58]
13. Bibliography [59-64]
1. Why Bother? (Current Problems)

• Current State of Network Encryption Usage

• Potential Weaknesses

• Therefore QKD
Current State of Network Encryption Usage

- DES ➔ AES (Symmetric all)
- PKI (Asymmetric – 2 key)
- IPSEC (Symmetric, AES)
- SSL (Negotiated – PKI/Symm)
2. 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 Can Break It!
Potential Weaknesses

• PKI Based on assumptions about factoring large numbers.
• Security of PKI Key Vault
• Security of $P_r$ Key Distribution
What is The Classical Key Distribution Problem?

- One-time-pads (1 key/1 message)
  - IT IS SYMMETRIC!
  - Key as long as message (K~M)
  - Vernam Cipher (XOR, ⊕)
  - ONLY Unbreakable Code
- If done right
  - The Key (PAD) Distribution Problem
Therefore QKD [1/2]

- Computation capability is increasing non-linearly
- Quantum Computers Promise to Completely Negate Efficacy of Current Encryption Technology (i.e., kill it dead) (not imminent)
Therefore QKD [2/2]

- **QKD is Based On Physics**
- **Unaffected By Either**
  - **Current Computer Technology**
  - or
  - **QUANTUM COMPUTING CAPABILITY**
QKD SOLVES THE KEY DISTRIBUTION PROBLEM

• It is a handshake protocol
• It can sense Eve \((Alice, Eve, Bob)\)
• Use classical or Q-encryption

Thereafter
More Secure Data Transmission

- QKD Used For:
  - IPSEC (for Internet) (& SSL)
  - Replace PKI, AES
  - It is a Vernam One-Time-Pad (~Break!)
  - Solves the key distribution problem

Summary: So What?
3. Current State

- **QKD**
  - There are products that do it (100 + km distances)
  - Open air QE coming to a satellite near you

- **QKD Education**
  - QE appearing in CS texts [Tanenbaum’s Networking]

- **Cultural Motivation to Learn**
  - 30% GDP derives from QM [Waite, Stephen R., 2002]
4. QM Background [1/7]

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

2. There is also a field of scalars that multiply them: \(ku \Rightarrow (|k||u|)\). This is scalar multiplication. Scalars here are complex #s.

3. In addition to this scalar multiplication, there is a vector·vector multiplication called the scalar product, the inner product, or the dot product. It yields a scalar and is notated \(u \cdot v\) \[“u dot v”\].
QM Background [2/7]

"Hermitian" Inner Product.

3. a. $\langle -, - \rangle$ [maps to vectors to a scalar (COMPLEX NUMBER)]
3. b. $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$ [ $u, v, w$ are vectors]
3. c. $\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle$
3. d. $\langle au, v \rangle = a \langle u, v \rangle$ [ $a$ is a COMPLEX NUMBER]
3. e. $\langle u, av \rangle = a^* \langle u, v \rangle$ [* is COMPLEX CONJUGATION]
3. f. $\langle u, v \rangle = \langle v, u \rangle^*$ [* is COMPLEX CONJUGATION]
3. g. $\langle u, u \rangle = |u|^2 \geq 0$ [= 0 iff $u = 0$]


If $u$ and $v$ are real: $\langle u, v \rangle = \langle v, u \rangle = \text{def} \ (u \cdot v)$

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

(C) Ronald I. Frank 2004, 2005
(V.9.)
4. $|\mathbf{u}| = (\mathbf{u} \cdot \mathbf{u}^*)^{1/2}$ is a real number.

5. **Hermitian operators** $[H=H^*]$ map vectors to vectors in the vector space. $H \mathbf{u} = \mathbf{v}$.

6. **Eigenvectors** (“ownvectors”) of an operator $H$ are those vectors that $H$ maps into multiples of themselves. $H \mathbf{u} = \lambda \mathbf{u}$. If $|\mathbf{u}| = 1$, $\lambda$ is an eigenvalue of $H$ associated with $\mathbf{u}$ [there can be more than one $\mathbf{u}$ for a given $\lambda$].

7. An Hermitian operator’s eigenvalues are real.

8. An Hermitian operator’s eigenvectors form a basis of the entire [Hermitian Vector] space.

9. In a real inner product space the symmetric operators ($A=A^t$) are the hermitian operators.
Why “EIGEN”? 

Let \( \mathbf{u}_i \) be the eigen vectors of \( H \) and 

Let \( \lambda_i \) be the corresponding eigen values. 

Then 

\[
H = \sum \lambda_i (\mathbf{u}_i \mathbf{u}_i^*)
\]

Notice that \( (\mathbf{u}_i \mathbf{u}_i^*) \) acts as a projector operator onto \( \mathbf{u}_i \).
Quantum Mechanics is “just” modeling a physical system by a Hermitian vector space.

- **Measurable Quantity** → **Hermitian Operator**
- **Measured Value** → **Eigenvalue**
- **Measured State** → **Eigenvector**
- **Gen. System States** → **Eigenvector Combination**
- **Probability of Value** → \((\text{Length})^2\) of projection on resultant eigenvector

[All states = length 1, all eigenvalues real]
QM Background [6/7]

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 **unknown** 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.
5. The \((\text{length})^2\) of the projected unit mixed state vector is the \text{PROBABILITY} of finding that Pure State in any given measurement.

6. All Basis Vectors are actually \text{eigenvectors} of the \text{operator} representing the measured quantity.

7. The \text{value of the eigenvalue} corresponding to the pure state is the \text{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.
5. Background (B.) (OTP, Vectors, Polarization, & Probability)

B. 1 One-time-pads (OTP)

B. 2 2-D Vector Uses

B. 2.1 Components as Projections

B. 3 Polarization of Light

B. 3.1 Polarized Photons

B. 3.2 Filtered Photons Have P=1

B. 4 Discrete Probability (Definition)

Addition (OR)

*Multiplication* (AND)
B. 1 One-time-pads (OTP)

- QE is to used create a shared key for a OTP
- The OTP is used to send an encrypted message
- This is done many time/sec (>100)
B. 2  2-D Vector Uses

- A photon state is a **unit** ‘vector’ \(\uparrow, \downarrow, \leftrightarrow, \rightarrow\), or \(\leftarrow\).  
  [We take only the ray not the direction]

- \(\{\uparrow, \downarrow\}\) are a **basis** of the 2-D space

- \(\{\leftarrow, \rightarrow\}\) are also a **basis** of the 2-D space

- These are also the 4 filters **directions** we use

- A photon in a state in one basis is represented
  - as a sum in the other basis
  - with projected lengths = \(1\cos(45^\circ)\)
  - giving \(1\cos^2(45^\circ) = .5\) as probabilities
B. 2.1 Components as Projections

$|w| = 1$ Means

$\alpha_1 = \cos(\theta)$

$\alpha_2 = \sin(\theta)$

$\theta = 45^\circ$

$\sin(45^\circ) = \cos(45^\circ)$

$= 1/\sqrt{2}$

$[\cos(45^\circ)]^2 = 1/2 = .5$

$\alpha_1 = |1||w|\cos(\theta)$
### B. 3 Polarization of Light

- A photon state is a unit of light.
- A photon can be polarized along a direction.
- A photon can be polarized by a filter.

#### Once polarized by a filter *(QM Think)*
- it passes through that filter \( p = 100\% \)
- it is blocked by a filter at \( 90^\circ \) \( p = 0 \% \)
- it passes a \( (45^\circ) \) filter \textbf{BUT}
  - it becomes \( (45^\circ) \) polarized
    - there is a 50\% chance of being one
    - there is a 50\% chance of being other
B. 3.1 Polarized Photons

A UNIT basis vector represented in a Second, 45° rotated basis has projection² = .5 on EITHER second-basis direction.

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

\[ \theta = \frac{\pi}{4} \]

\[ \theta = \frac{\pi}{4} \]

\[ \theta = \frac{\pi}{4} \]

\[ \theta = \frac{\pi}{4} \]

Horizontal = 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:

\[ \theta = \frac{\pi}{4} \]

Signs don't matter because we square lengths.

B. 3.1 Rotated Basis

\[ p = 0.5 = \cos(45^\circ)^2 \]

(C) Ronald I. Frank 2004, 2005

(V.9.)
B. 3.2

Filtered Photons Have P=1

They lie along the filter direction so:
\[ \cos(0^\circ)^2 = 1^2 = 1 = P. \]

OR

\[ \cos(180^\circ)^2 = (-1)^2 = 1 = P. \]
B. 3.2 Filtered Photons Have p=1

Filtered Photons Pass THE SAME FILTER With P = 1

The Photon Polarization Is Parallel To The Filter Axis

\[
\cos(0) = \cos(\pi) = \pm 1
\]

\[
P = \cos^2(0) = \cos^2(\pi)
\]

\[
P = (\pm 1)^2 = |\pm 1|^2 = 1
\]

Filtered Photons Pass The Other Filter of the Set With P = 0

The Photon Polarization Is Orthogonal To That Filter Axis

\[
\cos\left(\frac{\pi}{2}\right) = 0 \text{ and } \cos\left(-\frac{\pi}{2}\right) = 0
\]

\[
P = \cos^2\left(\pm \frac{\pi}{2}\right) = 0^2 = 0
\]
B. 4 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 $k = p_j + p_k$
6. QKD Background [1/3]

1. The whole purpose of the QKD algorithm is to find a secure OTP (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 + & × because that is what they look like.
   - They are rotated relative to each other by 45° TRICK!!! TRICK!!! TRICK!!!
QKD 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).

- Polarized **Photon State** Vectors
  - A state of vertical polarization is notated
  - A state of horizontal polarization is notated
  - A state of 45° right polarization is notated
  - A state of 45° left polarization is notated

  [We really want only the ray not the direction since signs don’t count because we square lengths]
We chose one state from each basis pair to represent a 1 bit (the other of the pair is the 0 bit) TRICK

\[
\begin{align*}
|\uparrow\downarrow\rangle & \equiv 1, & |\leftrightarrow\rangle & \equiv 0 \\
|\downarrow\uparrow\rangle & \equiv 1, & |\leftarrow\rightarrow\rangle & \equiv 0
\end{align*}
\]
7. Polarization Demo

See the bibliography for sources of demo equipment
8. What is QKD?

See the bibliography for sources
Quantum Encryption Algor.

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

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 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 (bits). If they agree there has been no Eve. Otherwise, there has been an Eve. DISCARD ALL!


(C) Ronald I. Frank 2004, 2005

(V.9.)
Discussion [1/5]

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 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.
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 ($\frac{1}{2}$).

The chance of picking N matching filters to Alice’s hidden choices is ($\frac{1}{2}$)$^N$ [the AND case]. ($\frac{1}{2}$)$^N$ 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.
Individual Photon Polarization Measurement is a Quantum Process

Knowing that the wrong basis gives either result with $p = 0.5$ (therefore no knowledge) is a quantum result.

Knowing that $p = 0.5$ because of the probability law of mixed state projections in $45^\circ$ 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.
Any attempt to read an unknown (mixed) photon and pass it on will introduce a probabilistic error.

This 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.
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.]
Quantum Encryption Algorithm Summary

Quantum Encryption Results

Quantum Encryption 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.
Alice
- Gen Bits
- Gen Sets & Filters
- Send Filtered Photons
- Call Bob: Filter SETS

Bob
- Gen Sets & Filters
- Measure Photons

Alice's Photons
- Alice's Filter Sets

Compare Filter SETS

Send Filtered Photons

Alice's Photons
- Alice's Filter Sets

Compare Filter SETS

QM Basis Rep of State Rep of Observable
Alice

- Alice Knows Good Bits
- Call Bob: w/Subset of BITS
  - Bob's Matched FilterSets
    - Alice's Subset Bits
      - NO Eve
      - GO
  - Alice's Subset Bits
    - NO Eve
    - If Bits Equal, NoEve

Bob

- Matched Sets (Bits)
- Compare Subset of BITS
  - Bob's Matched FilterSets

(C) Ronald I. Frank 2004, 2005
(V.9.)
W/ Eve 1 of 2

<table>
<thead>
<tr>
<th>Alice</th>
<th>Eve</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gen Bits</td>
<td>Gen Sets &amp; Filters</td>
<td>Gen Sets &amp; Filters</td>
</tr>
<tr>
<td>Gen Sets &amp; Filters</td>
<td>Gen Sets &amp; Filters</td>
<td>Gen Sets &amp; Filters</td>
</tr>
<tr>
<td>Send Filtered Photons</td>
<td>Measure Photons</td>
<td>Regens Photons</td>
</tr>
<tr>
<td>Alice's Filter Sets</td>
<td>Compare Filter Sets</td>
<td>Compare Filter SETS</td>
</tr>
<tr>
<td>Call Bob: Filter SETS</td>
<td>Compare Filter Sets</td>
<td>Compare Filter SETS</td>
</tr>
</tbody>
</table>

Alice's version of Photons

Eve's Version of Photons

QM Basis Rep of State Rep of Observable

QM No Cloning Theorem

December 2005

(C) Ronald I. Frank 2004, 2005 (V.9.)
Note Bob’s Info - So What

Call Bob: w/Subset of BITS

Alice Knows Good Bits

Matched Filter Sets

Bob's Matched Filter Sets

Bob's Matched Filter Sets

Matched Sets (Bits)

Alice's Subset Bits

Compare Subset of BITS

Compare Subset of BITS

Bob's Filter Sets

Alice's Subset Bits

NO GO

EVE Detected

Exposed

EVE Detected

Bits Not Equal

(C) Ronald I. Frank 2004, 2005
(V.9.)
Quantum Encryption Algor.

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

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 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!


December 2005

(C) Ronald I. Frank 2004, 2005

(V.9.)
Quantum Encryption Results

1. This leaves 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 Encryption OTP

One-time-pads are (classically) known (i.e., proven) unbreakable.
9. Algorithm Results

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

We can ALWAYS detect EVE eavesdropping.
10. 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).
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].
11. Simulator hands on.

Simulator Demo

See me for Java Code
12. Q. & A.
13. Bibliography (RLF)

- **ISECON 2003 (ISEDJ)**

- **AMCIS 2003**
  [http://aisel.isworld.org/article_by_author.asp?Author_ID=5578](http://aisel.isworld.org/article_by_author.asp?Author_ID=5578)
Bibliography
(Quantum Economy)

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


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


{Layperson’s introduction to QC & QE. My choice for selected topic readings in QC in IS courses.}
Bibliography
(Polarization Demo Materials)

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

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

{Search 3038490, then POLARIZER EXPERIMENTERS KIT
($19.95)}
Bibliography (QKD) 1/2


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


{Includes a layperson’s chapter on modern QE. My choice for selected topic readings in QKD & Cryptography in IS courses.}
Bibliography (QKD) 2/2


Products for QKD

Bibliography (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.

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