ISSN: 1545-679X

Information Systems Education Journal

Volume 3, Number 33 http://isedj.org/3/33/ August 6, 2005

In this issue:

An IS Undergraduate Course Module on Quantum Key Distribution

Ronald I. Frank
Pace University
Pleasantville, NY 10570 USA

Abstract: Quantum Key Distribution (QKD) is the use of quantum phenomena to create and distribute secure random symmetric private one-time keys (random bit strings) used for encrypting and decrypting messages. The encryption using these keys is known to be unbreakable even classically. QKD encryption is also called Quantum Encryption (QE). There are products on the market doing this today. DARPA is funding the use of QKD to replace IPSEC on the internet. QKD overcomes the only weakness of classical unbreakable one-time pads - the secure distribution of the pads themselves. Encryption is used for transmitting data securely. In previous papers I have proposed an IS course module covering QE, and I have discussed where it would fit into the IS curriculum. I have analyzed and presented an outline on the prerequisites for such an IS course module and provided an advanced tutorial for faculty or graduate students. This paper is my suggestion, in some detail, for such a module for undergraduate students. I simplify the presentation so that undergraduate IS students ought to be able to follow the discussion. They need only some remembrance of high school algebra. The relevant physics is presented in a purely descriptive form. Appendices contain the QKD (QE) algorithm in UML-like diagrams. This module should be teachable in two one-hour lectures. Due to space limitations, I have left out appendices on the Vernam one-time-pad, and a typical simulation run output which should be part of the module.

Keywords: quantum encryption, quantum cryptography, quantum key distribution, IS curriculum

---

Recommended Citation: Frank (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.)

This issue is on the Internet at **http://isedj.org/3/33/**

The **Information Systems Education Journal** (ISEDJ) is a peer-reviewed academic journal published by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP, Chicago, Illinois). • ISSN: 1545-679X. • First issue: 8 Sep 2003. • Title: Information Systems Education Journal. Variants: IS Education Journal; ISEDJ. • Physical format: online. • Publishing frequency: irregular; as each article is approved, it is published immediately and constitutes a complete separate issue of the current volume. • Single issue price: free. • Subscription address: subscribe@isedj.org. • Subscription price: free. • Electronic access: http://isedj.org/ • Contact person: Don Colton (editor@isedj.org)

EDSIG activities include the publication of ISEDJ, the organization and execution of the annual ISECON conference held each fall, the publication of the Journal of Information Systems Education (JISE), and the designation and honoring of an IS Educator of the Year. • The Foundation for Information Technology Education has been the key sponsor of ISECON over the years. • The Association for Information Technology Professionals (AITP) provides the corporate umbrella under which EDSIG operates.

An IS Undergraduate Course Module on Quantum Key Distribution (QKD) [Quantum Encryption (QE)]

Ronald I. Frank
rfrank@pace.edu
IS Department Pace University
Pleasantville, NY 10570 USA

Abstract

Quantum Key Distribution (QKD) is the use of quantum phenomena to create and distribute secure random symmetric private one-time keys (random bit strings) used for encrypting and decrypting messages. The encryption using these keys is known to be unbreakable even classically. QKD encryption is also called Quantum Encryption (QE). There are products on the market doing this today. DARPA is funding the use of QKD to replace IPSEC on the internet. QKD overcomes the only weakness of classical unbreakable one-time pads – the secure distribution of the pads themselves. Encryption is used for transmitting data securely.

In previous papers I have proposed an IS course module covering QE, and I have discussed where it would fit into the IS curriculum. I have analyzed and presented an outline on the prerequisites for such an IS course module and provided an advanced tutorial for faculty or graduate students. This paper is my suggestion, in some detail, for such a module for undergraduate students. I simplify the presentation so that undergraduate IS students ought to be able to follow the discussion. They need only some remembrance of high school algebra. The relevant physics is presented in a purely descriptive form. Appendices contain the QKD (QE) algorithm in UML-like diagrams. This module should be teachable in two one-hour lectures. Due to space limitations, I have left out appendices on the Vernam one-time-pad, and a typical simulation run output which should be part of the module.

Keywords: Quantum encryption, Quantum cryptography, Quantum key distribution, IS curriculum

1. INTRODUCTION

Quantum Key Distribution (QKD) is the use of quantum phenomena to create and distribute unbreakable symmetric one-time keys (random bit strings) which are used for classical message encrypting and decrypting. This is also called Quantum Encryption (QE). There are products on the market doing this today. See http://www.idquantique.com/qkd.html

Figure 1. QKD Boxes from Idquantique

DARPA is funding an effort at Harvad, BU, and BBN which will is prototyping a QKD network that could effectively replace IPSEC on the Internet [BBN 2004]. This is very much in the spirit of the original DARPA – BBN effort leading to the first routers and email.

The argument for QKD (BBN 2004) in outline, is that the current crypto schemes are built on unproved assumptions about the difficulty of certain mathematical factoring problems. Also, as quantum computing comes online, it will effectively break those codes (BBN 2004), (Johnson, George, 2003). So now is the time to develop and deploy more robust transmission security measures – before they become absolutely necessary. Some critical government and finance applications need this added robustness today.

In previous papers I have proposed and argued for an IS course module on QE for the IS curriculum and discussed where it would be placed (Frank 2003). I have analyzed and presented an outline on the prerequisites for such an IS course module and provided an advanced tutorial for faculty or advanced students (Frank 2004). This paper is my suggestion for a simplified version of such a module for undergraduate students. I am trying to simplify the module preparation process by giving this example.

I simplify the presentation so that undergraduate IS students ought to be able to follow the discussion. Appendices contain the algorithm in diagrams, and a review of the Vernam one-time pad. I choose one of the simpler algorithmic descriptions and leave out all advanced issues such as error correcting codes and advanced probability analysis since they are neither needed nor desirable at this level. The basic physical ideas are accessible to our students.

Students need only some remembrance of basic algebra and no trig. The trig needed is introduced here. The quantum and other physics "stuff" is self contained and of independent cultural interest.

Independently of QKD, there is an important reason for learning something about the applications of quantum mechanics. About 1/3 of our gross domestic product comes from quantum phenomena, and this will only grow in the future (Waite 2002).

The most robust (unbreakable) encryption method is based on Quantum Encryption/QKD (Johnson 2003), (Singh, 2002), (Nielsen and Chuang, 2000), (ArXiv.org, 2004) and (Tanenbaum, 2003). Products using this method are available on the open market (IdQuantique.com, 2004), and (MagiqTech,com 2004). They create absolutely secure one-time keys at 100b/sec. and send them in fiber up to 60 miles.

The basic QKD ideas I introduce are quantum system state, light polarization, and a peculiarity of system measurement in the quantum domain – the "No Cloning" theorem. This is all in a context of basic probability. For those who want a complete presentation of these topics see (Messiah, 1999) or (Nielsen and Chuang, 2000).

I first give a short statement of the probability facts I will use. Then I review polarization (sunglasses/telescopes). I proceed to simple two dimensional vectors, bases, and components, including projections and the cosine of an angle.

I connect these latter topics with polarization by using the direction of a linear polarization filter applied to photons. The filter polarizes the photons in a fixed direction. The direction of polarization is used as a two dimensional quantum state vector which lies in the plane perpendicular to the light's propagation.

By adding a quantum axiom – *the quantum state is represented as a vector* (here a two dimensional vector of polarization) we can apply the No Cloning theorem (states can't be copied). This then is all that is required to present and understand the QKD algorithm, in a simplified form, used in current products.

2. PROBABILITY

A discrete probability measure is a set of weights $\{p_i\}$ associated with events i and k, that has these properties:

1) For all i $\boxed{0 \le p_i \le 1}$ (0.1)
   [Positivity]
2) and $\boxed{\sum_i p_i = 1}$ (0.2)
   [Normalization]
3) They combine as follows:
   a. The probability of i and k: $\boxed{P(i\ and\ k) = p_i p_k}$ (0.3)
   [Joint occurrence law]
   b. The probability of i or k: $\boxed{P(i\ or\ k) = p_i + p_k}$ (0.4).
   [Disjoint occurrence law]

Later (optionally) we see the binomial distribution and its application to Bernoulli Trials. This is not a central point so it should be skipped. It is not a proper part of the actual algorithm. I use it only for a heuristic when discussing the probability of Bob choosing filter that match Alice's choices or Eve choosing filters that match Alice's.. Bayesian analysis is also not applicable here.

3. POLARIZATION OF LIGHT

Light is made up of two fields: the electric field and the magnetic field. See (Mathpages.com 2004). The two fields propagate together in a given direction (our old friend the light ray). The fields oscillate in a sine like pattern perpendicular to the direction of propagation. The magnetic field is always at a right angle to the electric field, so our first simplification is that we will consider only the electric field. If we know the electric field, we know where the magnetic field is: it is at right angles to the electric field!

There is one complication. The electric field (and its associated magnetic field) is rotating around the direction of propagation as it progresses. A Polaroid lens coating of our sunglasses (for an added $50 fee/lens!) allows through only the light (photons) whose fields are lined up with the direction (axis) of polarization of the lens (usually chosen to minimize the glare coming off water and metal surfaces). This reduces the amount of light but it also reduces the glare since glare is itself polarized and the lenses are chosen with an axis of polarization perpendicular to the usual direction of reflected water glare and glare reflected off metal surfaces.

Light (the combined electromagnetic field) is quantized into photons at the quantum level. We can think of the photons as having the oscillating behavior of the field and of having the ability to be modified by a

filter so that they only oscillate in parallel to the filter axis. That is: a photon which oscillates in parallel to the axis of a polarizing filter will pass through it unchanged, a photon oscillating at right angles to the filter axis gets totally blocked. A photon oscillating at an angle to the filter axis gets through, as we will see below, with a probability equal to the square of the cosine of the angle between the filter axis and the photon's oscillation (a positive number between 0 and 1).

A typical macroscopic experiment puts two polarizing filters in tandem. The first lets through light with a certain direction (mostly). If the second filter's polarization axis is parallel to the first we get a bright beam coming through.

If they have axes at right angles we see almost no light coming through. As we turn the filters relative to each other, the transmitted scene lightens and then darkens again as the square of the cosine of the angle between their axes. Later we see this as a probability of transmission of photons.

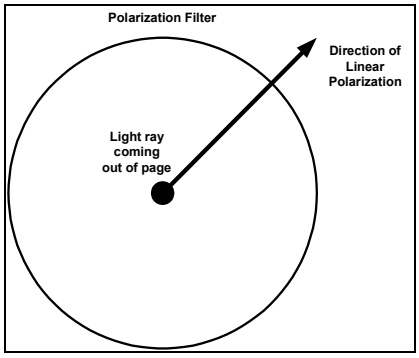


Figure 2. Planar filter **(/),** linear polarization.

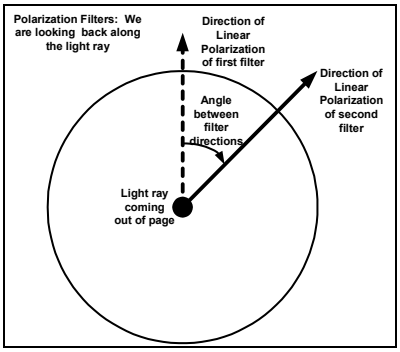


Figure 3. Tandem planar linear polarizing filters, **(|)** and **(/),** viewed from straight on.

Classroom Demonstrations
Effective and quick demos of polarization can be done using a classroom-lecture laser pointer and any inexpensive optics kit listed in the references. (B&H, Edmund Industrial Optics, Edmund Scientifics – all 2004)

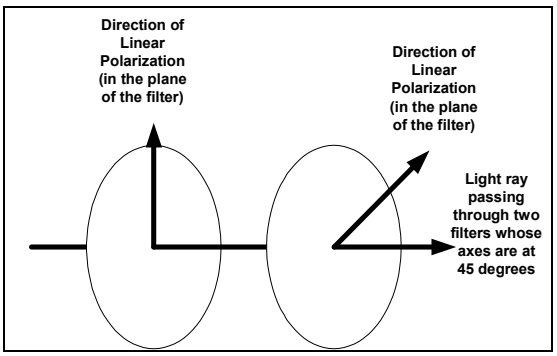


Figure 4. Tandem planar linear polarization filters, **(|)** and **(/),** viewed from an angle.

4. COSINE OF AN ANGLE

The cosine of an angle is defined as in this diagram: (adjacent side divided by hypotenuse).

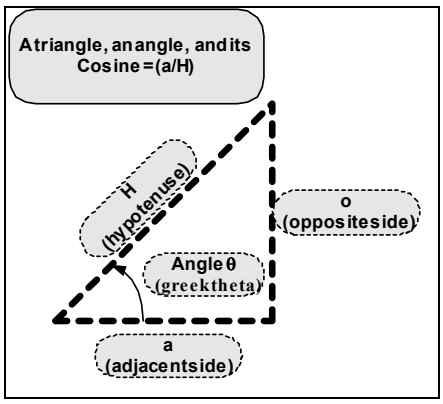


Figure 5. The definition of cosine

$$\cos(\theta) = \left(\frac{a}{H}\right) \tag{4.1}$$

5. TWO DIMENSIONAL VECTORS

Vector
A vector is defined as length and direction.

Basis
We usually pick N vectors of length 1 in an N dimensional space, place them at the origin (picked arbitrarily), pointing in mutually perpendicular (orthogonal) directions, and call them a basis.
There can be many bases. A 2-D basis could consist of any two non-parallel vectors. Any other vector can be written out as a sum of the two basis vectors. Unit length orthogonal bases make the sum simpler to figure out.

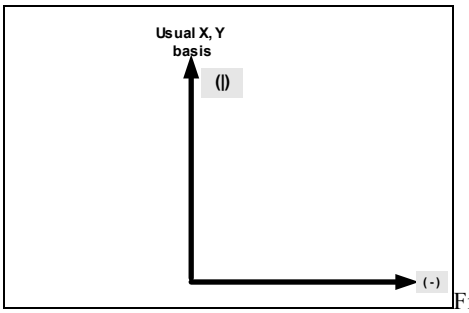


Figure 6. The usual 2-D Basis Vectors have length 1 **(–)** and **(|)**

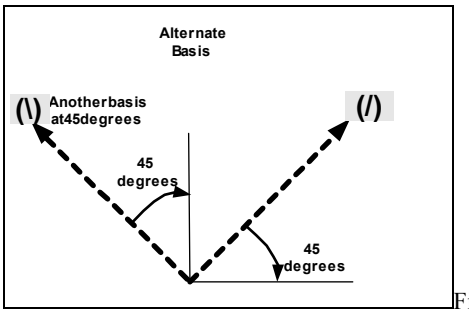


Figure 7. Another unit orthogonal basis **(/)** and **(\ )**

Components
An arbitrary vector (arbitrary direction and length) can be written as a weighted sum of the two basis vectors [remember we are limiting ourselves to a two dimensional space].

The arbitrary vector is the sum of two vectors, each in the direction of one of the basis directions. These are its components.

Coordinates in a basis
Given a basis: coordinates are the *lengths* of the components in that basis. The co-ordinates of the basis vectors themselves are the two pairs: (1,0) and (0,1). The coordinates are the length of the orthogonal (perpendicular) projections of the vector onto the basis vectors.

Orthogonal projections
Finding an orthogonal projection length is just finding the cosine of an angle.

Orthogonal unit vector projections
Notice that if the vector being projected is itself of unit length, then its coordinates ARE the cosines of the angles it makes with the basis vectors.

$$\cos(\theta) = \left(\frac{a}{H}\right) = \frac{1\cos(\theta)}{1} = \cos(\theta) \qquad (5.1)$$

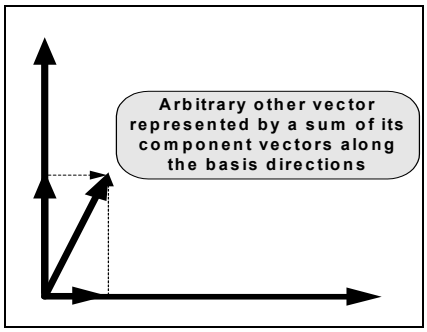


Figure 8. Components

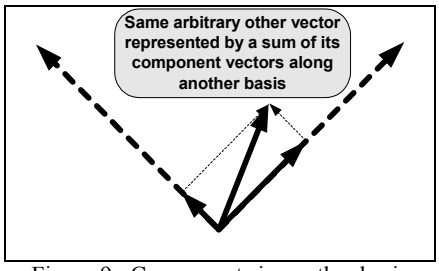


Figure 9. Components in another basis

Trick, trick, trick
If the vector being projected is a unit vector (length 1) and it lies at 45 degrees, then its projections are equal since

$$\cos(45°) = \frac{1}{\sqrt{2}} = \sin(45°) \qquad (5.2)$$

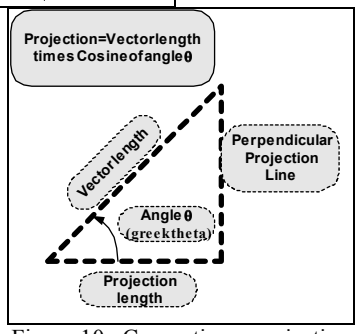


Figure 10. Computing a projection

Orthogonal Projections on the other basis vector
The projection on the other basis axis is the cosine of the compliment of the first angle. It equals the sine of that first angle.

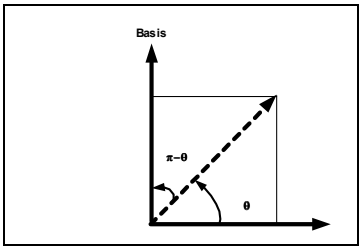


Figure 11. $\cos(\pi-\theta) = \sin(\theta)$

Four Factoids to be used later

1) The square of the projections of a 45 degree unit vector are:

$$\cos^2(45°) = \left(\tfrac{1}{\sqrt{2}}\right)^2 = .5 \quad (5.3)$$

2) The square of the projection of a unit vector on itself is:

$$\cos^2(0°) = (1)^2 = 1 \quad (5.4)$$

3) The square of the projection of a unit vector on a vector perpendicular to itself is:

$$\cos^2(90°) = (0)^2 = 0 \quad (5.5)$$

4) The sum of the squares of the coordinates of a unit vector is 1, so we can consider them probabilities.

$$\cos^2(45^\circ) + \sin^2(45^\circ) = \left(\tfrac{1}{\sqrt{2}}\right)^2 + \left(\tfrac{1}{\sqrt{2}}\right)^2 = \frac{1}{2} + \frac{1}{2} = 1 \quad (5.6).$$

6. QUANTUM SYSTEM STATE

State

A quantum system is represented by its states. A quantum system state is a vector in some suitable space (often infinite dimensional or at least more than 3-D). However in this case we can limit the system to a photon that can be polarized. Its quantum state is represented by a vector of length one in the direction of its polarization.

This is a rare example where the quantum state can be pictured in the real world (not a phase space) and is limited to only two dimensions!

Unit Multipliers (sort of a trick)

We are interested only in the length of the vector and its line of action. We will neglect factors of magnitude 1. For example, if a state vector is reversed (multiplied by –1) we consider it unchanged. It is still representing the same filter axis since physically a 180 degree turn makes no difference.

Basis or PURE states and their filters

A photon is in a "pure" state if it has just been measured (passed through a filter). WE NOW KNOW ITS STATE! If we measure it again with the same filter we get the same result with p=1. If we measure it with the complimentary filter of the pair we get NO result (NO photon). Probability of a photon is p = 0. *But this tells us the probability of the photon being in the other direction of the pair is p = 1. So we know the photon polarization. This weirdness happens only in 2-D where the pure states are either or.*

On the other hand, if we measure the known state with one of the *other pair* of filters we get out a photon in that state with p=.5 or in its complimentary state with p=.5. This is totally ambiguous.

Any two orthogonal filters can determine a basis set. We will use two special *sets* of filter pairs.

A filter pair (horizontal and vertical) **{|** and **–}** pass polarization states which are orthogonal and therefore form a basis of the 2-D space of polarization. **(|)** and **(–)** are called the **{+}** pair**.**

Similarly, a 45-degree left filter **(\)** and 45-degree right filter **(/)** form a mutually perpendicular set of axes. They can form another basis of the same two-dimensional space of polarization states. **(\ )** and **(/)** are called the **{X}** pair**.**

These two bases are at 45-degrees to each other. The polarization state of any photon can be written as a sum of the basis states of either basis. For example, each basis vector in each set can be written as a sum of the other basis set (underline indicates vector):

$$\underline{(\backslash)} = \frac{1}{\sqrt{2}}\underline{(|)} - \frac{1}{\sqrt{2}}\underline{(-)} \quad (6.1)$$

$$\underline{(/)} = \frac{1}{\sqrt{2}}\underline{(|)} + \frac{1}{\sqrt{2}}\underline{(-)} \quad (6.2)$$

$$\underline{(|)} = \frac{1}{\sqrt{2}}\underline{(\backslash)} + \frac{1}{\sqrt{2}}\underline{(/)} \quad (6.3)$$

$$\underline{(-)} = -\frac{1}{\sqrt{2}}\underline{(\backslash)} + \frac{1}{\sqrt{2}}\underline{(/)} \quad (6.4)$$

Notice the minus signs since **(\)** projects onto the negative of **(–),** and **(–)** projects onto the negative of **(\).** Notice that the sum of squares of ALL coordinates is always 1!

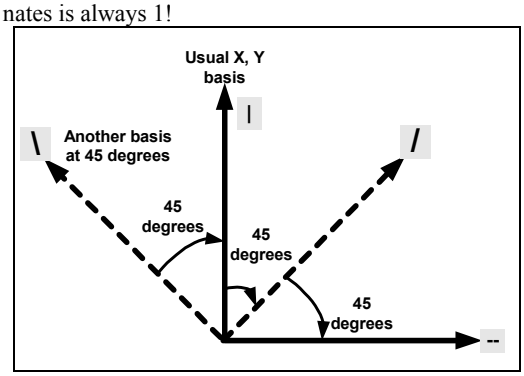


Figure 12. The two basis sets **{+} = {| , –}** and **{X} = {\ , /}**

Mixed States

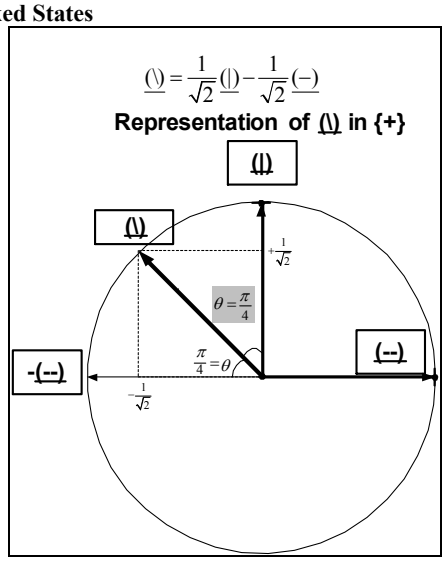


Figure 13. (\) represented in {+}

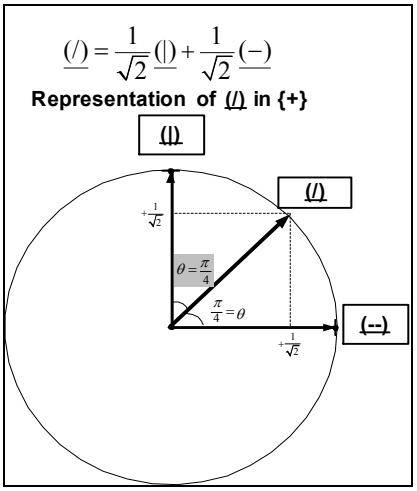


Figure 14. (/) represented in {+}

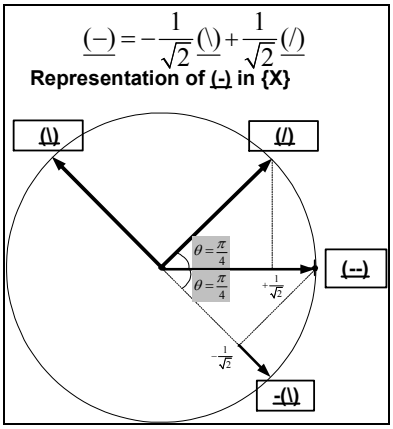


Figure 15. (-) represented in {X}

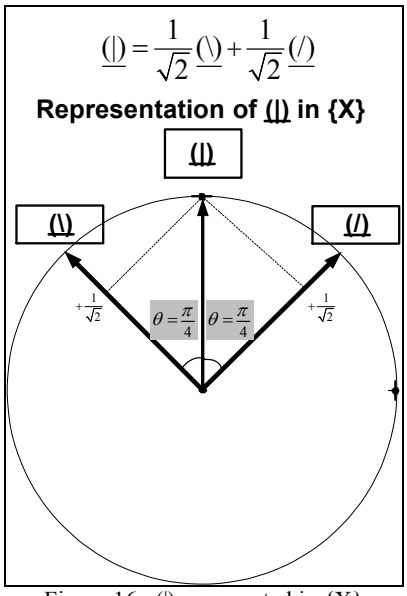


Figure 16. (|) represented in {X}

Just to be complete and to practice thinking about representing vectors in a basis, let's look at the representations of the bases in themselves!

Basis or PURE states

$$\underline{(|)} = (1)\underline{(|)} + (0)\underline{(-)} \quad \textit{and} \quad \underline{(-)} = (0)\underline{(|)} + (1)\underline{(-)} \tag{6.5}$$

$$\underline{(\backslash)} = (1)\underline{(\backslash)} + (0)\underline{(/)} \quad \textit{and} \quad \underline{(/)} = (0)\underline{(\backslash)} + (1)\underline{(/)} \tag{6.6}$$

Notice that the sum of squares of ALL coordinates is always 1!

7. CONNECTING IT ALL TOGETHER

A filtered photon is in a pure state. Its state vector is parallel to the filter - one of the basis vectors. If it is then sent through another filter (measured) we can only determine the probability of the outcome of the measurement. The probability is the square of the coordinate of the state vector as it is written in the measuring filter basis. See equations (6.1)-(6.6)

1) If the photon is sent through the same filter, we get the same result with a probability of 1. See the pure state equations above (6.5) and (6.6).
2) If it is sent through the same filter *set* but the other filter of the pair, we get the result of

NO MEASURED PHOTON (probability of 0). See the pure state equations above (6.5) and (6.6).

3) If it is sent through the any of the two filters of the other set, we can only predict the result with a probability of .5. See the mixed state equations (6.1)-(6.4) above or in Figures 13-16.

8. NO CLONING THEOREM

In general we can never know for sure what the state was *before our first measurement*. Since we have no prior knowledge of the before state, we can only give the probabilities of getting what we do measure, *assuming* some prior state.

This means that we can't copy exactly a prior state (clone it). The best we can do is that we measure the quantum system state and compute the probabilities of our measured state value given that we started out in an *assumed (but unknown)* prior state.

No Cloning Theorem: We can not copy exactly (clone) an unknown prior quantum state.

9. THE QUANTUM KEY DISTRIBUTION ALGORITHM

(Johnson, 2003; Nielsen and Chuang,, 2000; Singh, 2002; Tanenbaum, 2003)

0) Alice (sender) and Bob (receiver) agree to use two sets of polarization filters: **(+)** and **(X).** They choose which filtered photons will represent what bits before they start, say:

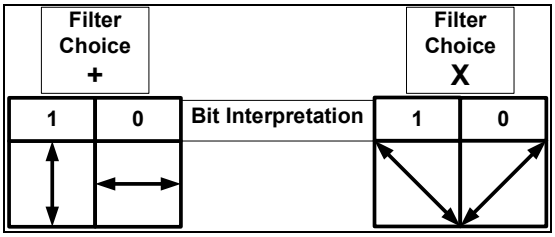


Figure 17. Filter Sets **{+}** & **{X}** and (arbitrary) bit-filter correspondences

1) Alice chooses N random bits [not an easy trick in itself]. and sends these N random bits (photons) using a random choice of N filters. Alice knows her bits, filter sets, and filters.

2) Bob uses a random choice of receiving filters. Bob knows his measured bits (photons) and his filters but he does not know what Alice sent – yet. Some measured bits will be errors because he chose the non-matching (incorrect) filter *set.*

   An incorrect filter set gives a bit error 50% of the time. A correct (matching) filter gives a correct bit 100% of the time. Some of Bob's bits might actually be bad because an eavesdropper (Eve) passed on modified bits. See step 5.

3) Alice phones Bob in the clear and tells him her sequence of filter SETS (Eve could hear this). Neither Bob nor Eve (an eavesdropper, if she exists) knows the bits yet.

4) Bob tells Alice in the clear which of his sequence of filter SETS agree (Eve could hear this). She won't know what actual filters Bob used.

   This determines a secret set of M known bit values, known to both Alice and Bob. This is a symmetric key for encryption - if no Eve.

   Some bits might be wrong if there was an Eve who corrupted the original bit string due to No Cloning.

5) Alice phones Bob again in the clear and reads to him a discardable subset of her actual bits. If Bob agrees, then there has been no Eve. All bits MUST be the same since they used the same filter sets. Otherwise, there has been an Eve due to bit stream corruption, so they must discard ALL bits and start over!

   It is highly UNlikely that in a long but discardable set of bits Eve would have chosen to pass on to Bob bits exactly matching those Alice sent. Since she can't copy them by the No Cloning Theorem, some will be in error (not the same as Alice sent). This causes the bit errors in Alice's read back to Bob.

Discussion

The 50% error rate in step 2 comes from a photon prepared in one filter basis by Alice then being measured in the other filter *basis* by Bob. The sent photon state vector gets projected onto Bob's filter's direction with probability 50% or onto its orthogonal direction also with a probability of 50%. Either gives Bob a *bit* value.

If Alice only sends Bob her bit choices he has a 50% chance of having read the correct bit even though it is from the wrong filter set. Fortunately she will send her filter choices, in step 3, so he will know this bit is

probably only 50% correct – so he drops it from consideration.

Notice that at no time does Eve know the bits in agreement (the key) because she does not know Bob's filter choices. She may know some bits in common with Bob because she luckily chose some filters matching Alice's correctly.

The bit read back in step 5 does not help Eve either. They are a subset of a bit string that she does not know and will be discarded anyway.

The best Eve can hope for is a possible denial of service attack.

There are two other ideas here. One is that the probability of her choosing ALL of the correct filter sets for an N bit string is $\boxed{\left(\frac{1}{2}\right)^N = \frac{1}{2^N}}$ (probability of a set of N ands) which is, for long strings, effectively 0. The second is the No Cloning Theorem which forces Eve to pass on guessed photons to Bob. The probability of Eve matching all of Alice's bits by chance is again vanishingly small.

A critical part of the algorithm is that EVE can't exactly mimic Alice's bit string to send on to Bob because of the No Cloning theorem. She MUST corrupt some of the bits she forwards on to Bob thus enabling the step 5 sensing of her presence.

A subtlety is that because of the filter set definitions and their 45 degree relationship to each other, Bob (and Eve) get some benefit. If they choose the correct filter set (by step 3) they actually know the bit even if they chose the wrong filter of the pair! In that case they measured NO PHOTON. This is a dead give away for both the bit (the other filter of the pair) and a fortiori the filter pair. This is a fortuitous situation that comes up only in two dimensions where there are no other dimensions for the complimentary state vector.

The probability of randomly choosing the correct filter pair for any bit is .5. Therefore many of the bits measured by Bob or Eve will be wrong. Although the actual algorithm uses error correcting codes (Nielsen and Chuang, 2000), the following heuristic is helpful.

Products now on the market determine long keys at about 100b/sec.

The appendix contains a pair of diagrams of the algorithm.

10. CONCLUSION

Because the best available encryption is problematic, we need to employ more robust encryption methods especially in networking. A provable unbreakable encryption method is based on QKD. With a little high school algebra and some elementary purely descriptive physics we can get a basic understanding of how QKD works.

We are using single photons and their quantum physical properties. We are creating one-time keys (known unbreakable) 100b/sec. QKD overcomes the one critical weakness of classical unbreakable one-time-pads – the secure distribution of the pads themselves. The encryption of messages proceeds classically and is known unbreakable! QKD is the solution of choice in critical environments.

Even if there is an eavesdropper, we can sense it. Otherwise, the key is secure.

No future speed up of computing can threaten this method as PKI is threatened (factoring large numbers depends on the speed of your computer). QKD is founded on physical properties that won't change in time.

11. REFERENCES

BBN, 2004
http://www.bbn.com/networking/quantumcryptography.html {The DARPA project to build the next level of secure Internet.}

B & H, 2004
http://www.bhphotovideo.com/
{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, 2004
http://www.edmundoptics.com/
{Search KIT, then OPTICS DISCOVERY KIT ($17.95). This is an American Optical Society of America classroom experiments kit – ages 10 – adult.}

Edmund Scientifics, 2004
http://scientificsonline.com/
{Search 3038490, then POLARIZER EXPERIMENTERS KIT ($19.95)}

Frank, Ronald I. 2003, "The Quantum Computing (QC), Quantum Encryption (QE), And Quantum Information (QI Curriculum (Why? Now? Never?)". *Information Systems Education Journal Volume 1, Number 46 December 27,, ISSN 1545-679x.* {also contains general QM references.} http://216.228.254.11/1/46/index.html {Contains an argument for doing this module}

Frank, Ronald I. 2004, "A Presentation Of The Prerequisite Topics And A Module For A Quantum Encryption (QE) Topic In An Is Course". *Proceedings Of AMCIS 2004 To Appear. {Discusses the prerequisites and a more advanced graduate module than presented here}*

Johnson, George, 2003, A Short Cut Through Time. Alfred A. Knoph Pubs. ISBN 0-375-41193-3. {Layperson's introduction to QC & QE. About Quantum Computers – mentions breaking PKI}

Messiah, Albert, 1999, Quantum Mechanics. Dover (1999 paper version of the John Wiley 1958 two volume set) ISBN 0-486-40924-4.

{I include this reference only for completeness, not as a suggested starting point. It is an old favorite of mine, is readily available, complete, and inexpensive. It is not an IS book. It is a well-known text for graduate work in physics and assumes a substantial background in both physics and mathematics such as a large part of (Courant 1953).

It contains no information on the modern topics of QC, QI, or QE, having come before these, but it is a pleasant read for a deeper background.}

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 (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. }

Singh, Simon, 2002, The Code Book. Anchor Books ISBN 0-385-49532-3. Includes a layperson's chapter on modern QE.}

http://www.arxiv.org 2004, {Search Quantum Cryptography - All Years}

http://www.idquantique.com/ 2004 {a product house}

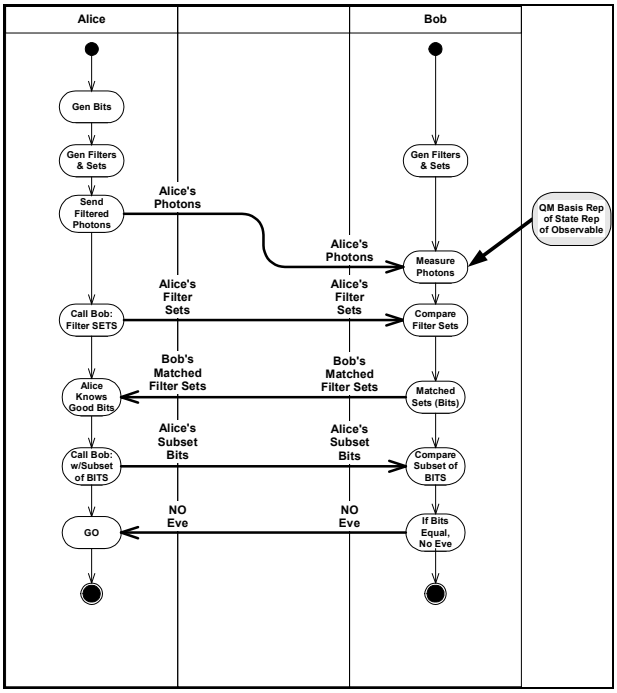
http://magiqtech.com/ 2004 {another product house}

http://www.mathpages.com/rr/s9-04/9-04.htm, 2004, {spin and polarization are often confused.}

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

Waite, Stephen R., 2002, Quantum Investing. Thomson Texere. ISBN 1587991403

12. APPENDIX – ALGORITHM DIAGRAM – NO EVE



13. APPENDIX – ALGORITHM DIAGRAM – WITH AN EVE