A TALK ON QUANTUM CRYPTOGRAPHY OR HOW ALICE OUTWITS EVE VERSION 1.5

SAMUEL J. LOMONACO, JR.

ABSTRACT. Alice and Bob wish to communicate without the archvillainess Eve eavesdropping on their conversation. Alice, decides to take two college courses, one in cryptography, the other in quantum mechanics. During the courses, she discovers she can use what she has just learned to devise a cryptographic communication system that automatically detects whether or not Eve is up to her villainous eavesdropping. Some of the topics discussed are Heisenberg's Uncertainty Principle, the Vernam cipher, the BB84 and B92 cryptographic protocols. The talk ends with a discussion of some of Eve's possible eavesdropping strategies, opaque eavesdropping, translucent eavesdropping, and translucent eavesdropping with entanglement.

SHORT ABSTRACT. This is a story about how Alice ingeniously devises two different quantum cryptographic communication protocols (i.e., BB84 and B92) that prevent archvillainess Eve from eavesdropping on Alice's communications with Bob. How does Alice do this? Also, how does she implement her ideas in optics?

CONTENTS

1. Preface 2
1.1. The Unique Contribution of Quantum Cryptography 2
1.2. A Note to the Reader 3
2. Introduction 3
3. A Course on Classical Cryptography 3
3.1. Alice's enthusiastic decision 3
3.2. Plaintext, ciphertext, key, and ... Catch 22 4
3.3. Practical Secrecy 4
3.4. Perfect Secrecy 5
3.5. Computational Security 7

Date: January 27, 2001.

Partially supported by ARL Contract #DAAL01-95-P-1884, ARO Grant #P-38804-PH-QC, the Computer Security Division of NIST, and the L-O-O-P Fund.

This paper is a revised version of a paper published in "Coding Theory, and Cryptography: From Geheimscheimschreiber and Enigma to Quantum Theory," (edited by David Joyner), Lecture Notes in Computer Science and Engineering, Springer-Verlag, 1999 (pp. 144-174). It has been reproduced with the permission of Springer-Verlag.

4. A Course on Quantum Mechanics 9
4.1. Alice's Reluctant Decision 9
4.2. The Classical World – Introducing the Shannon Bit 9
4.3. The Quantum World – Introducing the Qubit 9
4.4. Where do qubits live? 10
4.5. Some Dirac notation – Introducing kets 10
4.6. Finally, a definition of a qubit 11
4.7. More Dirac notation – Introducing bras and bra-c-kets 11
4.8. Activities in the quantum world – Unitary transformations 12
4.9. Observables in quantum mechanics – Hermitian operators 12
4.10. The Heisenberg uncertainty principle – A limitation on what we can actually observe 13
4.11. Young's two slit experiment – An example of Heisenberg's uncertainty principle 14
5. The Beginnings of Quantum Cryptography 17
5.1. Alice has an idea 17
5.2. Quantum secrecy – The BB84 protocol without noise 18
5.3. Quantum secrecy – The BB84 protocol with noise 22
6. The B92 quantum cryptographic protocol 25
7. There are many other quantum cryptographic protocols 26
8. A comparison of quantum cryptography with classical and public key cryptography 26
9. Eavesdropping strategies and counter measures 27
9.1. Opaque eavesdropping 27
9.2. Translucent eavesdropping without entanglement 28
9.3. Translucent eavesdropping with entanglement 28
9.4. Eavesdropping based on implementation weaknesses 28
10. Implementations 29
11. Conclusion 29
12. Acknowledgement 30
References 30

1. Preface

1.1. **The Unique Contribution of Quantum Cryptography.** Before beginning our story, I'd like to state precisely what is the unique contribution of quantum cryptography.

> Quantum cryptography provides a new mechanism enabling the parties communicating with one another to:
>
> Automatically Detect Eavesdropping

Consequently, it provides a means for determining when an encrypted communication has been compromised.

1.2. **A Note to the Reader.** This paper is based on an invited talk given at the Conference on Coding theory, Cryptology, and Number Theory held at the US Naval Academy in Annapolis, Maryland in October of 1998. It was also given as an invited talk at the Quantum Computational Science Workshop held in conjunction with the Frontiers in Computing Conference in Annapolis, Maryland in February of 1999, at a Bell Labs Colloquium in Murray Hill, New Jersey in April of 1999, at the Security and Technology Division Colloquium of NIST in Gaithersburg, Maryland, and at the Quantum Computation Seminar at the U.S. Naval Research Labs in Washington, DC.

My objective in creating this paper was to write it exactly as I had given the talk. But ... Shortly after starting this manuscript, I succumbed to the temptation of greatly embellishing the story that had been woven into the original talk. I leave it to the reader to decide whether or not this detracts from or enhances the paper.

2. Introduction

We begin our crypto drama with the introduction of two of the main characters, **Alice** ♡and♡ **Bob**, representing respectively the **sender** and the **receiver**. As in every drama, there is a triangle. The triangle is completed with the introduction of the third main character, the archvillainess **Eve**, representing the **eavesdropper**.

Our story begins with Alice and Bob attending two different universities which are unfortunately separated by a great distance. Alice would like to communicate with Bob without the ever vigilant Eve eavesdropping on their conversation. In other words, how can Alice talk with Bob while at the same time preventing the evil Eve from listening in on their conversation?

3. A Course on Classical Cryptography

3.1. **Alice's enthusiastic decision.** Hoping to find some way out of her dilemma, Alice elects to take a course on cryptography, Crypto 351 taught by Professor Shannon with guest lecturers Diffie, Rivest, Shamir, and Adleman. Alice thinks to herself, "Certainly this is a wise choice. It is a very applied course, and surely relevant to the real world. Maybe I will learn enough to outwit Eve?"

3.2. **Plaintext, ciphertext, key, and ... Catch 22.** Professor Shannon begins the course with a description of classical cryptographic communication systems, as illustrated in Fig. 1. Alice, the sender, encrypts her **plaintext** P into **ciphertext** C using a **secret key** K which she shares only with Bob, and sends the ciphertext C over an **insecure channel** on which the evil Eve is ever vigilantly eavesdropping. Bob, the receiver, receives the ciphertext C, and uses the secret key K, shared by him and Alice only, to decrypt the ciphertext C into plaintext P.

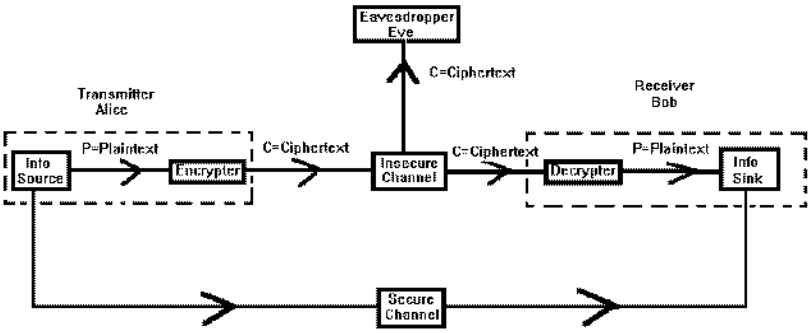

Figure 1. A classical cryptographic communication system.

What is usually not mentioned in the description of a classical cryptographic communication system is that Alice and Bob must first communicate over a **secure channel** to establish a secret key K shared only by Alice and Bob before they can communicate in secret over the insecure channel. Such a channel could consist, for example, of a trusted courier, wearing a trench coat and dark sunglasses, transporting from Alice to Bob a locked briefcase chained to his wrist. In other words, we have the famous Catch 22 of classical cryptography, namely:

> **Catch 22.** There are perfectly good ways to communicate in secret, provided we can communicate in secret ...

Professor Shannon then goes on to discuss the different types of classical communication security.

3.3. **Practical Secrecy.** A cryptographic communication system is **practically secure** if the encryption scheme can be broken after X years, where X is determined by one's security needs and by existing technology. Practically secure cryptographic systems have existed since antiquity. One example would be the Caesar cipher used by Julius Caesar during the during the Gallic wars, a cipher that was difficult for his opponents to break at that time, but easily breakable by today's standards. A modern day example of a practically secure classical cryptographic system is the digital encryption

standard (DES) which has just recently been broken[1]. For this and many other reasons, DES is to be replaced by a more practically secure classical encryption system, the Advanced Encryption Standard (AES). In turn, AES will be replaced by an even more secure cryptographic system should the advances in technology ever challenge its security.

3.4. **Perfect Secrecy.** A cryptographic communication is said to be **perfectly secure** if the ciphertext C gives no information whatsoever about the plaintext P, even when the design of the cryptographic system is known. In mathematical terms, this can be stated succinctly with the equation:

$$PROB(P \mid C) = PROB(P).$$

In other words, the probability of plaintext P given ciphertext C, written $PROB(P|C)$, is equal to the probability of the plaintext P.

An example of a perfectly secure classical cryptographic system is the **Vernam Cipher**, better known as the **One-Time-Pad**. The plaintext P is a binary sequence of zeroes and ones, i.e.,

$$P = P_1, P_2, P_3, \ \ldots \ P_n, \ \ldots$$

The secret key K consists of a totally random binary sequence of the same length, i.e.,

$$K = K_1, K_2, K_3, \ \ldots \ , \ K_n, \ \ldots$$

The ciphertext C is the binary sequence

$$C = C_1, C_2, C_3, \ \ldots \ C_n, \ \ldots$$

obtained by adding the sequences P and K bitwise modulo 2, i.e.,

$$C_i = P_i + K_i \bmod 2 \qquad \text{for} \qquad i = 1, 2, 3, \ \ldots$$

For example,

$$\begin{array}{rcl} P & = & 0110 \quad 0101 \quad 1101 \\ K & = & 1010 \quad 1110 \quad 0100 \\ \hline C = P \oplus K & = & 1100 \quad 1011 \quad 1001 \end{array}$$

This cipher is perfectly secure if key K is totally random and shared only by Alice and Bob. It is easy to encode with the key K. If, however, one succumbs to the temptation of using the same key K to encode two different plaintexts $P^{(1)}$ and $P^{(2)}$ into ciphertexts $C^{(1)}$ and $C^{(2)}$, then the cipher system immediately changes from a perfectly secure cipher to one that is easily broken by even the most amateur cryptanalyst. For, $C^{(1)} \oplus C^{(2)} =$

[1]Tim O'Reilly and the Electronic Frontier Foundation have constructed a computing device for $250,000 which does an exhaustive key search on DES in 4.5 days[19]. See also [2] and [14]. As far as I know, triple DES has not been broken.

$P^{(1)} \oplus P^{(2)}$ is easily breakable because of the redundancy that is usually present in plaintext.

The only problem with the one-time-pad is that long bit sequences must be sent over a secure channel before it can be used. This once again leads us to the Catch 22 of classical cryptography, i.e.,

> **Catch 22.** There are perfectly good ways to communicate in secret, provided we can communicate in secret ...

... and to the:

- **Key Problem 1.** *Catch 22*: A secure means of communicating key is needed.[2]

Finally, there are two other key problems in classical cryptography in need of a solution, namely:

- **Key Problem 2.** *Authentication*: Alice needs to determine with certainty that she is actually talking to Bob, and not to an impostor such as Eve.
- **Key Problem 3.** *Intrusion Detection*: Alice needs a means of determining whether or not Eve is eavesdropping.

In summary, we have the following checklist for classical cryptographic systems:

Check List for Classical Crypto Systems	
■ Catch 22 Solved?	**NO**
■ Authentication?	**NO**
■ Intrusion Detection?	**NO**

[2]Hired trench coats are exorbitantly expensive and time consuming.

3.5. **Computational Security.** Relatively recently in the history of cryptography, Diffie and Hellman [7], [8] suggested a new type cryptographic secrecy. A cipher is said to be **computationally secure** if the computational resources required to break it exceed anything possible now and into the future. For example, a cipher would be computationally secure if the number of bits of computer memory required to break it were greater than the number of atoms in the universe, or if the computational time required to break it exceeded the age of the universe. Cryptographic systems can be created in such a way that it is computationally infeasible to find the decryption key D even when the encryption key E is known. To create such a cryptographic system, all one would need is a trap-door function f.

Definition 1. *A function f is a* ***trap-door function*** *if*

1) *f is easy to compute, i.e., polynomial time computable, and*
2) *Given the function f, the inverse function f^{-1} can not be computed from f in polynomial time, i.e., such a computation is superpolynomial time, intractable, or worse.*

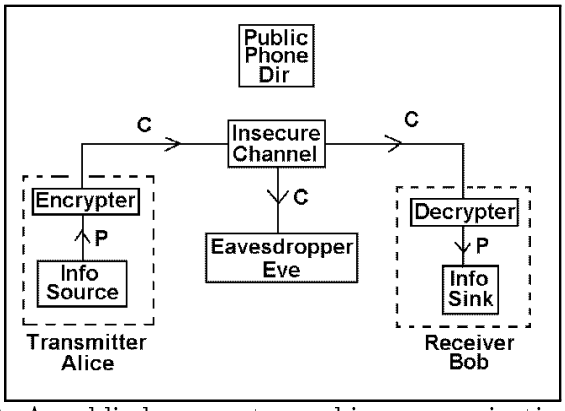

Figure 2. A public key cryptographic communication system

A trap-door function E can be used to create a **public key cryptographic system** as illustrated in Fig.2. All parties who wish to communicate in secret should choose their own trap-door function E and place it in a **public directory**, the "**yellow pages**," for all the world to see. But they should keep their decryption key $D = E^{-1}$ secret. Since E is a trap-door function, it is computationally infeasible for anyone to use the publicly known E to find the decryption key D. So D is secure in spite of the fact that its inverse E is publicly known.

If Alice wishes to send a secret communication to Bob, she first looks up in the yellow pages Bob's encryption key E_B, encrypts her plaintext P with Bob's encryption key E_B to produce ciphertext $C = E_B(P)$, and then sends the ciphertext C over a public channel. Bob receives the ciphertext C, and

decrypts it back into plaintext $P = D_B(C)$ using his secret decryption key D_B.

Alice can even do more than this. She can authenticate, i.e., sign her encrypted communication to Bob so that Bob knows with certitude that the message he received actually came from Alice and not from an Eve masquerading as Alice. Alice can do this by encrypting her signature $\mathcal{ALICE}$ using her secret decryption key D_A into $D_A(\mathcal{ALICE})$. She then encrypts plaintext P plus her signature $D_A(\mathcal{ALICE})$ using Bob's publicly known encryption key E_B to produce the signed ciphertext $C_{\mathcal{S}} = E_B(P + D_A(\mathcal{ALICE}))$, and then sends her signed ciphertext $C_{\mathcal{S}}$ over the public channel to Bob. Bob can then decrypt the message as he did before to produce the signed plaintext $P + D_A(\mathcal{ALICE})$. Bob can verify Alice's digital signature $D_A(\mathcal{ALICE})$ by looking up Alice's encryption key E_A in the "yellow pages," and using it to find her signature $E_A(D_A(\mathcal{ALICE})) = \mathcal{ALICE}$. In this way, he authenticates that Alice actually sent the message because only she knows her secret decryption key. Hence, only she could have signed the plaintext.[3]

The RSA cryptographic system is believed to be one example of a public key cryptographic system. There are many public software implementations of RSA, e.g., PGS (Pretty Good Security).

Thus, besides solving the authentication problem for cryptography, public key cryptographic systems appear also to solve the Catch 22 of cryptography. However, frequently the encryption and decryption keys of a public key cryptographic system are managed by a central key bank. In this case, the Catch 22 problem is still there. For that reason, we have entered 'MAYBE' in the summary given below.

Check List for PKS	
■ Catch 22 Solved?	**MAYBE**
■ Authentication?	**YES**
■ Intrusion Detection?	**NO**

[3]Because of the need for brevity, we have not discussed all the subtleties involved with digital signatures. For example, for more security, Alice should add a time stamp and some random symbols to her signature. For more information on digital signatures, please refer to one of the standard references such as [18].

4. A Course on Quantum Mechanics

4.1. **Alice's Reluctant Decision.** In spite of Alice's many intense efforts to avoid taking a course in quantum mechanics, she was finally forced by her university's General Education Requirements (GERs) to register for the course Quantum 317, taught by Professor Dirac with guest lecturers Feynman, Bennett, and Brassard. She did so reluctantly. "After all," she thought, "Certainly this is an insane requirement. Quantum mechanics is not applied. It's too theoretical to be relevant to the real world. Ugh! But I do want to graduate."

4.2. **The Classical World – Introducing the Shannon Bit.** Professor Dirac began the course with a brief introduction to the classical world of information. In particular, Alice was introduced to the classical Shannon Bit, and shown that he/she/it is a very decisive individual. The Shannon Bit is either 0 or 1, but by no means both at the same time.

"Hmm ... ," she thought, "I bet that almost everyone I know is gainfully employed because of the Shannon Bit."

The professor ended his brief discussion of the Shannon Bit by mentioning that there is one of its properties that we take for granted. I.e., it can be copied.

4.3. **The Quantum World – Introducing the Qubit.** Next Professor Dirac switched to the mysterious world of the quantum. He began by introducing the runt of the Bit clan, i.e., the Quantum Bit, nicknamed **Qubit**. He began by showing the class a small dot, i.e., a quantum dot. In fact it was so small that Alice couldn't see it at all. He promptly pulled out a microscope[4], and projected a large image on a screen for the entire class to view.

Professor Dirac went on to say, "In contrast to the decisive classical Shannon Bit, the Qubit is a very indecisive individual. It is both 0 and 1 at the same time! Moreover, unlike the Shannon Bit, the Qubit cannot be copied because of the no cloning theorem of Dieks, Wootters, and Zurek[6][25]. Qubits are very slippery characters, exceedingly difficult to deal with."

"One example of a qubit is a spin $\frac{1}{2}$ particle which can be in a spin-up state $|1\rangle$ which we label as 1, in a spin-down state $|0\rangle$ which we label as 0, or in a **superposition** of these states, which we interpret as being both 0 and 1 at the same time." (The term "superposition" will be explained shortly.)

"Another example of a qubit is the polarization state of a photon. A photon can be in a vertically polarized state $|\updownarrow\rangle$. We assign a label of 1 to this state. It can be in a horizontally polarized state $|\leftrightarrow\rangle$. We assign a

[4]This is a most unusual microscope!

label of 0 to this state. Or, it can be in a superposition of these states. In this case, we interpret its state as representing both 0 and 1 at the same time."

"Anyone who has worn polarized sunglasses should be familiar with the polarization states of the photon. Polarized sunglasses eliminate glare because they let through only vertically polarized light while filtering out the horizontally polarized light that is reflected from the road."

4.4. **Where do qubits live?** But where do qubits live? They live in a Hilbert space $\mathcal{H}$. By a Hilbert space, we mean:

Definition 2. *A **Hilbert Space** is a vector space over the complex numbers* $\mathbb{C}$ *together with an inner product*

$$\langle \quad , \quad \rangle : \mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{C}$$

such that

1) $\langle u_1 + u_2, v\rangle = \langle u_1, v\rangle + \langle u_2, v\rangle$ *for all* $u_1, u_2, v \in \mathcal{H}$
2) $\langle u, \lambda v\rangle = \langle \lambda u, v\rangle$ *for all* $u, v \in \mathcal{H}$ *and* $\lambda \in \mathbb{C}$
3) $\langle u, v\rangle^* = \langle v, u\rangle$ *for all* $u, v \in \mathcal{H}$ *, where the superscript '$*$' denotes complex conjugation.*
4) *For every Cauchy sequence* $u_1, u_2, u_3, \ \ldots$ *in* $\mathcal{H}$*,*

$$\lim_{n\to\infty} u_n \text{ exists and lies in } \mathcal{H}$$

In other words, a Hilbert space is a vector space over the complex numbers $\mathbb{C}$ with a sequilinear inner product in which sequences that should converge actually do converge to points in the space.

4.5. **Some Dirac notation – Introducing kets.** The elements of $\mathcal{H}$ are called **kets**, and will be denoted by

$$|label\rangle \ ,$$

where '$|$' and '$>$' are left and right delimiters, and '*label*' denotes any label, i.e., name, we wish to assign to a ket.

4.6. **Finally, a definition of a qubit.** So finally, we can define what is meant by a qubit.

Definition 3. *A **qubit** is a ket (state) in a two dimensional Hilbert space $\mathcal{H}$.*

Thus, if we let $|0\rangle$ and $|1\rangle$ denote an arbitrary orthonormal basis of a two dimensional Hilbert space $\mathcal{H}$, then each qubit in $\mathcal{H}$ can be written in the form

$$|qubit\rangle = \alpha_0 |0\rangle + \alpha_1 |0\rangle$$

where α_0, $\alpha_1 \in \mathbb{C}$. Since any scalar multiple of a ket represents the same state of an isolated quantum system, we can assume, without loss of generality, that $|qubit\rangle$ is a ket of unit length, i.e., that

$$|\alpha_0|^2 + |\alpha_1|^2 = 1$$

The above qubit is said to be in a **superposition** of the states $|0\rangle$ and $|1\rangle$. This is what we mean when we say that a qubit can be simultaneously both 0 and 1. However, if the qubit is observed it immediately "makes a decision." It "decides" to be 0 with probability $|\alpha_0|^2$ and 1 with probability $|\alpha_1|^2$. Some physicists call this the **"collapse"** of the wave function[5].

4.7. **More Dirac notation – Introducing bras and bra-c-kets.** Given a Hilbert space $\mathcal{H}$, let

$$\mathcal{H}^* = Hom(\mathcal{H}, \mathbb{C})$$

denote the set of all linear maps from $\mathcal{H}$ to $\mathbb{C}$. Then $\mathcal{H}^*$ is actually a Hilbert space, called the **dual** Hilbert space of $\mathcal{H}$, with scalar product and vector sum defined by:

$$\begin{cases} (\lambda \cdot f)(|\Psi\rangle) = \lambda (f(|\Psi\rangle)), & \text{for all } \lambda \in \mathbb{C} \text{ and for all } f \in \mathcal{H}^* \\ (f_1 + f_2)(|\Psi\rangle) = f_1(|\Psi\rangle) + f_2(|\Psi\rangle), & \text{for all } f_1, f_2 \in \mathcal{H}^* \end{cases}$$

We call the elements of $\mathcal{H}^*$ **bra**'s, and denote them as:

$$\langle label|$$

We can now define a bilinear map

$$\mathcal{H}^* \times \mathcal{H} \longrightarrow \mathbb{C}$$

by

$$(\langle \Psi_1|)(|\Psi_2\rangle) \in \mathbb{C}$$

since bra $\langle \Psi_1|$ is a complex valued function of kets. We denote this product more simply as

$$\langle \Psi_1 \mid \Psi_2 \rangle$$

and call it the **Bra-c-Ket** (or **bracket**) of bra $\langle \Psi_1|$ and ket $|\Psi_2\rangle$.

[5]It is very difficult, if not impossible, to find two physicists who agree on the subject of quantum measurement. The phrase "collapse of the wave function" immediately engenders a "war cry" in most physicists. For that reason, "collapse" is enclosed in quotes.

Finally, the bracket induces a dual correspondence[6] between $\mathcal{H}$ and $\mathcal{H}^*$, i.e.,

$$|\Psi_2\rangle \overset{D.C.}{\longleftrightarrow} \langle\Psi_1|$$

4.8. **Activities in the quantum world – Unitary transformations.** All "activities" in the quantum world are linear transformations

$$U : \mathcal{H} \longrightarrow \mathcal{H}$$

from the Hilbert space $\mathcal{H}$ into itself, called **unitary transformations** (or, **unitary operators**). If we think of linear transformations as matrices, then a **unitary transformation** U is a square matrix of complex numbers such that

$$\overline{U}^T U = I = U\overline{U}^T$$

where $\overline{U}^T$ denotes the matrix obtained from U by conjugating all its entries and then transposing the matrix. We denote $\overline{U}^T$ by $U^\dagger$, and refer to it as the **adjoint** of U.

Thus, an "activity" in the quantum world would be, for example, a unitary transformation U that carries a state ket $|\Psi_0\rangle$ at time $t = 0$ to a state ket $|\Psi_1\rangle$ at time $t = 1$, i.e.,

$$U : |\Psi_0\rangle \longmapsto |\Psi_1\rangle$$

4.9. **Observables in quantum mechanics – Hermitian operators.** In quantum mechanics, what does an observer observe?

All **observables** in the quantum world are linear transformations

$$\mathcal{O} : \mathcal{H} \longrightarrow \mathcal{H}$$

from the Hilbert space $\mathcal{H}$ into itself, called **Hermitian operators** (or, **self-adjoint operators**). If we think of linear transformations as matrices, then a **Hermitian operator** $\mathcal{O}$ is a square matrix of complex numbers such that

$$\overline{\mathcal{O}}^T = \mathcal{O}$$

where $\overline{\mathcal{O}}^T$ again denotes the matrix obtained from $\mathcal{O}$ by conjugating all its entries, and then transposing the matrix. As before, we denote $\overline{\mathcal{O}}^T$ by $\mathcal{O}^\dagger$, and refer to it as the **adjoint** of $\mathcal{O}$.

Let $|\varphi_i\rangle$ denote the eigenvectors, called **eigenkets**, of an observable $\mathcal{O}$, and let a_i denote the corresponding eigenvalue, i.e.,

$$\mathcal{O} : |\varphi_i\rangle = a_i\,|\varphi_i\rangle$$

In the cases we consider in this talk, the eigenkets form an orthonormal basis of the underlying Hilbert space $\mathcal{H}$.

[6]This is true for finite dimensional Hilbert spaces. It is more subtle for infinite dimensional Hilbert spaces.

Finally, we can answer our original question, i.e.,

What does an observer observe?

Let us suppose that we have a physical device M that is so constructed that it measures an observable $\mathcal{O}$, and that we wish to use M to measure a quantum system which just happens to be in a quantum state $|\Psi\rangle$. We assume $|\Psi\rangle$ is a ket of unit length. The quantum state $|\Psi\rangle$ can be written as a linear combination of the eigenkets of $\mathcal{O}$, i.e.,

$$|\Psi\rangle = \sum \alpha_i |\varphi_i\rangle$$

When we use the device M to measure $|\Psi\rangle$, we observe the eigenvalue a_i with probability $p_i = |\alpha_i|^2$, and in addition, after the measurement the quantum system has "collapsed" into the state $|\varphi_i\rangle$. Thus, the outcome of a measurement is usually random, and usually has a lasting impact on the state of the quantum system.

We can use Dirac notation to write down an expression for the average observed value. Namely, the **averaged observed value** is given by the expression $\langle\Psi|\,(\mathcal{O}\,|\Psi\rangle)$, which is written more succinctly as $\langle\Psi|\,\mathcal{O}\,|\Psi\rangle$, or simply as $\langle\mathcal{O}\rangle$.

4.10. **The Heisenberg uncertainty principle – A limitation on what we can actually observe.** There is, surprisingly enough, a limitation of what can be observed in quantum mechanics.

Two observables A and B are said to be **compatible** if they commute, i.e., if

$$AB = BA.$$

Otherwise, they are said to be **incompatible**.

Let $[A, B]$, called the **commutator** of A and B, denote the expression

$$[A, B] = AB - BA$$

In this notation, two operators A and B are compatible if and only if $[A, B] = 0$. Finally, let

$$\triangle A = A - \langle A\rangle$$

The following principle is one expression of how quantum mechanics places limits on what can be observed:

Heisenberg's Uncertainty Principle[7]

$$\left\langle (\triangle A)^2 \right\rangle \left\langle (\triangle B)^2 \right\rangle \geq \frac{1}{4} \left\| \langle [A, B] \rangle \right\|^2$$

[7]We have assumed units have been chosen such that $\hbar = 1$.

where $\left\langle (\triangle A)^2 \right\rangle = \langle \Psi | \, (\triangle A)^2 \, | \Psi \rangle$ is the **mean squared standard deviation** of the observed eigenvalue, written in Dirac notation. It is a measure of the uncertainty in A.

This if A and B are incompatible, i.e., do not commute, then, by measuring A more precisely, we are forced to measure B less precisely, and vice versa. We can not simultaneously measure both A and B to to unlimited precision. Measurement of A somehow has an impact on the measurement of B.

4.11. **Young's two slit experiment – An example of Heisenberg's uncertainty principle.** For the purpose of illustrating Heisenberg's Uncertainty Principle, Professor Dirac wheeled out into the classroom a device to demonstrate Young's two slit experiment. The device consisted of an electron gun which spewed out electrons[8] in the direction of a wall with two slits. The electrons that managed to pass through the two slits then impacted on a backstop which consisted of a 1600×1200 rectangular lattice of extremely small counters. From the back of the backstop, all of the 1,920,000 tiny counters on the backstop were individually connected to a PC by a cable consisting of a dense bundle of filaments.

Professor Dirac pointed to the PC, and explained that the PC was setup to display on the CRT's 1600×1200 pixel screen the individual running total counts of all the backstop counters . He went on to say that the intensity $P(i,j)$ of pixel (i,j) on the screen was proportional to the total number of electrons counted so far by the counter at position (i,j) in the backstop.

Professor Dirac proceeded to demonstrate what the device could actually do. He turned on the electron gun, and turned down its intensity so low that the probability of more than two electrons being emitted at the same time was negligibly small.

His first experiment with the device was to cover slit 2, allowing the incoming electrons to pass only through slit 1. He reset all the counters on the backstop to zero, and then stepped back to let the students in his class view the screen.

Initially nothing could be seen on the screen but blackness. However, gradually an intensity pattern began to form on the screen. At first the displayed pattern was indiscernible. But eventually it began to look like the intensity pattern of a classical two dimensional Gaussian distribution. He then pressed a key on his computer to show a three dimensional plot of the intensity $P(i,j)$ as a surface in 3-space. Then with the click of a mouse, he displayed a plot of the intensity $P(i,j)$ along the vertical line $j = 800$

[8]The original Young's two slit experiment used photons rather than electrons.

going down the center of the screen. The plot was that of the bell shaped classical one dimensional Gaussian distribution curve P_1, as shown in Fig. 3a. This was a clear indication that the random impacts on the backstop were obeying the classical Gaussian distribution.

When he repeated the experiment with the slit 1 instead of slit 2 covered, exactly the same pattern of a classical two dimensional Gaussian distribution pattern was seen, but only this time shifted vertically down a short distance on the screen. A plot of the intensity $P(i,j)$ of along the vertical line $j = 800$ going down the center of the screen is indicated by curve P_2 shown in Fig. 3a.

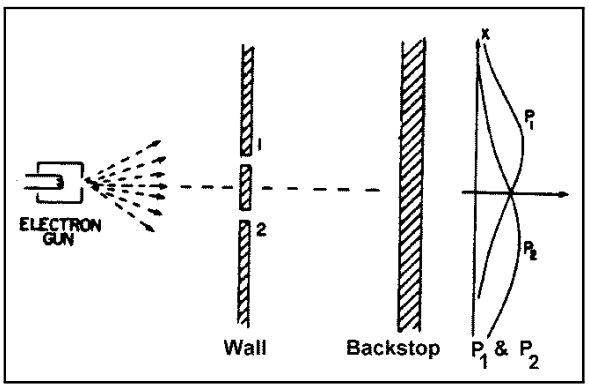

Figure 3a. Young's two slit experiment with one slit closed.

Professor Dirac then asked the students in the class what pattern they thought would appear if he left both of the slits uncovered. Most of the class responded by saying that the resulting light pattern would simply be the sum of the two patterns, i.e., the bell shaped curve $P_1 + P_2$, as illustrated in Fig. 3c by the curve labeled P'_{12}. Most of the class was convinced that the two classical probability distributions would simply add, as many of them had learned in the probability course Prob 323.

The remainder of the class stated quite emphatically that they did not care what happened. What was being illustrated was far from an applied area, and hence not relevant to their real world. Or so they thought ...

Professor Dirac smiled, and then proceeded to uncover both slits. What appeared on the screen to almost everyone's surprise was not the pattern with the bell shape $P_1 + P_2$. It was instead a light pattern with a wavy bell shaped curve, as illustrated by the curve P_{12} in Fig. 3b.

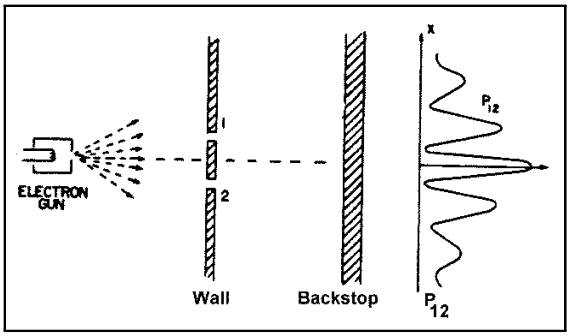

Figure 3b. Young's two slit experiment with both slits open.

Professor Dirac explained, "Something non-classical had occurred. Unlike classical probabilities, the quantum probabilities (or more correctly stated, the quantum amplitudes) had interfered with one another to produce an interference pattern. In the dark areas, one finds destructive interference. In the bright areas, one finds constructive interference."

"Indeed, something non-classical is happening here."

"Strangely enough, quantum mechanics is telling us that each electron is actually passing through both slits simultaneously! It is as if each electron were a wave and not a particle."

"But what happens when we actually try to observe through which slit each electron passes?"

Professor Dirac pulled out his trusty microscope[9] to observe which of the two slits each electron passed through. He reset all the backstop counters to zero, turned on the device, and began observing through which slit each electron passed through. The class was much surprised to find that the wavey interference pattern did not appear on the screen this time. Instead, what appeared was the classical intensity pattern all had initially expected to see in the first place, i.e., the intensity pattern of the bell shaped curve $P_{12} = P_1 + P_2$, as shown in Fig. 3c.

"So we see that, when observed, the electrons act as particles and not as waves!"

[9]This is a most unusual microscope.

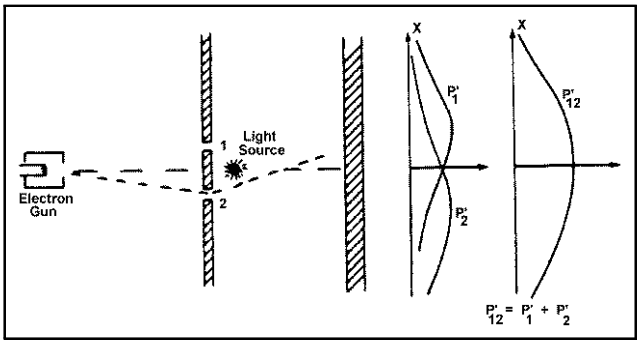

Figure 3c. Young's 2 slit experiment when the slit through which the electron passes is determined by observation.

After a brief pause, Professor Dirac said, "This is actually an example of the Heisenberg Uncertainty Principle. We can see this as follows:"

"In the experiment, we are effectively observing two incompatible observables, the position operator X (i.e., which slit each electron passes through) and the momentum operator P (i.e., the momentum with which each electron leaves the slitted wall.) When we observe the momentum P, the interference pattern is present. But when we observe the position X, the interference pattern vanishes. We can not observe position without disturbing momentum, and vice versa."

5. The Beginnings of Quantum Cryptography

5.1. **Alice has an idea.** After class on her way back to her dorm room, Alice began once again to ruminate over her dilemma in regard to Bob and Eve.

"If only her message to Bob were like the interference pattern in Young's two slit experiment. Then, if the prying Eve were to observe which of the two slits each of the electrons emerged from (i.e., 'listen in'), Bob would know of her presence. For, if Eve were observing the individual electrons as they left the slits, the pattern on the screen would distorted from the beautiful wavy interference pattern in a direction toward the dull ugly Gaussian distribution pattern. Bob would see this distortion, and thereby be able to surmise that Eve was eavesdropping."

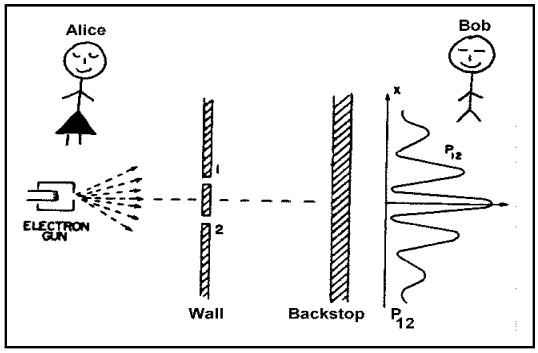

Figure 4a. Bob sees an interference pattern when Eve is not eavesdropping.

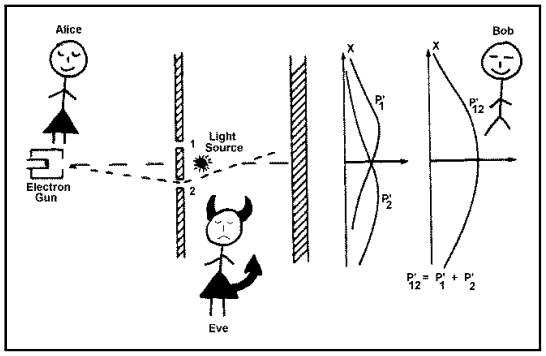

Figure 4b. Bob sees no interference pattern when Eve is eavesdropping.

"This idea has possibilities. Maybe quantum mechanics is relevant after all!"

Her mind began to race. "Perhaps something like Young's two slit experiment could be used to communicate random key K? Then Bob could tell which key had been compromised by an intruder such as Eve. But most importantly, he could also surmise which key had not been compromised. Bob could then communicate to me over the phone (or even over any public channel available also to Eve) whether or not the key had been compromised, without, of course, revealing the key itself. Any uncompromised key could then be employed to send Bob a message by using the one-time-pad that was mentioned yesterday in Crypto 351."

"The beauty of this approach is that the one-time-pad is perfectly secure. There is no way whatsoever that Eve could get any information about our conversation. This would be true even if I used the campus radio station to send my encrypted message."

"The evil Eve is foiled! Eureka! Contrary to student conventional wisdom, both cryptography and quantum mechanics are relevant to the real world!"

"I have discovered a new kind of secrecy, i.e., quantum secrecy, which has built-in detection of eavesdropping based on the principles of quantum mechanics. I can hardly wait to tell Professor Dirac. She ran immediately to his office."

After listening to Alice's excited impromptu, and at times disjointed, explanation, Professor Dirac suggested that she present her newly found discoveries in his next class. Alice happily agreed to do so.

5.2. **Quantum secrecy – The BB84 protocol without noise.** Two days later, after two sleepless but productive nights of work, Alice was prepared for her presentation. She walked in the classroom for Quantum 317 carrying an overhead projector and a sizable bundle of transparencies.

After Professor Dirac had turned the large lecture hall over to her, she began as follows:

"Let us suppose that I (Alice) would like to transmit a secret key K to Bob. Let us also suppose that someone by the name of Eve intends to make every effort to eavesdrop on the transmission and learn the secret key."

Wouldn't you know it. Eve just so happens to be sitting in the classroom!

"My objective today is to show you how the principles of quantum mechanics can be used to build a cryptographic communication system in such a way that the system detects if Eve is eavesdropping, and which also gives a guarantee of no intrusion if Eve is not eavesdropping."

"A diagrammatic outline of the system I'm about to describe is shown on the screen. (Please refer to Fig. 5.) Please note that the system consists of two communication channels. One is a non-classical one-way quantum communication channel, which I will soon describe. The other is an ordinary run-of the-mill classical two-way public channel, such as a two-way radio communication system. I emphasize that this classical two-way channel is public, and open to whomever would like to listen in. For the time being, I will assume that the two-way public channel is noise free."

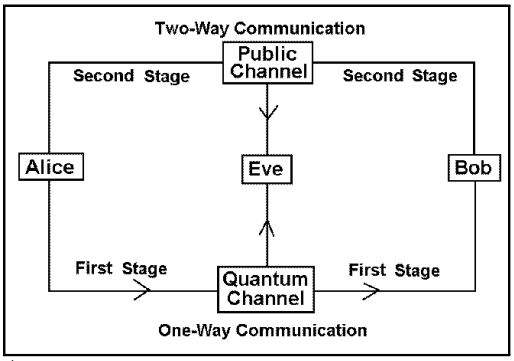

Figure 5. A quantum cryptographic communication system.

"I will now describe how the polarization states of the photon can be used to construct a quantum one-way communication channel[10]."

"From Professor Dirac's last lecture, we know that the polarization states of a photon lie in a two dimensional Hilbert space $\mathcal{H}$. For this space, there are many orthonormal bases. We will use only two for our quantum channel."

"The first is the basis consisting of the vertical and horizontal polarization states, i.e., the kets $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$, respectively. We will refer to this

[10]Any two dimensional quantum system such as a spin $\frac{1}{2}$ particle could be used.

orthonormal basis as the **vertical/horizontal (V/H) basis**, and denote this basis with the symbol '$\boxplus$.' "

"The second orthonormal basis consists of the polarization states $|\nearrow\rangle$ and $|\nwarrow\rangle$, which correspond to polarizations directions formed respectively by 45% clockwise and counter-clockwise rotations off from the vertical. We call this the **oblique basis**, and denote this basis with the symbol '$\boxtimes$.' "

"If I (Alice) decide to use the VH basis $\boxplus$ on the quantum channel, then I will use the following **quantum alphabet**:

$$\begin{cases} \text{“1”} & = & |\updownarrow\rangle \\ \text{“0”} & = & |\leftrightarrow\rangle \end{cases}$$

In other words, if I use this quantum alphabet on the quantum channel, I will transmit a "1" to Bob simply by sending a photon in the polarization state $|\updownarrow\rangle$., and I will transmit a "0" by sending a photon in the polarization state $|\leftrightarrow\rangle$."

"On the other hand, if I (Alice) decide to use the oblique basis $\boxtimes$, then I will use the following **quantum alphabet**:

$$\begin{cases} \text{“1”} & = & |\nearrow\rangle \\ \text{“0”} & = & |\nwarrow\rangle \end{cases},$$

sending a "1" as a photon in the polarization state $|\nearrow\rangle$, and sending a "0" as a photon in the polarization state $|\nwarrow\rangle$."

"I have chosen these two bases because the Heisenberg Uncertainty Principle implies that observations with respect to the $\boxplus$ basis are incompatible with observations with respect to the $\boxtimes$ basis. We will soon see how this incompatibility can be translated into intrusion detection."

Alice	$\boxplus$	$\boxtimes$	$\boxtimes$	$\boxtimes$	$\boxplus$	$\boxtimes$	$\boxplus$	$\boxtimes$	$\boxplus$	$\boxtimes$
	$\updownarrow$	$\nwarrow$	$\nwarrow$	$\nearrow$	$\updownarrow$	$\nwarrow$	$\leftrightarrow$	$\nearrow$	$\leftrightarrow$	$\nearrow$
	1	0	0	1	1	0	0	1	0	1
		*		*				*		*
Bob	$\boxtimes$	$\boxtimes$	$\boxplus$	$\boxtimes$	$\boxplus$	$\boxtimes$	$\boxplus$	$\boxplus$	$\boxplus$	$\boxplus$
	1	0	1	1	1	0	0	0	0	0
Raw Key⇒		0		1	1	0	0		0	

Fig. 6a. The BB84 protocol without Eve present (No noise)

Alice and Bob now communicate with one another using a two stage protocol, called the **BB84 protocol**[?]. (Please refer to Figs. 6a and 6b.)

In stage 1, Alice creates a random sequence of bits, which she sends to Bob over the quantum channel using the following protocol:

Stage 1 protocol: Communication over a quantum channel

Step 1. Alice flips a fair coin to generate a random sequence S_{Alice} of zeroes and ones. This sequence will be used to construct a secret key shared only by Alice and Bob.

Step 2. For each bit of the random sequence, Alice flips a fair coin again to choose at random one of the two quantum alphabets. She then transmits the bit as a polarized photon according to the chosen alphabet.

Step 3. Each time Bob receives a photon sent by Alice, he has no way of knowing which quantum alphabet was chosen by Alice. So he simply uses the flip of a fair coin to select one of the two alphabets and makes his measurement accordingly. Half of the time he will be lucky and choose the same quantum alphabet as Eve. In this case, the bit resulting from his measurement will agree with the bit sent by Alice. However, the other half of the time he will be unlucky and choose the alphabet not used by Alice. In this case, the bit resulting from his measurement will agree with the bit sent by Alice only 50% of the time. After all these measurements, Bob now has in hand a binary sequence S_{Bob}.

Alice and Bob now proceed to communicate over the public two-way channel using the following stage 2 protocol:

Stage 2 protocol: Communication over a public channel

Phase 1. *Raw key extraction*

Step 1. Over the public channel, Bob communicates to Alice which quantum alphabet he used for each of his measurements.

Step 2. In response, Alice communicates to Bob over the public channel which of his measurements were made with the correct alphabet.

Step 3. Alice and Bob then delete all bits for which they used incompatible quantum alphabets to produce their resulting **raw keys**. If Eve has not eavesdropped, then their resulting raw keys will be the same. If Eve has eavesdropped, their resulting raw keys will not be in total agreement.

Phase 2. *Error estimation*

Step 1. Over the public channel, Alice and Bob compare small portions of their raw keys to estimate the error-rate R, and then delete the disclosed bits from their raw keys to produce their **tentative final keys**. If through their public disclosures, Alice and Bob find no errors (i.e., $R = 0$), then they know that Eve was not eavesdropping and that their tentative keys must be the same **final key**. If they discover at least one error during their public disclosures (i.e., $R > 0$), then they know that Eve has been eavesdropping. In this case, they discard their tentative final keys and start all over again[11].

Alice	⊞	⊠	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊠
	↕	↖	↖	↗	↕	↖	↔	↗	↔	↗
	1	0	0	1	1	0	0	1	0	1

Eve	⊠	⊞	⊞	⊠	⊞	⊞	⊠	⊠	⊞	⊞
	1	0	1	1	1	1	0	1	0	0

Bob	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊞	⊞	⊞
	1	0	1	1	1	1	1	0	0	0
	*	0	*	1	1	1	1	*	0	*
						E	E			

Fig 6b. The BB84 with Eve present (No noise)

5.3. **Quantum secrecy – The BB84 protocol with noise.** Alice continues her presentation by addressing the issue of noise.

"So far we have assumed that our cryptographic communication system is noise free. But every realistic communication system has noise present. Consequently, we now need to modify our quantum protocol to allow for the presence of noise."

"We must assume that Bob's raw key is noisy. Since Bob can not distinguish between errors caused by noise and by those caused by Eve's intrusion, the only practical working assumption he can adopt is that all errors are caused by Eve's eavesdropping. Under this working assumption, Eve is always assumed to have some information about bits transmitted from Alice to Bob. Thus, raw key is always only **partially secret**."

[11]If Eve were to intercept each qubit received from Alice, to measure it, and then to masqurade as Alice by sending on to Bob a qubit in the state she measured, then Eve would be introducing a 25% error rate in Bob's raw key. This method of eavesdropping is called **opaque eavesdropping**. We will discuss this eavesdropping strategy as well as others at a later time.

"What is needed is a method to distill a smaller secret key from a larger partially secret key. We call this **privacy amplification**. We will now create from the old protocol a new protocol that allows for the presence of noise, a protocol that includes privacy amplification."

Stage 1 protocol: Communication over a quantum channel

This stage is exactly the same as before, except that errors are now also induced by noise.

Stage 2 protocol: Communication over a public channel

Phase 1 protocol: Raw key extraction.

This phase is exactly the same as in the noise-free protocol, except that Alice and Bob also delete those bit locations at which Bob should have received but did not receive a bit. Such "non-receptions" could be caused by Eve's intrusion or by **dark counts** in Bob's detection device. The location of dark counts are communicated by Bob to Alice over the public channel.

Phase 2 protocol: Error estimation.

Over the public channel, Alice and Bob compare small portions of their raw keys to estimate the error-rate R, and then delete the disclosed bits from their raw key to produce their **tentative final keys**. If R exceeds a certain threshold R_{Max}, then privacy amplification is not possible If so, Alice and Bob return to stage 1 to start over. On the other hand, if $R \leq R_{Max}$, then Alice and Bob proceed to phase 3.

Phase 3 protocol: Extraction of reconciled key[12].

In this phase[13], Alice and Bob remove all errors from what remains of raw key to produce a common error-free key, called **reconciled key**.

Step 1. Alice and Bob publically agree upon a random permutation, and apply it to what remains of their respective raw keys. Next Alice and Bob partition the remnant raw key into blocks of length ℓ, where the length ℓ is chosen so that blocks of that length are unlikely to have more than one error. For each of these blocks, Alice and Bob publically compare overall parity checks, making sure each time to discard the last bit of each compared block. Each time an

[12]There are more efficient and elegant procedures than the procedure descibed in Stage 2 Phase 3. See [13] for references.

[13]The procedure given in Stage 2 Phase 3 is only one of many different possible procedures. In fact, there are much more efficient and elegant procedures than the one described herein.

overall parity check does not agree, Alice and Bob initiate a binary search for the error, i.e., bisecting the block into two subblocks, publically comparing the parities for each of these subblocks, discarding the right most bit of each subblock. They continue their bisective search on the subblock for which their parities are not in agreement. This bisective search continues until the erroneous bit is located and deleted. They then continue to the next ℓ-block.

This step is repeated, i.e., a random permutation is chosen, a remnant raw key is partitioned into blocks of length ℓ, parities are compared, etc.. This is done until it becomes inefficient to continue in this fashion.

Step 2. Alice and Bob publically select randomly chosen subsets of remnant raw key, publically compare parities, each time discarding an agreed upon bit from their chosen key sample. If a parity should not agree, they employ the binary search strategy of Step 1 to locate and delete the error.

- Finally, when, for some fixed number N of consecutive repetitions of Step 2, no error is found, Alice and Bob assume that to a high probability, the remnant raw key is without error. Alice and Bob now rename the remnant raw key **reconciled key**, and proceed to the next phase.

Phase 4: Privacy amplification

Alice and Bob now have a common reconciled key which they know is only partially secret from Eve. They now begin the process of **privacy amplification**, which is the extraction of a secret key from a partially secret one.

Step 1. Alice and Bob compute from the error-rate R obtained in Phase 2 of Stage 2 an upper bound k of the number of bits of reconciled key known by Eve.

Let n denote the number of bits in reconciled key, and let s be a **security parameter** to be adjusted as required.

Step 2. Alice and Bob publically select $n-k-s$ random subsets of reconciled key, without revealing their contents. The undisclosed parities of these subsets become the final secret key.

It can be shown that Eve's average information about the final secret key is less than $2^{-s}/\ln 2$ bits.

The bell rang, indicating the end of the period. The entire class with two exceptions, immediately raced out of the lecture hall, almost knocking Alice

down as they passed by. Professor Dirac thanked Alice for an excellent presentation.

As Alice left, she saw Eve in one of the dark recesses of the large lecture hall with her head resting on the palm of her hand as if in deep thought. She had a frown on her face. Alice left with a broad smile on her face.

6. The B92 quantum cryptographic protocol

In the next class, Alice continued her last presentation.

In thinking about the BB84 protocol this weekend, I was surprised to find that it actually is possible to build a different quantum protocol that uses only one quantum alphabet instead of two. I'll call this new quantum protocol **B92**."

"As before, we will describe the protocol in terms of the polarization states of the photon[14]."

"As our quantum alphabet, we choose

$$\begin{cases} \text{“1”} & = & |\theta_+\rangle \\ \\ \text{“0”} & = & |\theta_-\rangle \end{cases} ,$$

where $|\theta_+\rangle$ and $|\theta_-\rangle$ denote respectively the polarization states of a photon linearly polarized at angles θ and $-\theta$ with respect to the vertical, where $0 < \theta < \frac{\pi}{4}$."

"We assume that Bob's quantum receiver, called a **POVM receiver**[3], is base on the following observables[15]:

$$\begin{cases} A_{\theta_+} & = & \frac{1 \, - \, |\theta_-\rangle\langle\theta_-|}{1 \, + \, \langle\theta_+|\theta_-\rangle} \\ \\ A_{\theta_-} & = & \frac{1 \, - \, |\theta_+\rangle\langle\theta_+|}{1 \, + \, \langle\theta_+|\theta_-\rangle} \\ \\ A_? & = & 1 - A_{\theta_+} - A_{\theta_-} \end{cases} ,$$

where A_{θ_+} is the observable for $|\theta_+\rangle$, A_{θ_-} the observable for $|\theta_-\rangle$ and $A_?$ is the observables for inconclusive receptions."

The **B92** quantum protocol is as follows:

Stage 1 protocol. Communication over a quantum channel.

Step 1. The same as in the BB84 protocol. Alice flips a fair coin to generate a random sequence S_{Alice} of zeroes and ones. This sequence will be used to construct a secret key shared only by Alice and Bob.

[14]Any two dimensional quantum system such as a spin $\frac{1}{2}$ particle could be used.

[15]The observables A_{θ_+}, A_{θ_-}, and $A_?$ form a postive operator value measure (POVM).

Step 2. The same as in the previous protocol, except this time Alice uses only one alphabet, the one above. So she does not have to flip a coin to choose an alphabet.

Step 3. Bob uses his POVM receiver to measure photons received from Alice.

Stage 2. Communication in four phases over a public channel.

This stage is the same as in the BB84 protocol, except that in phase 1, Bob publically informs Alice as to which time slots he received non-erasures. The bits in these time slots become Alice's and Bob's raw keys.

Alice completed her discussion of the B92 protocol with,

"Eve's presence is again detected by an unusual error rate in Bob's raw key. Moreover, for some but not all eavesdropping strategies, Eve can also be detected by an unusual erasure rate for Bob."

Alice then stepped down from the lecture hall podium and returned to her seat.

7. There are many other quantum cryptographic protocols

Before continuing our story about Alice, Bob, and Eve, there are a few points that need to be made:

There are many other quantum cryptographic protocols. Quantum protocols showing the greatest promise for security are those based on EPR pairs. Unfortunately, the technology for implementing such protocols is not yet available. For references on various protocols, please refer to [13].

8. A comparison of quantum cryptography with classical and public key cryptography

Quantum cryptography's unique contribution is that it provides a mechanism for eavesdropping detection. This is an entirely new contribution to cryptography. On the other hand, one of the main drawbacks of quantum cryptography is that it provides no mechanism for authentication, i.e., for detecting whether or not Alice and Bob are actually communicating with each other, and not with an intermediate Eve masquerading as each of them. Thus, the Catch 22 problem is not solved by quantum cryptography. Before Alice and Bob can begin their quantum protocol, they first need to send an authentication key over a secure channel.

Thus, quantum cryptography's unique contribution is to provide a means of expanding existing secure key. Quantum protocols are secure key expanders. First a small authentication key is exchanged over a secure

channel. Then that key can be amplified to an arbitrary length through quantum cryptography.

Check List for Q. Crypto. Sys.	
■ Catch 22 Solved?	**YES & NO**
■ Authentication?	**NO**
■ Intrusion Detection?	**YES**

9. Eavesdropping strategies and counter measures

Now let us resume our story:

Not a split second after Alice had seated herself, Eve raised her hand and asked for permission to make her own presentation to the class. Professor Dirac yielded the podium, not knowing exactly what to expect, but nonetheless elated that his usually phlegmatic class was beginning to show signs of something he had not seen for some time, class participation and initiative.

Eve began, "In the last two classes, Alice has suggested that I (Eve) might be eager to eavesdrop on her conversations with my ♡close♡ friend ♡Bob♡. I assure you that simply is in no way true."

"But such innuendo really doesn't bother me."

9.1. **Opaque eavesdropping.** "What really irks me is that Alice suggests that, if I were to eavesdrop (which never would happen), then I (Eve) would use **opaque eavesdropping**. By **opaque eavesdropping**, I mean that I (Eve) would intercept and observe (measure) Alice's photons, and then masquerade as Alice by sending photons in the states I had measured on to Bob."

"I assure you that, if I ever wanted to eavesdrop (which will never be the case), I would not use such a simplistic form of intrusion."

Eve really wanted to use the adjective 'stupid' instead of 'simplistic,' but restrained herself.

Eve then said indignantly, "If I ever were to eavesdrop (which would never happen), I would use more sophisticated, more intelligent, and yes ... , more deliciously devious schemes!"

9.2. **Translucent eavesdropping without entanglement.** "I (Eve) could for example make my probe interact unitarily with the information carrier from Alice, and then let it proceed on to Bob in a slightly modified state. For the B92 protocol, the interaction is given by:

$$\begin{cases} |\theta_+\rangle\,|\psi\rangle \longmapsto U\,|\theta_+\rangle\,|\psi\rangle = \left|\theta'_+\right\rangle|\psi_+\rangle \\ |\theta_-\rangle\,|\psi\rangle \longmapsto U\,|\theta_-\rangle\,|\psi\rangle = \left|\theta'_-\right\rangle|\psi_-\rangle \end{cases},$$

where $|\psi\rangle$ and $|\psi_\pm\rangle$ denote respectively the state of my (Eve's) probe before and after the interaction and where $|\theta_\pm\rangle$ and $\left|\theta'_\pm\right\rangle$ denote respectively the state of Alice's photon before and after the interaction."

9.3. **Translucent eavesdropping with entanglement.** "Another approach, one of the most sophisticated, would be for me (EVE) to entangle my probe with the information carrier from Alice, and then let it proceed on to Bob. For the B92 protocol, the interaction is given by:

$$\begin{cases} |\theta_+\rangle\,|\psi\rangle \longmapsto U\,|\theta_+\rangle\,|\psi\rangle = a\left|\theta'_+\right\rangle|\psi_+\rangle + b\left|\theta'_-\right\rangle|\psi_+\rangle \\ |\theta_-\rangle\,|\psi\rangle \longmapsto U\,|\theta_-\rangle\,|\psi\rangle = b\left|\theta'_+\right\rangle|\psi_-\rangle + a\left|\theta'_-\right\rangle|\psi_-\rangle \end{cases},$$

where $|\psi\rangle$ and $|\psi_\pm\rangle$ denote respectively the state of my (Eve's) probe before and after the entanglement and where $|\theta_\pm\rangle$ and $\left|\theta'_\pm\right\rangle$ denote respectively the state of Alice's photon before and after the entanglement."

9.4. **Eavesdropping based on implementation weaknesses.** "On the other hand, I could also take advantage of implementation weaknesses."

"One of the great difficulties with quantum cryptography is that technology has not quite caught up with it. Many devices, such as lasers, do not emit a single quantum, but many quanta at each emission time. The implementation of quantum protocols really requires single-quantum emitters. Such single-quantum emitters are now under development. Until such emitters become available, the quantum protocols can only be approximately implemented."

"For example, for many optical implementations of quantum protocols, the laser intensity is turned down so that on the average only one photon is produced every 10 pulses. Thus, if anything is emitted at all (one chance out of 10), then the probability that it is a single photon is extremely high. However, when there is an emission, then there is a probability of $\frac{1}{200}$ that more than one photon is emitted. So it is conceivable that I (Eve) could build an eavesdropping device that would detect multiple photon transmissions, and, when so detected, would divert one of the photons for measurement. In this way, I (Eve) could conceivably read $\frac{1}{200}$ of Alice's transmission without being detected. One way of countering this type of threat is to allow for it

during privacy amplification. Another is to develop devices which actually truly emit one quanta at a time."

"Finally, depending on Alice's implementation, it might also be possible for me (Eve) to gain information simply by observing Alice's transmitter without measuring its output. This may or may not be far fetched."

Eve then returned to her seat. Her face was lit up with a sinister grin of satisfaction.

10. Implementations

Before continuing our story, we should mention that quantum cryptographic protocols have been implemented over more than 30 kilometers of fiber optic cable, [20],[21],[22], [23], and most amazingly, over more than a kilometer of free space [4], [5], [11],[9], [10] in the presence of ambient sunlight. There have been a number of ambitious proposals to demonstrate the feasibility of quantum cryptography in earth to satellite communications. And as mentioned earlier, there is a clear need for the development of single-quantum emitting devices.

11. Conclusion

Much remains to be done. There has been some work on the development of multiple-user quantum cryptographic protocols for communication networks[24]. There also have been at least two independent claims of the proof of ultimate security, i.e., a proof that quantum cryptographic protocols are impervious to all possible eavesdropping strategies [12], [15], [16], [17].

Our story continues:

As Alice sat in her seat, she happened to spy in the corner of her eye an abrupt change in Eve's demeanor. Eve suddenly became agitated, lit up with excitement, and started to frantically write on her notepad. The bell rang. Eve immediately jumped up, and raced out of the lecture hall, being pushed along by the usual frantic mass of students, equally eager to get out of the classroom.

As Eve whisked past, Alice caught just a fleeting glimpse of Eve's notepad. All Alice was able to discern in that brief moment was an illegible jumble of equations and ... yes, ... the acronym "POVM."

Alice thought to herself, "Oh, well! ... Forget it! I think I'll just visit Bob this weekend."

THE END[16]

12. Acknowledgement

I would like to thank Howard Brandt and Lov Grover for their helpful suggestions. I would also like to thank the individuals who attended my talk. Their many comments and insights were of invaluable help in writing this paper. Thanks are also due to the NIST Computer Security Division for providing an encouraging environment in which this paper could be completed.

References

[1] Bennett, Charles H., and Gilles Brassard, **Quantum cryptography: Public key distribution and coin tossing**, International Conference on Computers, Systems & Signal Processing, Bagalore, India, December 10-12, 1984, pp 175 - 179.

[2] Biham, Eli, and Adi Shamir, "**Differential Crytanalysis of the Data Encryption Standard**," Springer-Verlag (1993).

[3] Brandt, Howard E., John M. Meyers, And Samuel J. Lomonaco,Jr., **Aspects of entangled translucent eavesdropping in quantum cryptography**, Phys. Rev. A, Vol. 56, No. 6, December 1997, pp. 4456 - 4465.

[4] Buttler, W.T., R.J. Hughes, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, C.G. Peterson, **Daylight quantum key distribution over 1.6 km**, quant-ph/0001088.

[5] Buttler, W.T., R.J. Hughes, P.G. Kwiat, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C.M. Simmons, **Free-space quantum ket distribution**, Phys. Rev. A ,(1998). (quant-ph/9801006).

[6] Dieks, D., Phys. Lett., **92**, (1982), p 271.

[7] Diffie, W., **The first ten years in public-key cryptography**, in "Contemporary Cryptology: The Science of Information Integrity," pp 135 - 175, IEEE Press (1992).

[8] Diffie, W., and M.E. Hellman, **New directions in cryptography**, IEEE Tranactions on Information Theory, **22** (1976), pp 644 - 654.

[9] Franson, J.D., and H. Ilves, **Quantum cryptography using polarization feedback,** Journal of Modern Optics, Vol. 41, No. 12, 1994, pp 2391 - 2396.

[10] Hughes, Richard J., William T. Buttler, Paul G. Kwiat, Steve K. Lamoreaux, George L. Morgan, Jane E. Nordholt, C. G. Peterson, **Practical quantum cryptography for secure free-space communications**, PRL (2000). (quant-ph/9905009).

[11] Jacobs, B.C. and J.D. Franson, **Quantum cryptography in free space**, Optics Letters, Vol. 21, November 15, 1996, p1854 - 1856.

[12] Lo, H.-K, and H.F. Chau, **Quantum computers render quantum key distribution unconditionally secure over arbitrarily long distance**, quant-ph/9803006.

[13] Lomonaco, Samuel J., **A quick glance at quantum cryptography**, Cryptologia, Vol. 23, No. 1, January, 1999, pp1-41. (quant-ph/9811056)

[14] Matsui, Mitsuru, **Linear crytanalysis method for DES cipher**, Lecture Notes in Computer Science, vol. 765, edited by T. Helleseth, Springer-Verlag (1994), pp386-397.

[15] Mayers, Dominic, Crypto'96, p343.

[16] Mayers, Dominic, and Andrew Yao, **Quantum cryptography with imperfect apparatus**, quant-ph/9809039.

[16] Any resemblance of the characters in this manuscript to individuals living or dead is purely coincidental.

[17] Mayers, Dominic, **Unconditional security in quantum cryptography**, quant-ph/9802025.

[18] Menezes, Alfred J., Paul C. van Oorschot, and Scott A. Vanstone, "Handbook of Applied Cryptography," CRC Press (1977).

[19] O'Reilly, Tim, and the Electronic Frontier Foundation, "Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design," (1st Edition), July 1998 (US) ISBN 1-56592-520-3 (272 pages) http://www.ora.com/catalog/crackdes/

[20] Phoenix, Simon J., and Paul D. Townsend, **Quantum cryptography: how to beat the code breakers using quantum mechanics**, Comtemporay Physics, vol. 36, No. 3 (1995), pp 165 - 195.

[21] Townsend, P.D., **Secure key distribution system based on quantum cryptography**, Electronic Letters, 12 May 1994, Vol. 30, No. 10, pp 809 - 811.

[22] Townsend, Paul D., and I Thompson, Journal of Modern Optics, **A quantum key distribution channel based on optical fibre**, Vol. 41, No. 12, 1994, pp 2425 - 2433.

[23] Townsend, P.D., J.G. Rarity, and P.R. Tapster, **Single photon interference in 10km long optical fibre interferometer,** Electronic Letters, **29** (1993), pp 634 - 635.

[24] Townsend, P.D., Nature 385, (1997), p 47.

[25] Wootters, W.K., and W.H. Zurek, **A single quantum cannot be cloned**, Nature, 299 (1982), pp982-983.

University of Maryland Baltimore County, Baltimore, MD 21250
E-mail address: Lomonaco@UMBC.EDU
URL: http://www.umbc.edu/~lomonaco