A Talk on Quantum Cryptography

or

How Alice Outwits Eve

by

Samuel J. Lomonaco,Jr.

CSEE Department
University of Marland Baltimore County
Baltimore, MD 21250

Email: Lomonaco@UMBC.EDU
WebPage: http://www.umbc.edu/~lomonaco

Quantum Cryptography provides a new mechanism enabling the parties communicating with one another to:

Automatically detect eavesdropping.

Consequenty, it provides a means of determining when ~~a communi~~ an encrypted communication has been compromised.

3

TYPES OF COMMUNICATION SECURITY

- PERFECT SECURITY(Shannon, 1949)

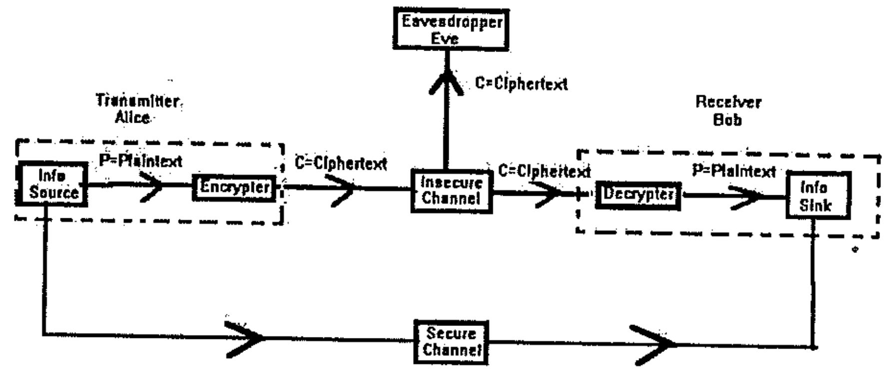
  Ciphertext C without key gives no information plaintext P

  $$\text{Prob}(P \mid C) = \text{Prob}(P)$$

- PRACTICAL SECRECY(Circa 10^6 BC)

  Cipher text breakable after x years

  Example: DES



A Classical Cryptographic Communication System

TYPES OF COMMUNICATION SECURITY (Cont.)

- COMPUTATIONAL SECURITY(Diffie-Hellman, circa 1970)

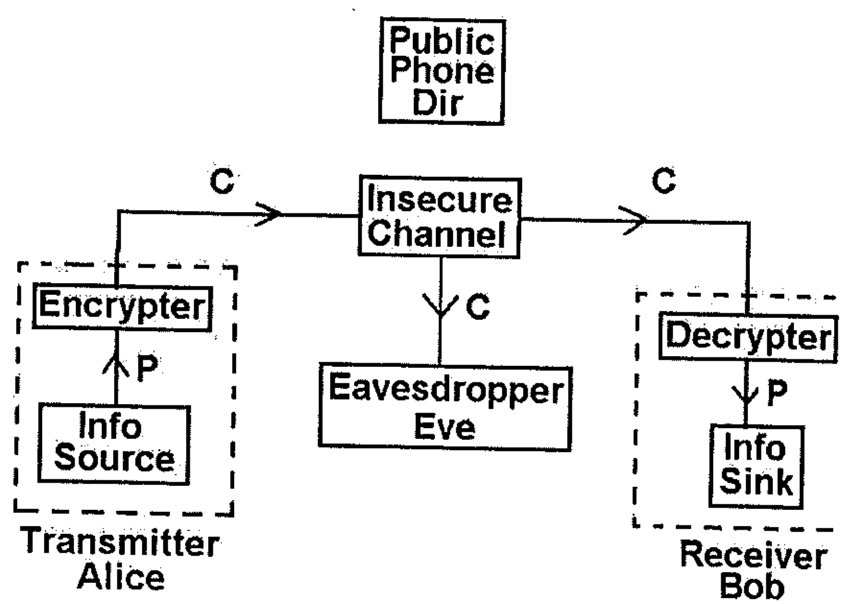
  Public Key Cryto Systems

  Example: RSA

- COMPUTATIONAL SECURITY(Diffie-Hellman, circa 1970)

  Public Key Cryto Systems

  Example: RSA



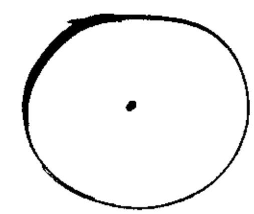
- PROBLEM: Long random bit sequences must be sent over a secure channel

- CATCH 22: There are perfectly good ways to communicate in secret provided we can communicate in secret ...

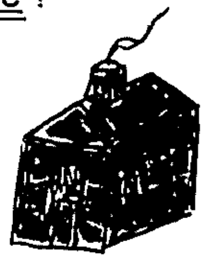
- KEY PROBLEM IN CRYPTOGRAPHY: Need some way of securely communicating key.

The Classical World

The Quantum World



Where does a Qubit Live ?

$\mathcal{H}$ =  Home

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

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

such that

1) $\langle u_1 + u_2,\ v \rangle = \langle u_1,\ v \rangle + \langle u_2,\ v \rangle$ and
   $\langle u,\ v_1 + v_2 \rangle = \langle u,\ v_1 \rangle + \langle u,\ v_2 \rangle$
2) $\langle u,\ \lambda v \rangle = \lambda \langle u,\ v \rangle$
3) $\overline{\langle u,\ v \rangle} = \langle v,\ u \rangle$
4) For ever Cauchy sequence $u_1,\ u_2,\ u_3,\ \ldots$ in $\mathcal{H}$,

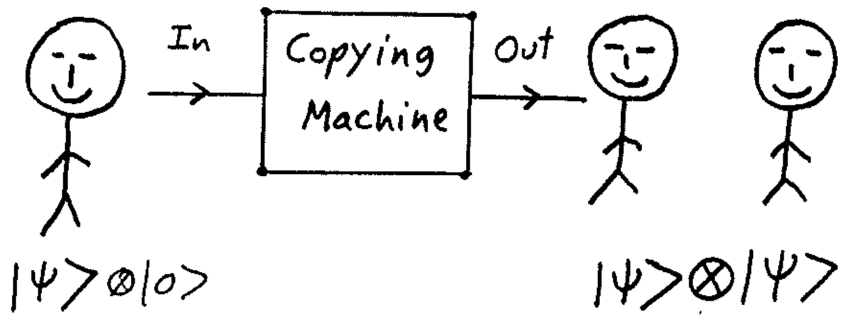
$$\lim_{n \to \infty} u_n \in \mathcal{H}$$

The elements of $\mathcal{H}$ will be called **kets**, and will be denoted by

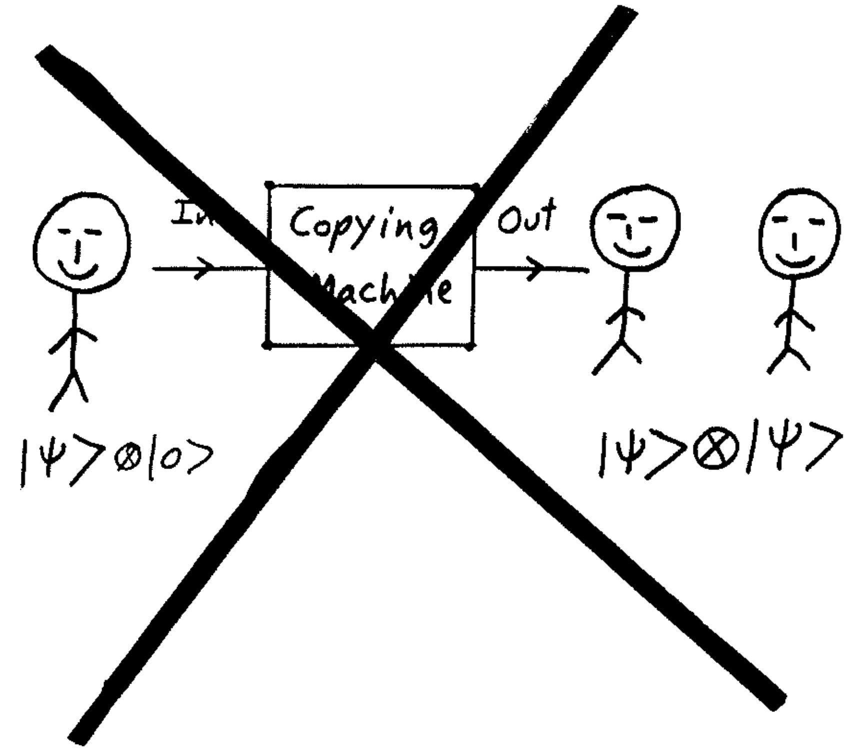
$$|\ \text{label}\ \rangle$$

A qubit is a Ket (State) in a 2-D Hilbert Space $\mathcal{H}$

Quantum Copying Machine ?



Quantum Copying Machine ?



Wootters & Zurek

& Dieks

No Cloning Theorem

Dirac Notation (Cont.)

$(\hbar = 1)$

- Consider a Quantum System in the state

$$|\psi\rangle \qquad \text{Ket}$$

- Suppose we measure many times the observable

$$A \qquad \text{Hermitian operator}$$

- Then the average value for many measurements of A is:

$$\langle\psi|\big(A|\psi\rangle\big) = \langle\psi|A|\psi\rangle$$

$$= \langle A\rangle$$

Avg. of A

Definition 0.1 Observables A and B are COMPATIBLE if

$$[A, B] = AB - BA = 0$$

Otherwise, A and B are INCOMPATIBLE.

Let

$$\Delta A = A - \langle A\rangle$$

HEISENBERG'S UNCERTAINTY PRINCIPLE

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

$\left\langle(\Delta A)^2\right\rangle$ is the the STANDARD DEVIATION. It is a measure in the uncertainty in the observable A.

$\{\hbar = 1\}$

Observables

$$\begin{cases} X & \text{Position Operator} \\ P & \text{Momentum operator} \end{cases}$$

Note: X & P are incompatible observables; for:

$$[X, P] = -i \neq 0$$

Therefore, by Heisenberg's uncertainty Principle,

$$\underbrace{\langle (\Delta X)^2 \rangle}_{\text{uncertainty in position}} \underbrace{\langle (\Delta P)^2 \rangle}_{\text{uncertainty in momentum}} \geq \frac{1}{4} \left\| [X, P] \right\| = \frac{1}{4}$$

Ergo, to know precisely which of the two slits the electron passed through forces the momentum to be uncertain.

- IDEA: Heisenberg uncertainty can be used to detect eavesdropping by Eve when a key R is sent.

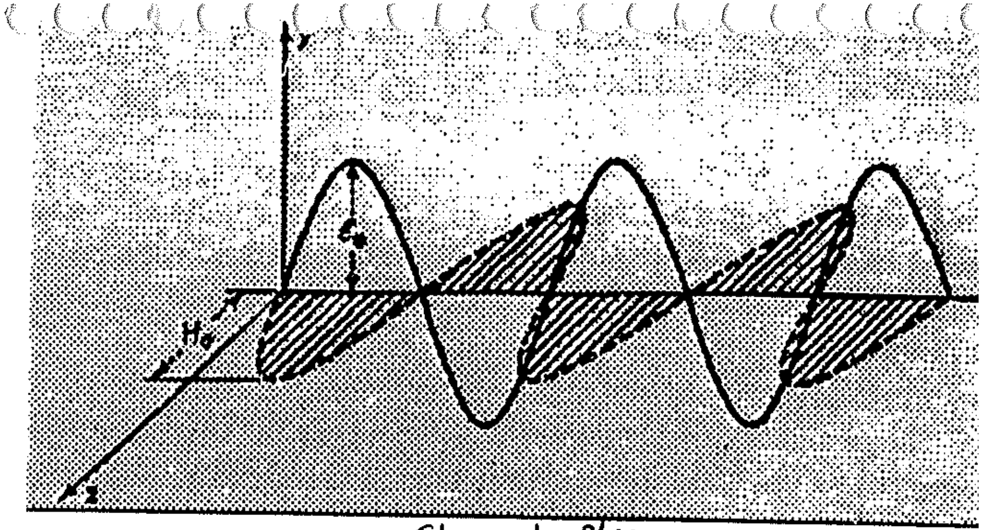
- But HOW do we exploit Heisenberg uncertainty to detect Eve's eavesdropping?

15b

TYPES OF COMMUNICATION SECURITY (Cont.)

• QUANTUM SECRECY (Bennett-Brassard, 1984)

Built-in detection of eavesdropping



Classical Physics

(Without Noise)

BB84 QUANTUM CRYPTOGRAPHIC PROTOCOL

- The vertical and horizontal polarization states, $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$ resp, form a basis of $\mathcal{H}$ which we will call the vertical/horizontal (V/H) basis $\boxplus$.

- The slanted polarization states $|\nearrow\rangle$ and $|\nwarrow\rangle$ form another basis of $\mathcal{H}$ which we will call the oblique basis $\boxtimes$.

- For the V/H basis $\boxplus$, Alice & Bob agree to communicate via the following quantum alphabet:

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

- For the oblique basis $\boxtimes$, Alice & Bob agree to communicate via the following quantum alphabet:

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

- Because of Heisenberg's uncertainty principle, Alice & Bob know that observations with respect to the $\boxplus$ bais are incompatible with observation with respect to the $\boxtimes$ basis.

- So Alice communicates to Bob by randomly choosing between the two quantum alphabets $\boxplus$ and $\boxtimes$.

- Over the quantum channel, Alice sends her message to Bob, randomly choosing between the quantum alphabets for each bit sent

- Over a public channel, Bob communicates to Alice which quantum alphabets he used for each measurement

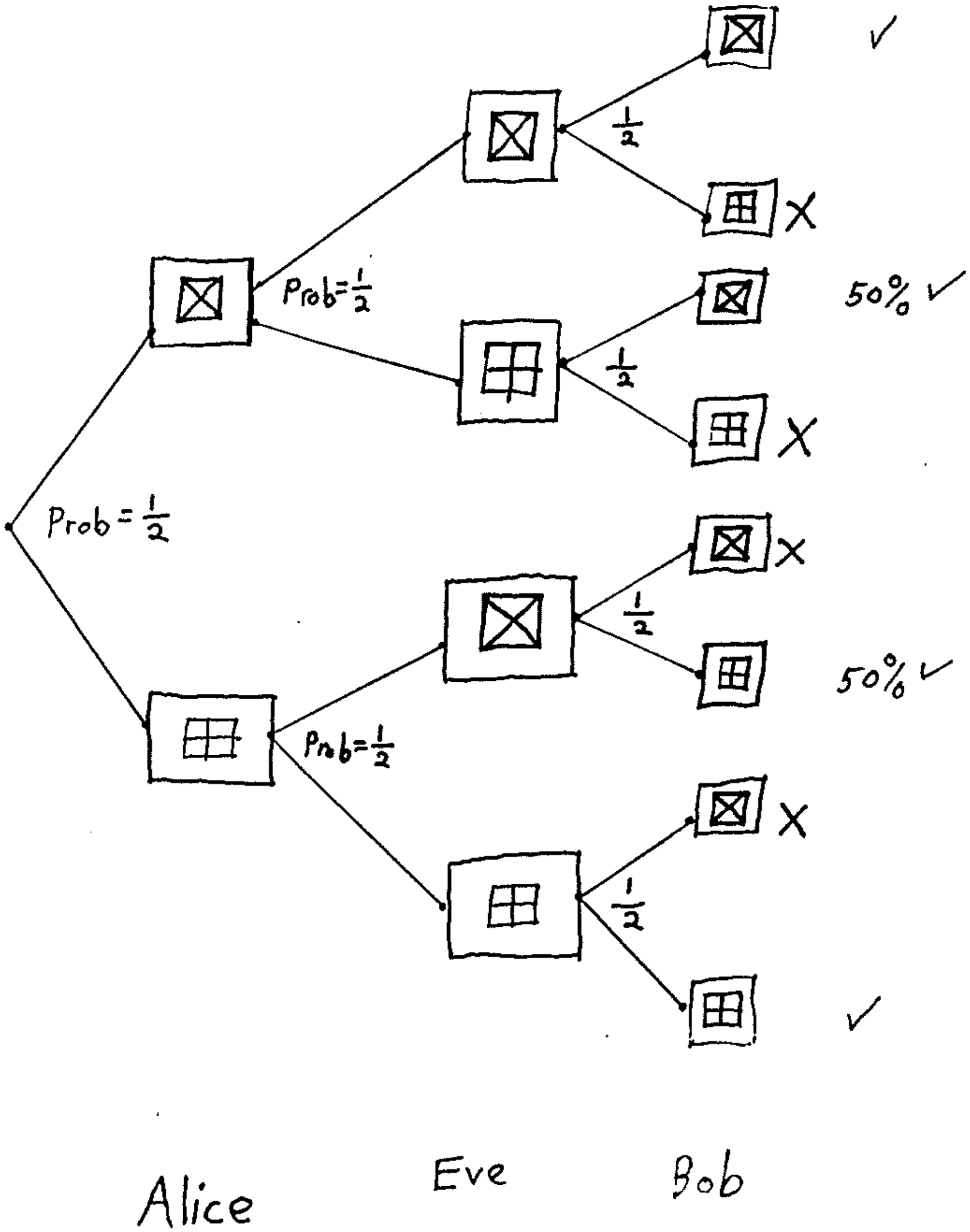
- Over the public channel, Alice reponds by telling Bob which of his measurements were made with the correct alphabet.

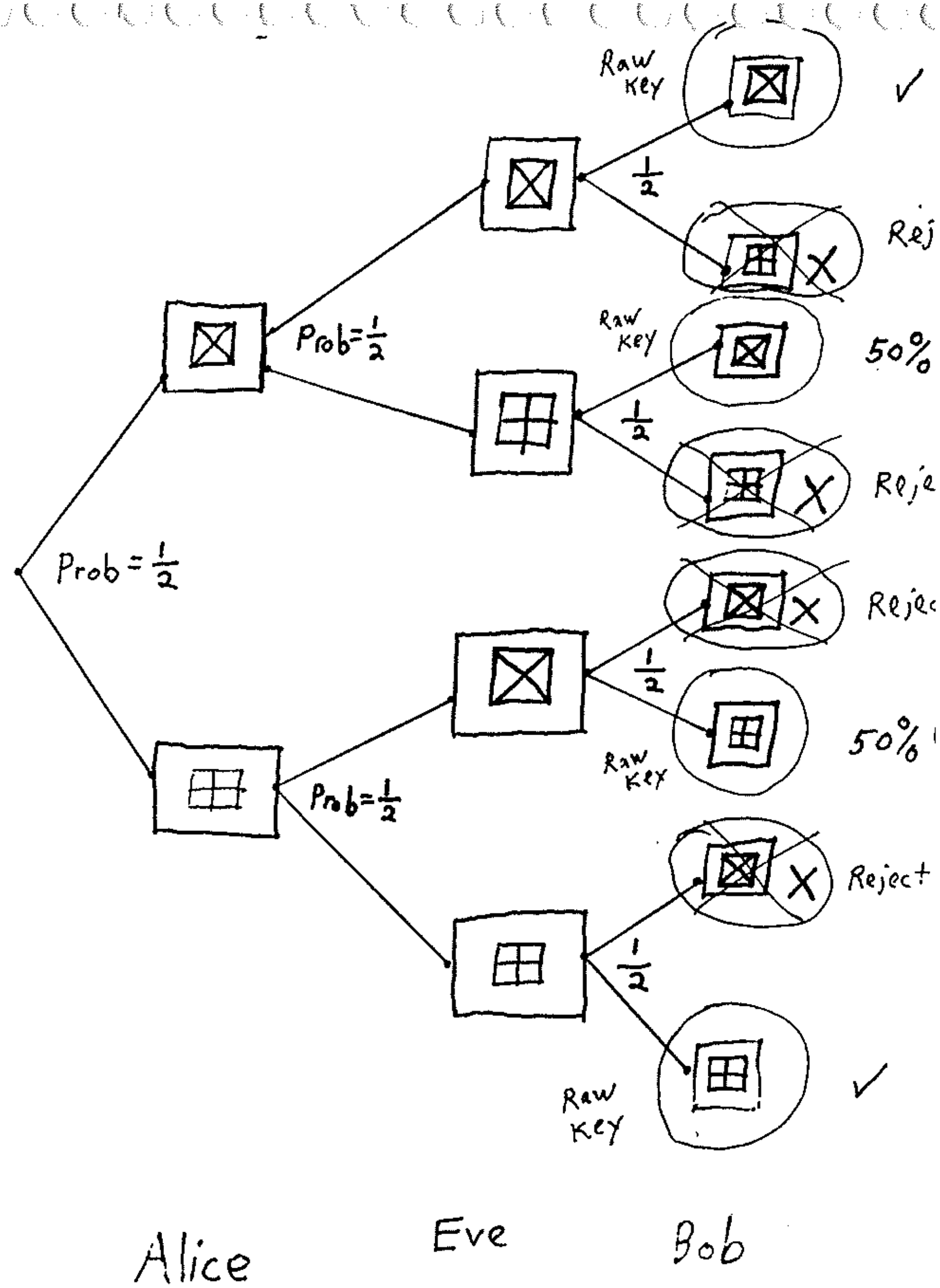
- Alice & Bob then then delete all bits for which they used incompatible quantum alphabets to produce there resulting RAW KEYs.

- If Eve has not eavesdropped, then their two RAW keys will be the same.

- Over the public channel, Alice & Bob compare common small portions of their RAW KEYs, and then delete the disclosed bits from their RAW KEY to produce their FINAL KEY.

- If Alice & Bob find through there public disclosure revealed no errors, then they know that Eve was not present, and now share a common FINAL KEY.


Prob = 1/2
Prob = 1/2
Prob = 1/2
1/2
1/2
1/2
1/2
50%
50%
Alice
Eve
Bob


Raw Key
Raw Key
Raw Key
Raw Key
Prob = 1/2
Prob = 1/2
Prob = 1/2
1/2
1/2
1/2
1/2
50%
50%
Reject
Alice
Eve
Bob

PRIVACY AMPLIFICATION: Distilling a smaller secret key from a larger partially secret key

PREAMBLE TO PRIV. AMP.

- Alice and Bob begin by permuting raw key with a publically disclosed random permutation
- Alice and Bob publically compare some blocks of raw key to estimate error rate Q.
- Alice and Bob discard any portion of the raw key that was publically disclosed
- $Q \geq Threshold \Rightarrow$ Priv. Amp. not possible. Restart everything!

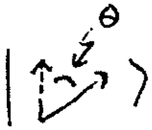
If $Q < Threshold$, then priv. amp. begins

- Based on Q, Alice and Bob estimate that $\leq k$ bits out of n knwown by Eve
- Let s = a security parameter to be adjusted as required.
- Alice & Bob compute the parities of $n - k - s$ publically chosen random subsets
- Both Alice and Bob keep these parities secret. These parities form the final secret key.

B92 Protocol

- Use 2-dim. $\mathcal{H}$ for polarized photons

- Quantum Alphabet

$$1 = |\oplus\rangle =$$ 

$$0 = |\ominus\rangle =$$ 

$$0 < \theta < \frac{\pi}{2}$$

$$\therefore \langle \oplus | \ominus \rangle = \sin 2\theta$$

Measurement Operators

$$\left\{ \begin{aligned} A_{\oplus} &= \frac{1 - |\ominus\rangle\langle\ominus|}{1 + \langle\oplus|\ominus\rangle} \\ A_{\ominus} &= \frac{1 - |\oplus\rangle\langle\oplus|}{1 + \langle\oplus|\ominus\rangle} \\ A_{?} &= 1 - A_{\oplus} - A_{\ominus} \end{aligned} \right\}$$

non-commuti
observable

26
30
316

OPAQUE EAVESDROPPING

Eve intercepts Alice's message, and the masquerades as Alice by sending her received message to Bob.

TRANSLUCENT EAVESDROPPING WITHOUT ENTANGLEMENT

Eve makes the information carrier unteract unitarily with her probe, and then letting it proceed on to Bob in a slightly modified state.

$$|\oplus\rangle\,|\psi\rangle \Longrightarrow |\oplus'\rangle\,|\psi_+\rangle$$
or
$$|\ominus\rangle\,|\psi\rangle \Longrightarrow |\ominus'\rangle\,|\psi_-\rangle$$

where $|\psi\rangle$ denotes the state of the probe.

Next ?

- Earth/satelite Communication
  - Proposed by Franson
    Hughes
- Single photon sources
  - Stanford Univ.

Difficulties

- Multi-User Quantum Crypto Protocols
  - Substantial Progress has been made
- Proof that Quantum Crypto Protocols are imperious to all possible eavesdropping strategies.