Title: Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source

Date: Jun 03, 2007 03:00 PM

URL: http://pirsa.org/07060050

Abstract:

The Truth About Bob

Chris Erven

June 3, 2007

Overview

- Motivation
- Quantum Key Distribution Protocol and Security
- Details of the System
  - Entangled Photon Source
  - Free-Space Link and Detector Optics
  - Electronics
  - Software
- Experimental Results
  - QKD
  - Bell Measurement
- Future Work

Overview

- Motivation
- Quantum Key Distribution Protocol and Security
- Details of the System
  - Entangled Photon Source
  - Free-Space Link and Detector Optics
  - Electronics
  - Software
- Experimental Results
  - QKD
  - Bell Measurement
- Future Work

Meet Bob

Martin "Bob" Laforest

Bob with the ladies

$\text{Fidelity}_{\text{ladies}} \ll 1$

Bob with the ladies

$\text{Fidelity}_{\text{ladies}} \ll 1$

Bob with the ladies

$\text{Fidelity}_{\text{ladies}} \ll 1$

Bob with the ladies

$\text{Fidelity}_{\text{ladies}} \ll 1$

Bob with the ladies

$\text{Fidelity}_{\text{ladies}} \ll 1$

Bob with the ladies

$\text{Fidelity}_{\text{ladies}} \ll 1$

Bob and Eve

"Eve" Boileau

Bob and Eve... and Alice

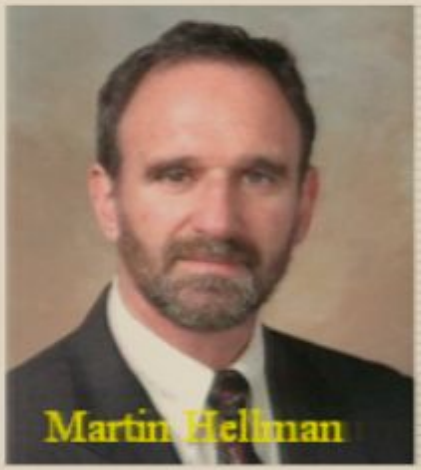
"Eve" Boileau

"Alice" Bouquillon

Motivation

Tvetujuvujpo Dzqifs

Whitfield Diffie



Martin Hellman

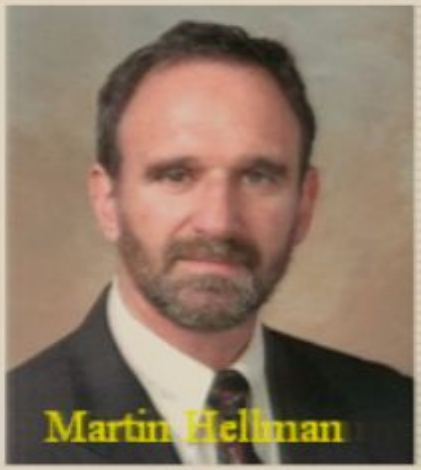
Ron Rivest, Adi Shamir, Len Adleman

The Vernam One-Time Pad

Motivation

Substitution Cypher

Whitfield Diffie



Martin Hellman

The Vernam One-Time Pad

Ron Rivest, Adi Shamir, Len Adleman

Goal

University of Waterloo

Goal

To distribute a **secret**, **shared**, **random bit string** between Alice and Bob which they can use to encrypt/decrypt messages

Quantum Key Distribution – the BBM92 Protocol (developed by Bennett, Brassard, and Mermin in 1992)

+

The Vernam One-Time Pad

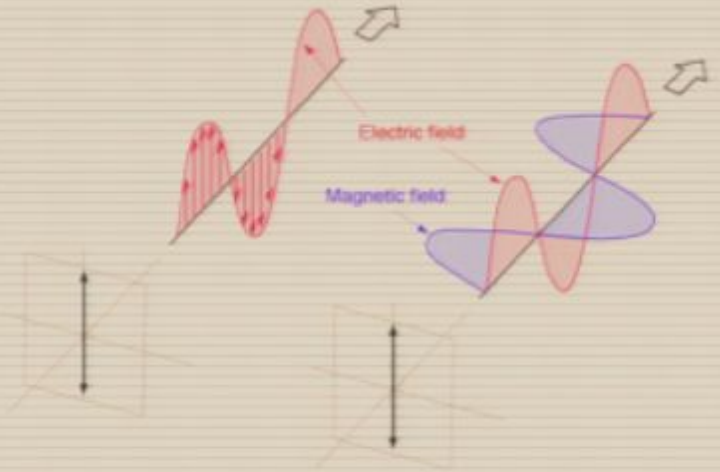
Unconditional Security!

IQC

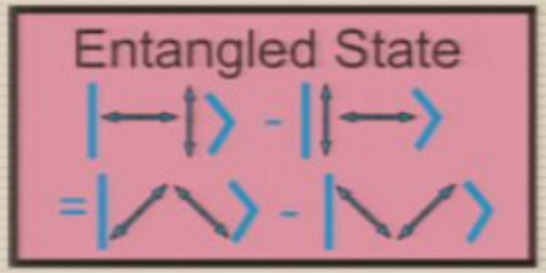
General Setup and Protocol

Quantum Cryptography

- Quantum Cryptography exploits the principles of quantum mechanics to enable provably secure distribution of private information
- We can use two things from quantum information theory to help us
  - Entangled Bell state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle - |V\rangle|H\rangle)$
  - No cloning theorem
- How is this quantum?
  - Using distinctly quantum correlations (entanglement) which are stronger then a classically correlated state in order to get security
- Is this really secure?
  - Always detect an eavesdropper
  - A number of security proofs have been developed
- We'll be using the polarization of photons as our qubits since it is easy to deal with



Description of the Protocol (BBM92)



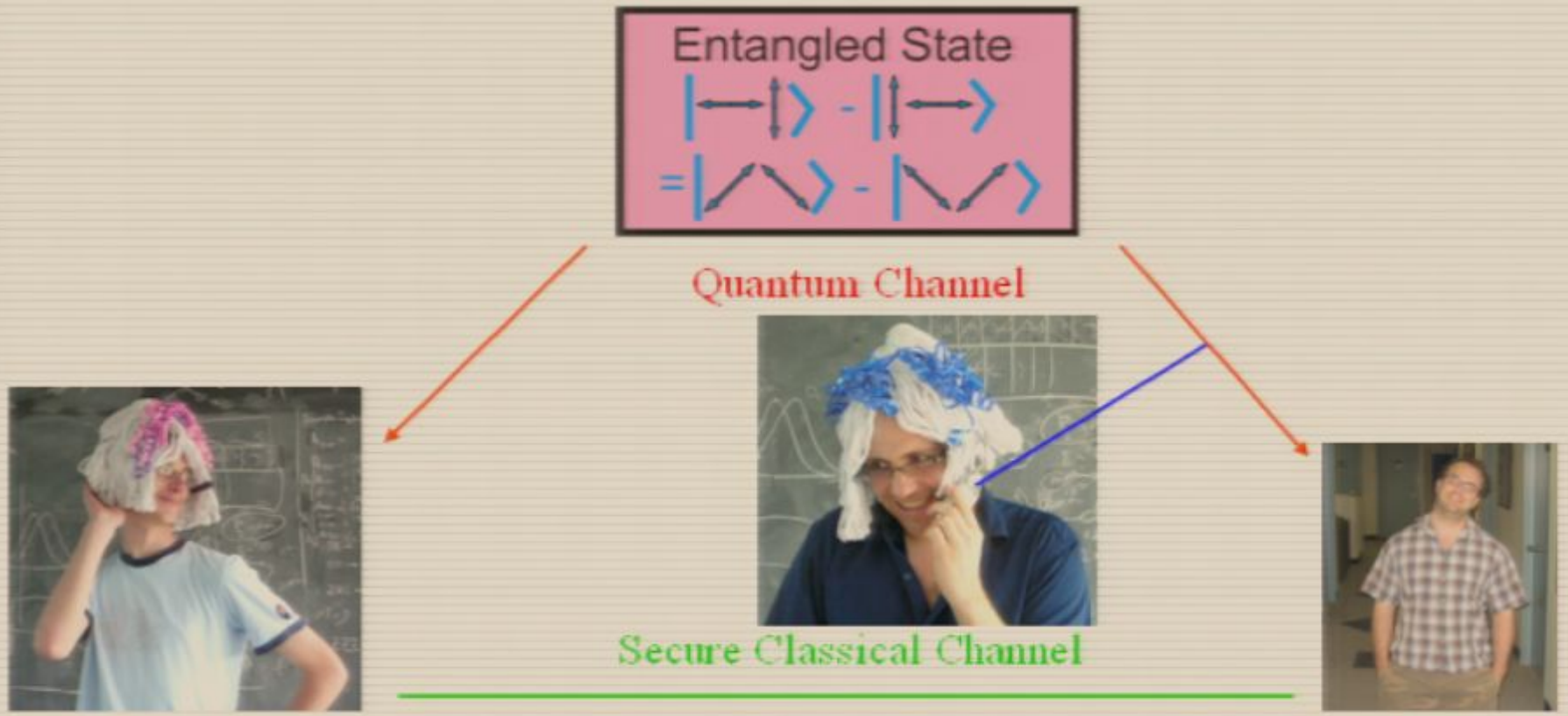
Quantum Channel

Secure Classical Channel

- Distribute pairs of photons to Alice and Bob in the entangled state

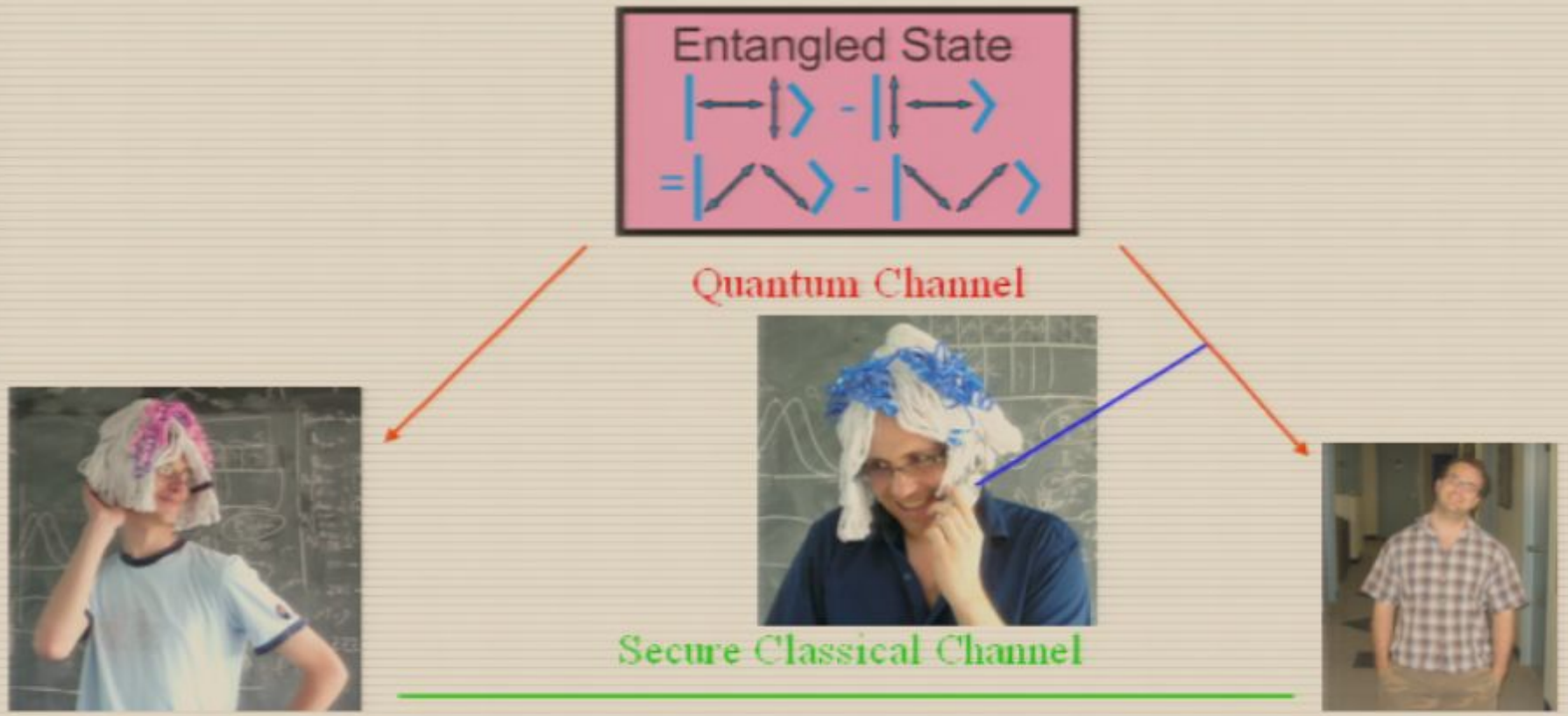
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H_1V_2\rangle - |V_1H_2\rangle) = \frac{1}{\sqrt{2}}(|+_1-_2\rangle - |-_1+_2\rangle)$$

Description of the Protocol (BBM92)



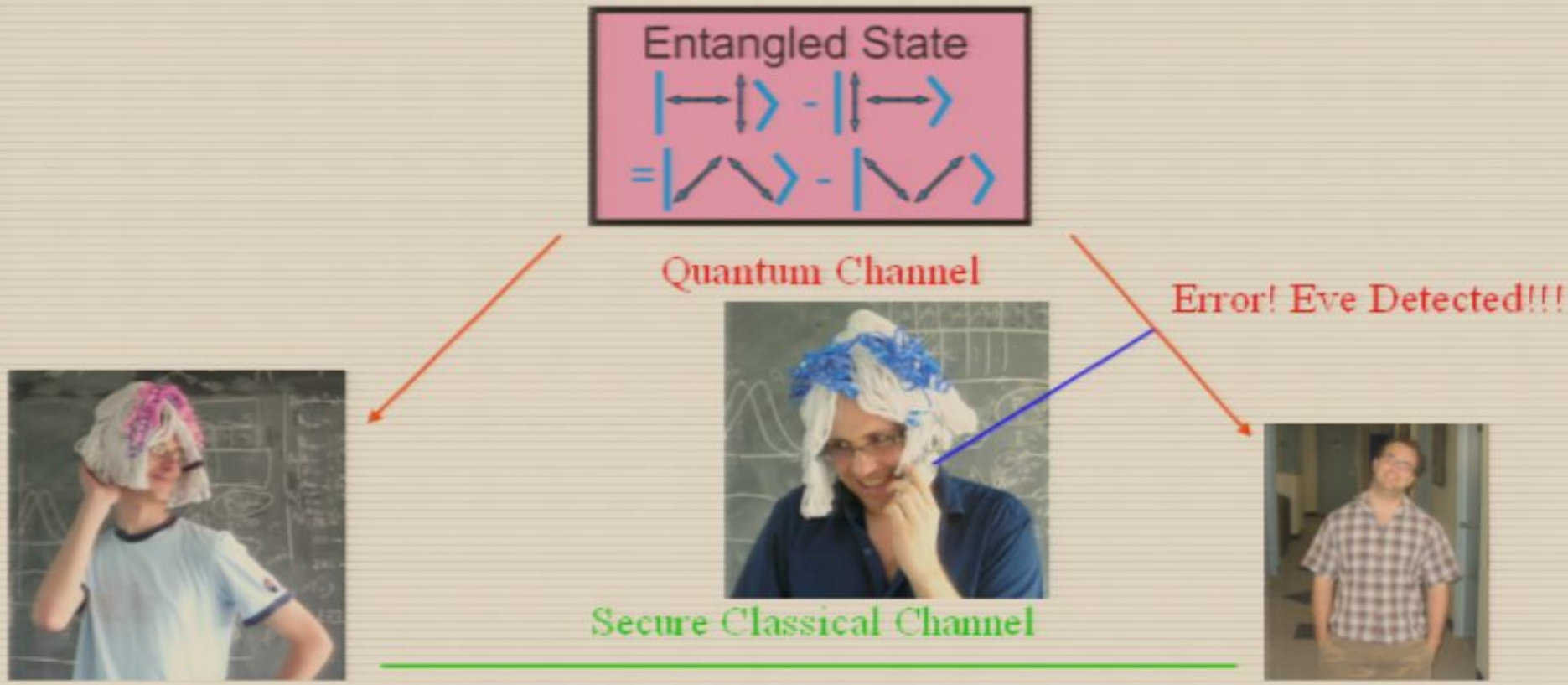
- Alice and Bob perform polarization measurements on their incoming photons randomly in 1 of 2 complementary bases (H/V or +/-)

Description of the Protocol (BBM92)



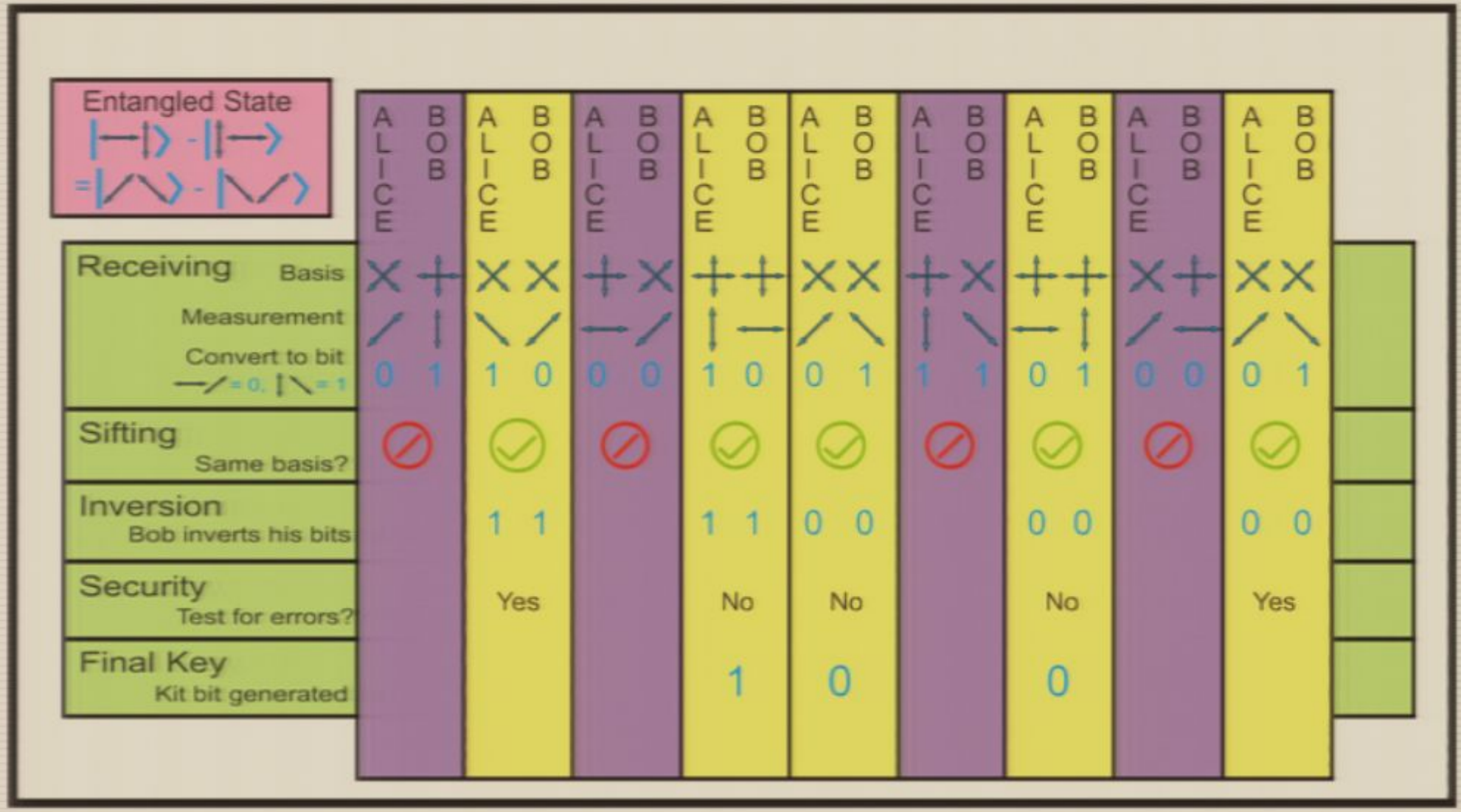
- Alice and Bob observe anti-correlated measurements when measuring in the same basis
- Assign (classical) bit value {H,+} → 0 and {V,–} → 1
- Bob inverts his key (anti-correlated source state)

Description of the Protocol (BBM92)



- Any eavesdropper inevitably induces errors into the key
- Alice and Bob estimate a quantum bit error rate (QBER) to detect any eavesdroppers

Example of the QKD Protocol Running

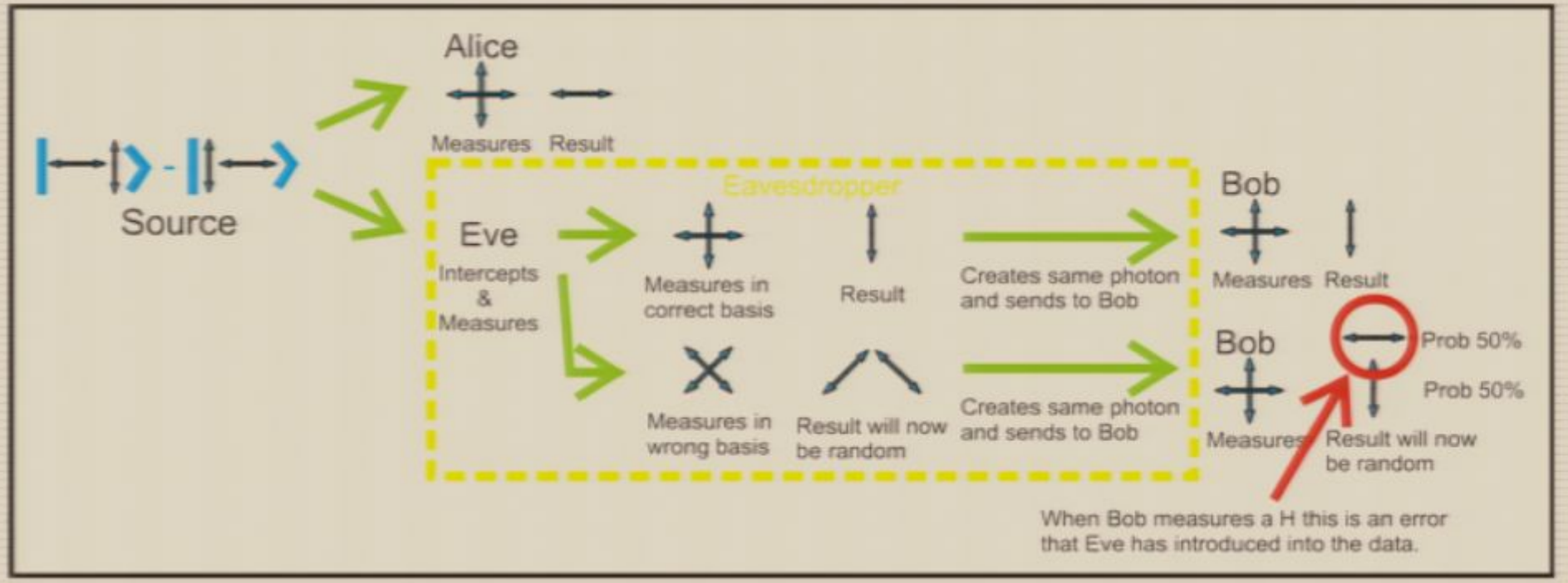


Security Against Intercept-Resend Attack

Entangled State

$$|\leftrightarrow\rangle|\updownarrow\rangle - |\updownarrow\rangle|\leftrightarrow\rangle$$
$$= |\nearrow\rangle|\nwarrow\rangle - |\nwarrow\rangle|\nearrow\rangle$$

Use the special property of this entangled state that no matter what basis you measure it in, you will always get orthogonal measurement results for the two photons, but any eavesdropping attempt will wreck this state



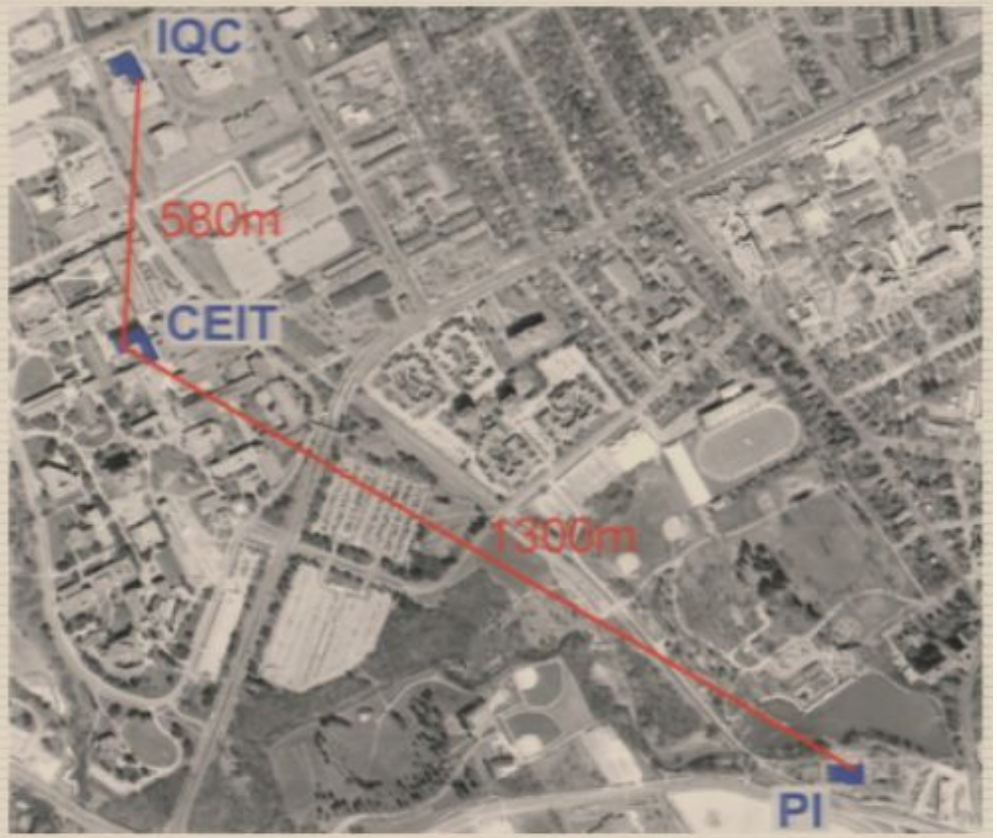
"Measurement disturbs a quantum system."

Further Security

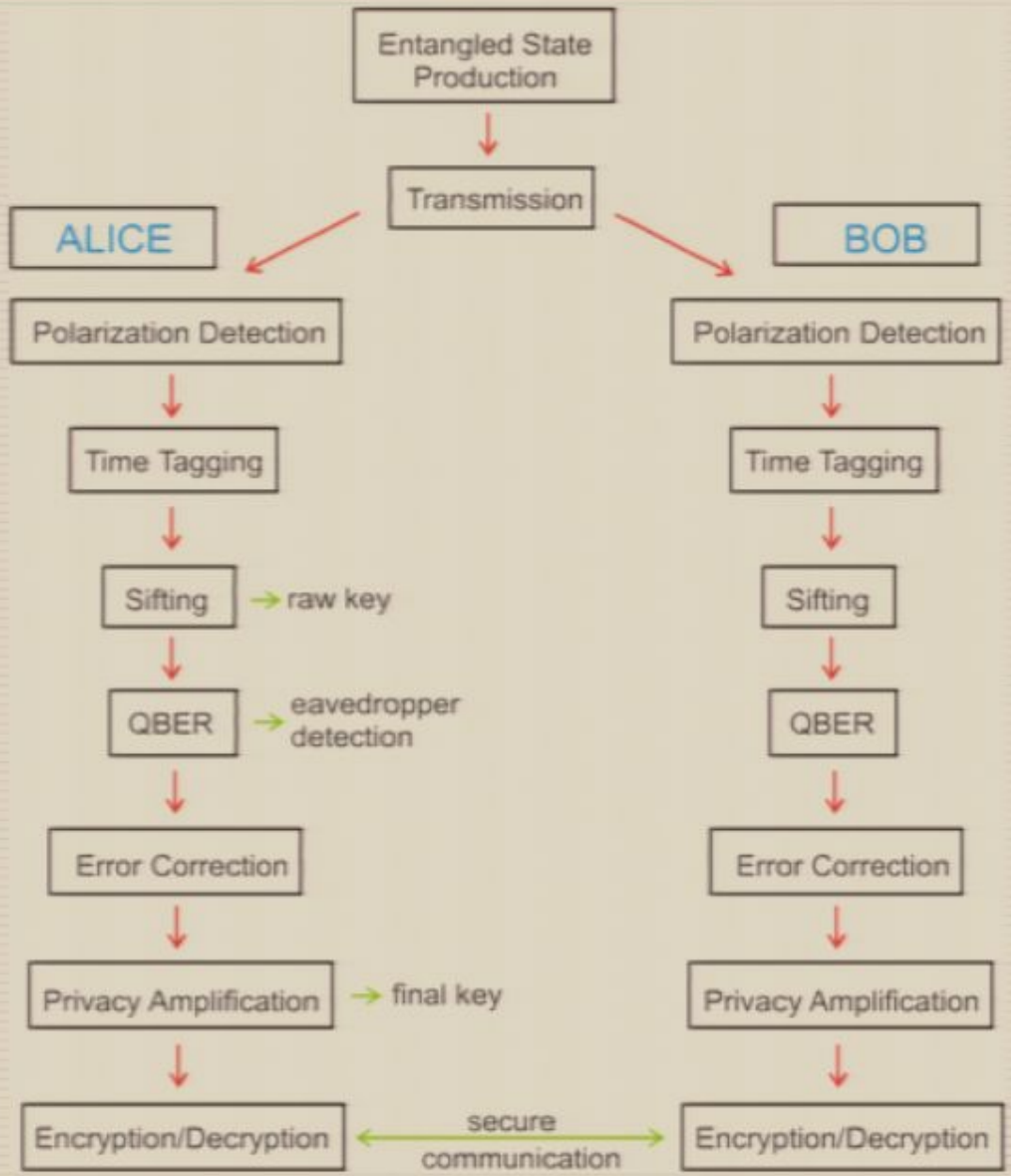
- Symmetric individual attacks secure for an error rate < 14.6%
  - Security is based on finding an expression for Eve's maximal Shannon information for her optimum measurement strategy
  - Alice and Bob will then only be able to create a secret key if their mutual Shannon information is greater then the Eve-Alice or Eve-Bob information
- Coherent attacks secure for an error rate < 11%
  - Dominic Mayers came up with a security proof in 1996
- Quantum Cloning (Buzek and Hillery)
  - Optimal quantum cloning procedure produces states with a maximum fidelity $F = 0.82$ with the original state
- Ekert's original intuition
  - An eavesdropper cannot create a 3 particle state where two particles will reproduce the results of the $|\psi^-\rangle$ state in a Bell experiment and the third particle will give the eavesdropper information about Alice's and Bob's measurements

Why use a Free Space link?

- Most QKD schemes that have been implemented have used fibres to distribute photons
  - Limitations:
    1) distance <100 km
    2) fibre - measurement wavelengths
    3) birefringence
- We want to use the polarization degrees of freedom as our qubits since they're easy to work with in the lab
- The atmosphere is not birefringent - doesn't introduce any random polarization rotations (random unitaries)
- Towards global communication

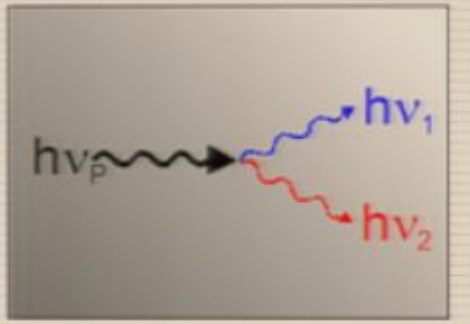


Overview of System



Entangled State Production

- Use a non-linear optical process called Parametric Down-Conversion to create a pair of polarization correlated photons



- The non-linear optical crystal has a Hamiltonian with a non-linear portion which looks like

$$H^{NL} \approx \sum_{p,p'} \int d^3k \int d^3k' \Delta(\bar{k}_0 - \bar{k} - \bar{k}') F_0 e^{-i\omega_0 t} a_0(\bar{k}_0, p_0) a_1^\dagger(\bar{k}, p) a_2^\dagger(\bar{k}', p') + H.C.$$

- The evolution of the state of the photons generated by the down-conversion process in the Dirac picture looks like

$$|\psi_D(t)\rangle \approx |\psi_D(t_0)\rangle + \frac{1}{i\hbar} \int_t^t dt' H_D^{NL}(t') |\psi_D(t_0)\rangle$$

- Taking a product state of the laser and the vacuum as the initial state yields

$$|\psi\rangle \approx \sum_{p,p'} \int d^3k \int d^3k' F_0 \Delta(\bar{k}_0 - \bar{k} - \bar{k}') \Delta(\bar{\omega}_0 - \bar{\omega} - \bar{\omega}') a_0(\bar{k}_0, p_0) a_1^\dagger(\bar{k}, p) a_2^\dagger(\bar{k}', p') |laser\rangle_0 |vac\rangle_{1,2}$$

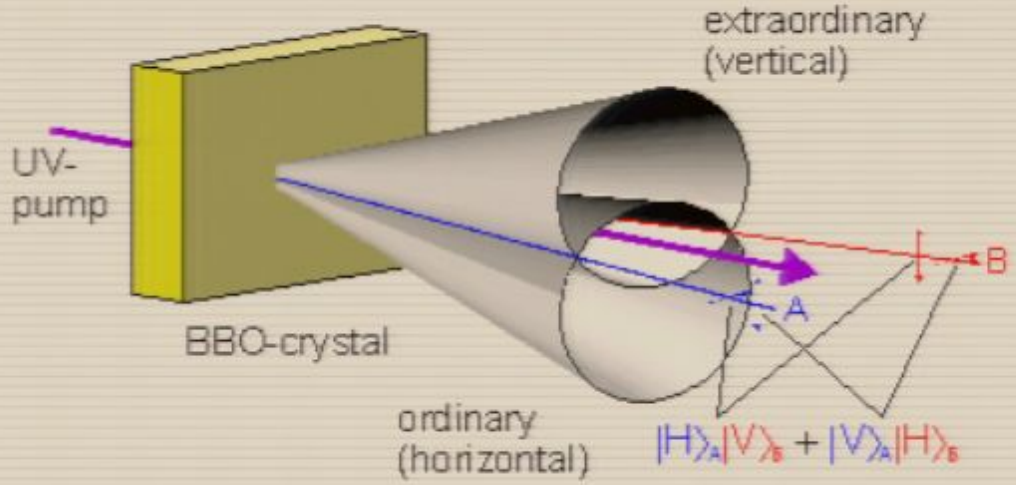
- You can see from this equation the two phase matching conditions

$\bar{k}_0 \approx \bar{k} + \bar{k}'$ Conservation of Momentum

$\omega_0 \approx \omega + \omega'$ Conservation of Energy

Entangled State Production

- The correlated photons emerge from the crystal on two cones diametrically opposite to each other

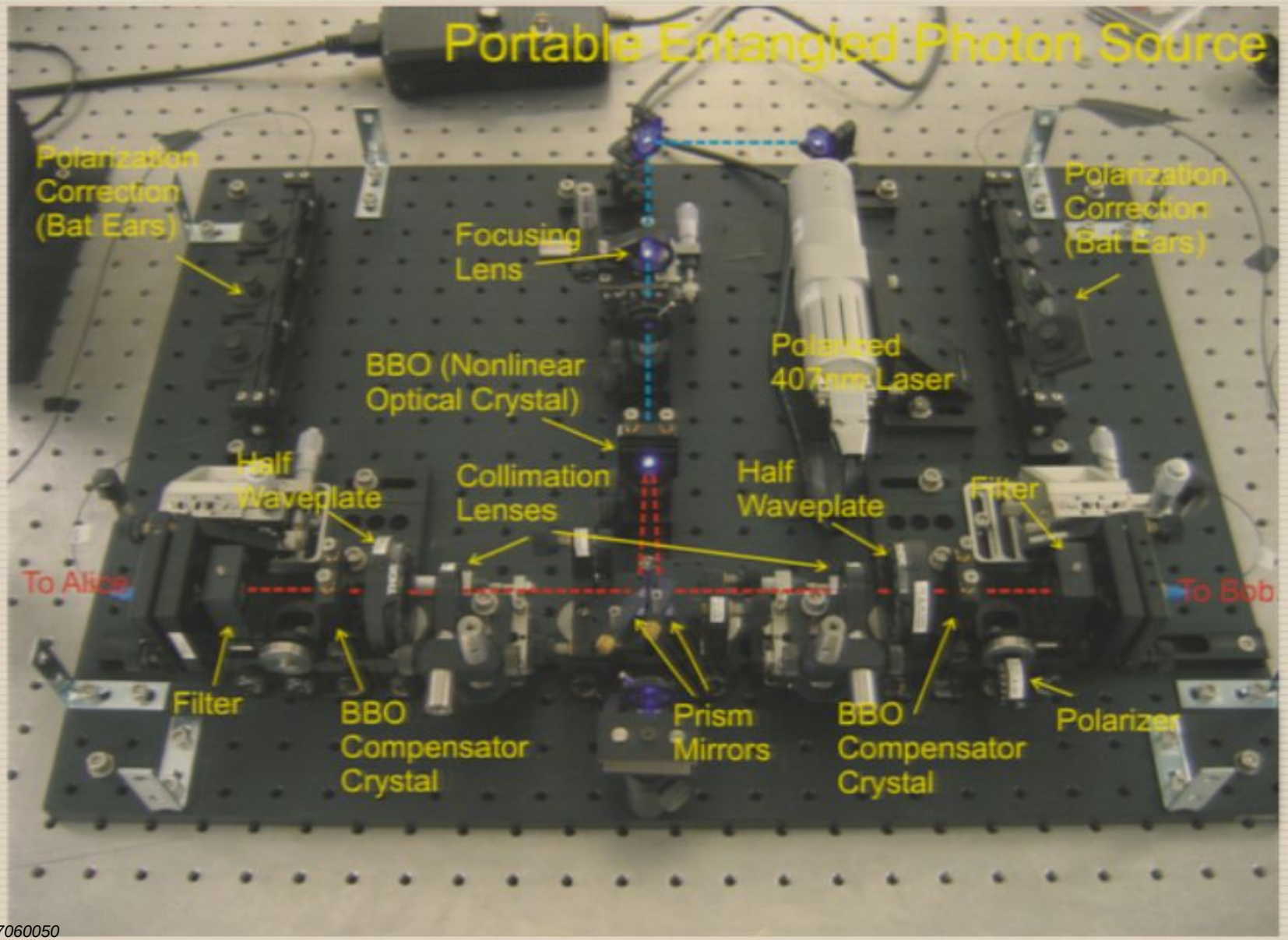


Conservation of Momentum

$$\bar{k}_0 \approx \bar{k} + \bar{k}'$$

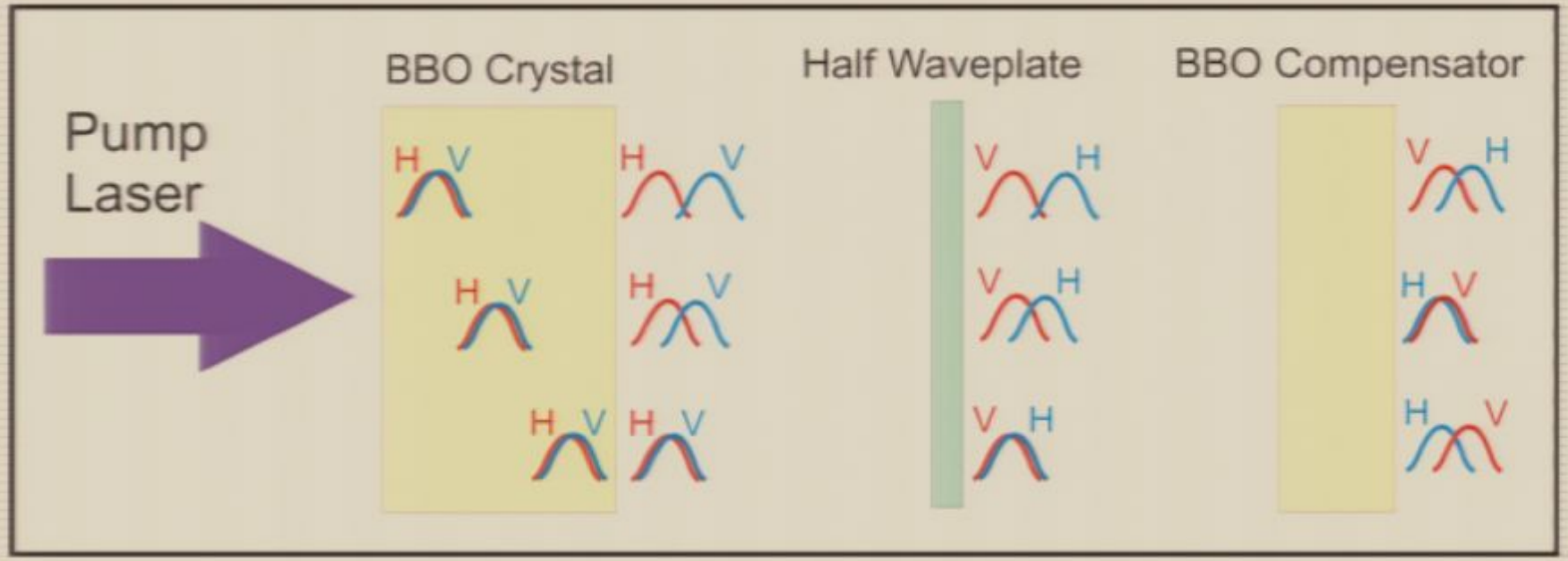
- Exactly one horizontally and one vertically polarized photon is produced in each pair
- Spectrally and spatially filter photons along intersection lines of cones to obtain polarization entangled photons

Portable Entangled Photon Source



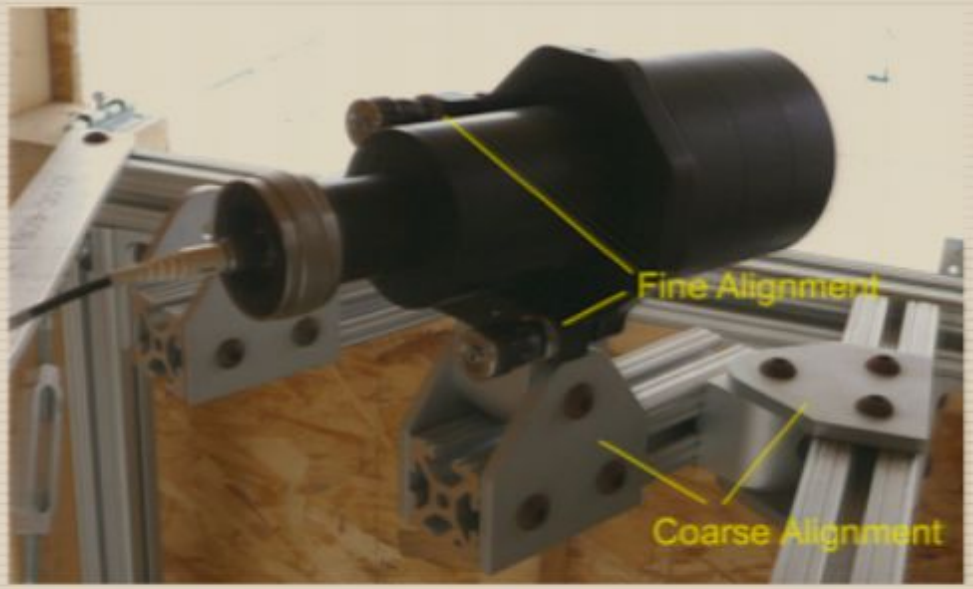
Walk-off Compensation

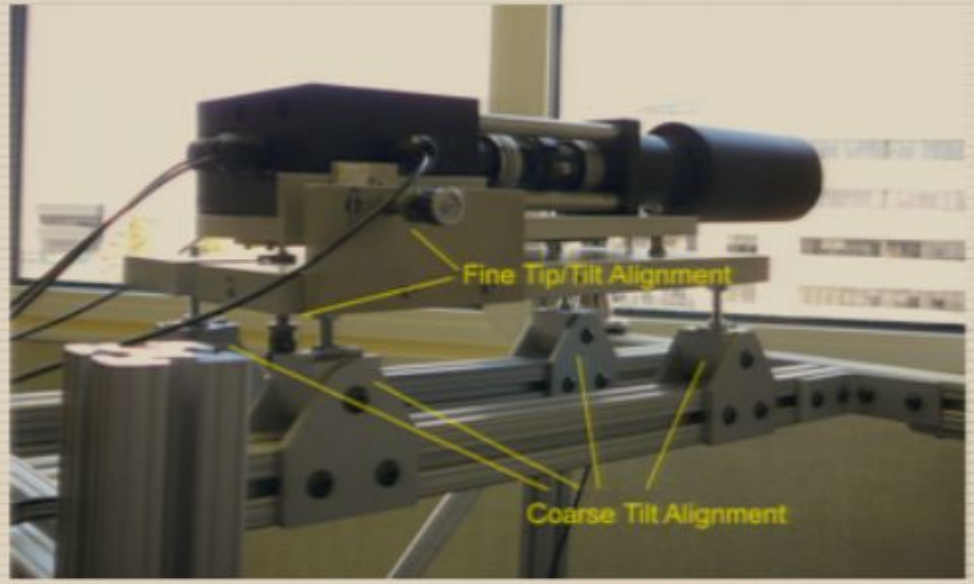
- Within the crystal, the ordinary (V) and extraordinary (H) photons have different velocities and propagate along different directions because of the birefringent nature of the down-conversion crystal
- The resulting longitudinal and transverse walk-offs have to be compensated for in order to produce high quality entanglement



Free Space Transmission - Telescopes

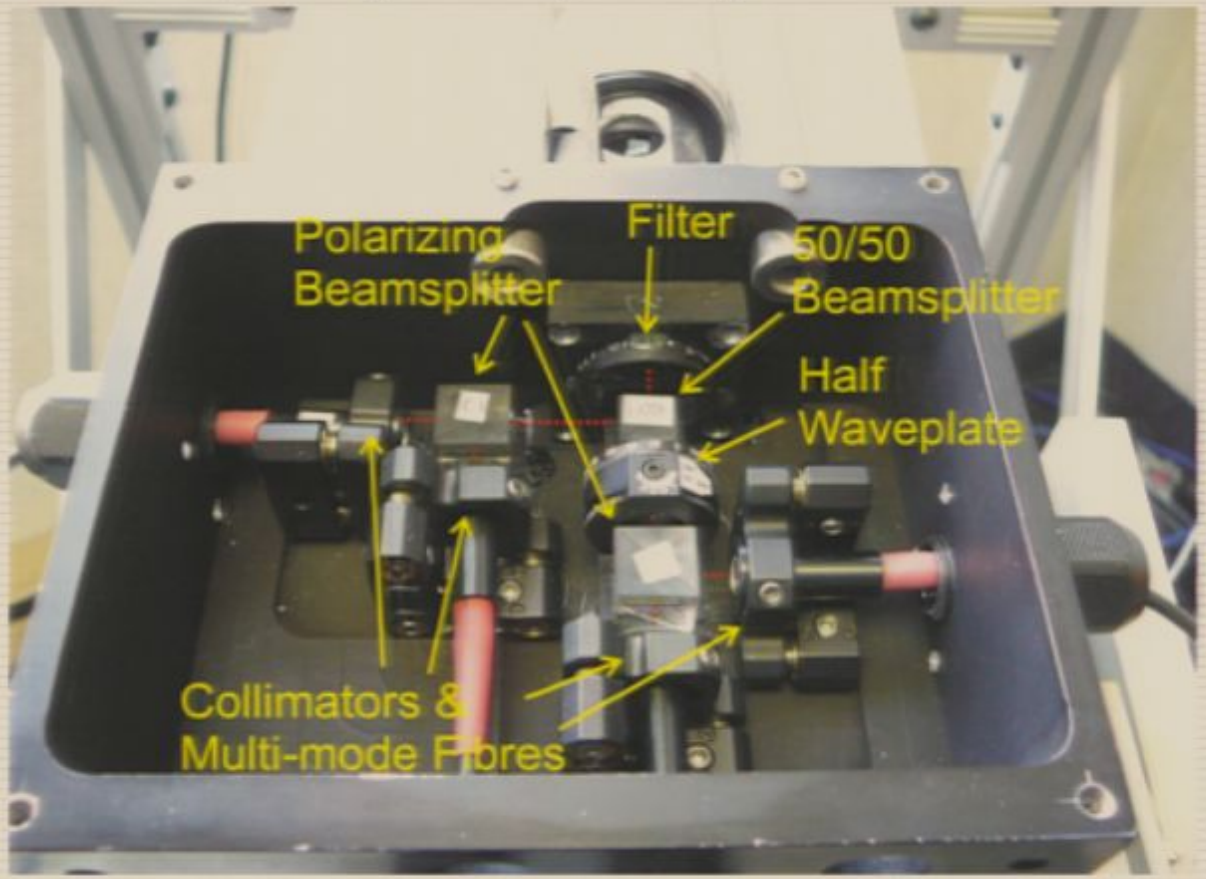
- Sender and Receiver telescopes to transmit the entangled photons
- The telescopes expand and collimate the beam to 3 inches (for alignment, beam spreading, and beam wander)





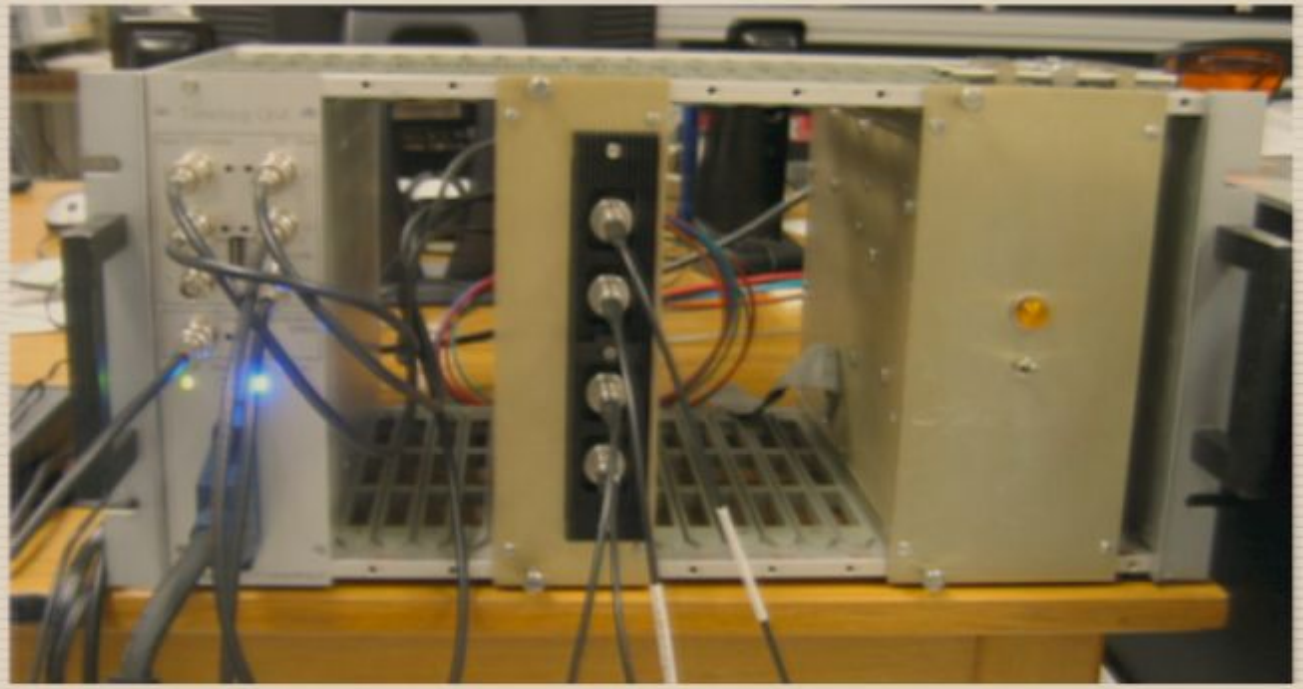
Detection – Polarization Measurement

- Have to make polarization measurements in 1 of 2 bases -- a non-polarizing beamsplitter makes our random basis choice
- Measurement in the H/V basis is accomplished with a polarizing beamsplitter
- Measurement in the +/- basis is accomplished with a half waveplate (set to rotate the photons by 45°) and a polarizing beamsplitter



Detection - Electronics

- Use silicon avalanche photodiodes to detect the polarization measured photons (photon detection efficiency of these devices can be upwards of 70%)
- The TTL pulses are time tagged with a highly accurate (~156.25ps) time
- Need very high timing accuracy between 2 spatially distributed systems (use a GPS receiver)



Software

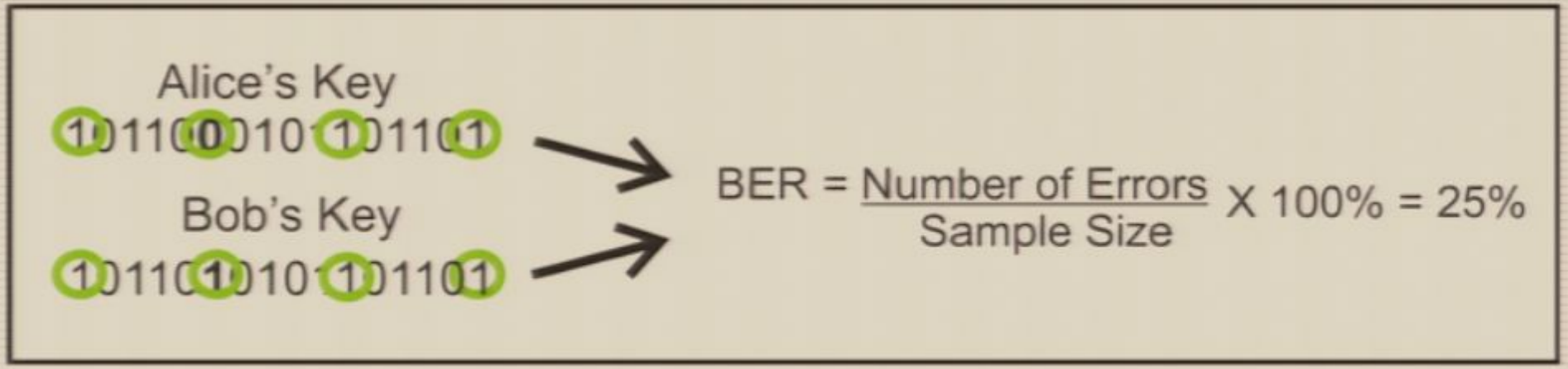
- Custom multi-threaded software was written to perform the BBM92 protocol
- The two computer clocks are first synchronized to within ~100ms
- A communication connection over a public internet channel is established
- Alice and Bob begin to measure incoming photons, a separate measurement thread syncs the start of the measurement process and then continuously measures incoming photons
- The measurements are passed to a coincidence thread, which sends Alice's time-tag information to Bob and then finds the coincident events in the two lists

$$C_{accidental} = C_{Alice} \times C_{Bob} \times \Delta t_{cw}$$

- The coincidence thread then sifts Alice's and Bob's measurement results down to only those coincident events, this is known as the raw key

Software: Calculating the QBER

- The raw key is then passed on to a key generation thread responsible for performing the BBM92 protocol
- The key generation thread first randomly chooses 10% of Alice's and Bob's secret raw key and compares them over a public internet channel in order to estimate a bit error rate (QBER)
- A QBER of 14.6% or less is allowable in order to generate a provably secure secret key



Software – Error Correction

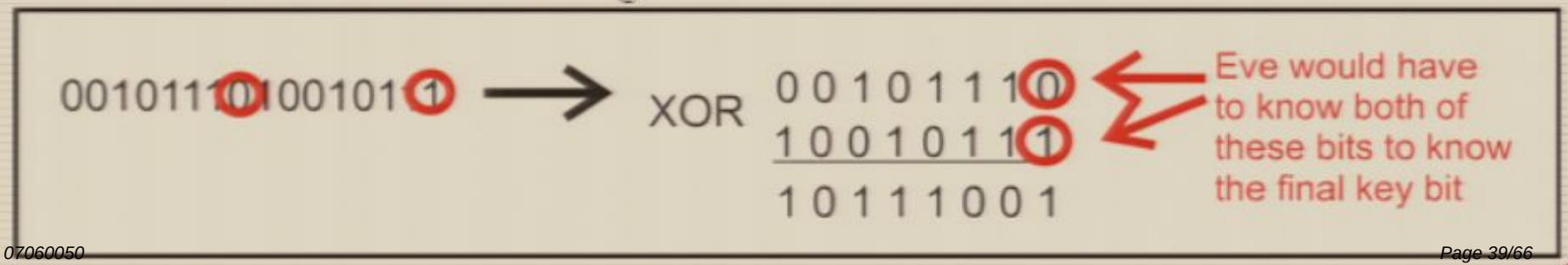
- The key generation thread then performs the Cascade error correction algorithm
- It uses the BINARY primitive to find an error between Alice's and Bob's bit strings (represented by A and B) when there's an odd number of errors
- The BINARY primitive works in the following manner
  - Alice sends Bob the parity of the first half of her bit string A
  - Bob determines whether an odd number of errors occurred in the first half or second half of their strings by testing the parity of the first half of his bit string B and comparing it to the parity sent by Alice
  - This process is repeatedly applied to the half determined in step 2 until an error is eventually found
- The Cascade algorithm uses the BINARY primitive to correct all of the errors between Alice's and Bob's key with a high probability
- It performs a number of passes through the key in order to correct the errors

Software – Error Correction

- The Cascade algorithm works in the following manner
  - Alice and Bob break their raw key up into blocks of k_1 bits
  - Alice computes the parities of her blocks and sends them to Bob
  - Bob uses the BINARY primitive to correct an error in each block where his parity differs from Alice's
  - At this point, all of Alice's and Bob's blocks have an even number of errors (possibly zero)
  - Alice and Bob repeat the steps above by choosing a new random block size k_i and a random function f_i which is used to randomly break their key up into new blocks
  - If any errors are found, this means there must have been two errors (an even number of errors) at an earlier step, since one has now been corrected, the algorithm goes back to the first pass and corrects the other error
  - The number of passes was chosen to be four based on interpolating the Cascade benchmark data in Brassard and Salvail's paper

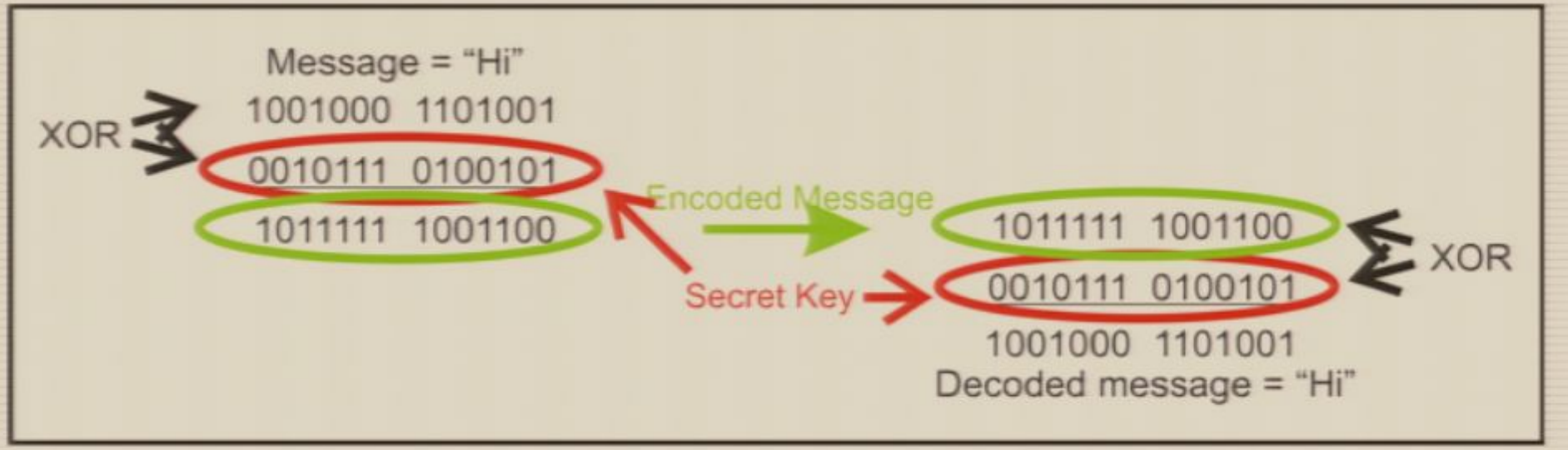
Software – Privacy Amplification

- The information that was leaked during error correction along with any information the eavesdropper might have gained from interacting with some photon pairs now has to be eliminated using a privacy amplification protocol at the cost of reducing the secret key size
- The software uses a universal hash function developed by Carter and Wegman
- This shortens the key by approximately the number of bits that were revealed during error correction, plus the appropriate number of bits based on the observed error rate
- Simple example
  - Alice and Bob split their key in half and XOR the two halves together
  - In order for Eve to have a final bit in the key, she must have known BOTH bits that were XOR'd together

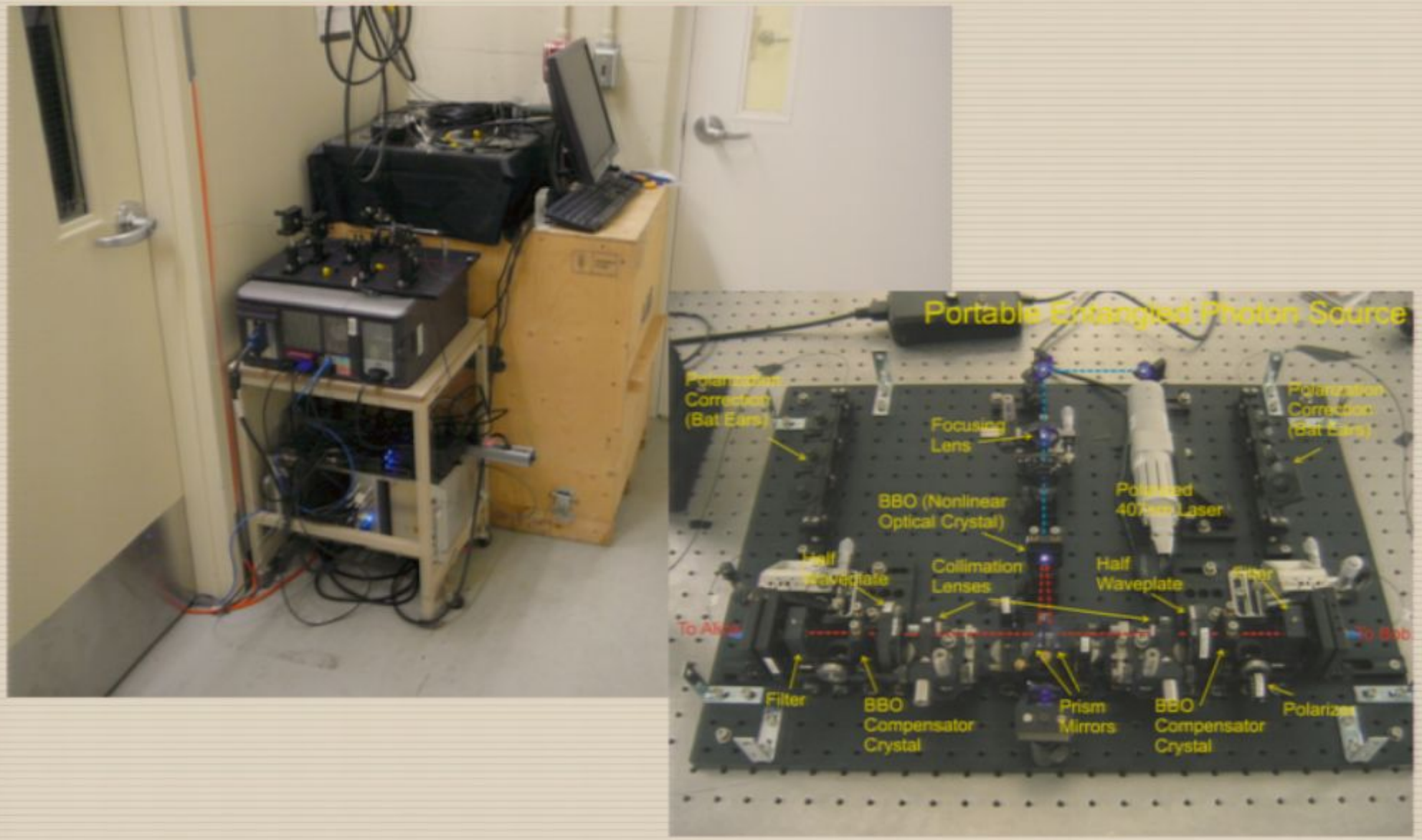


Software – Encrypting/Decrypting

- The software then uses the generated key to encrypt and decrypt data sent between Alice and Bob using the Vernam One-Time Pad
- The encryption operation is the XOR operation

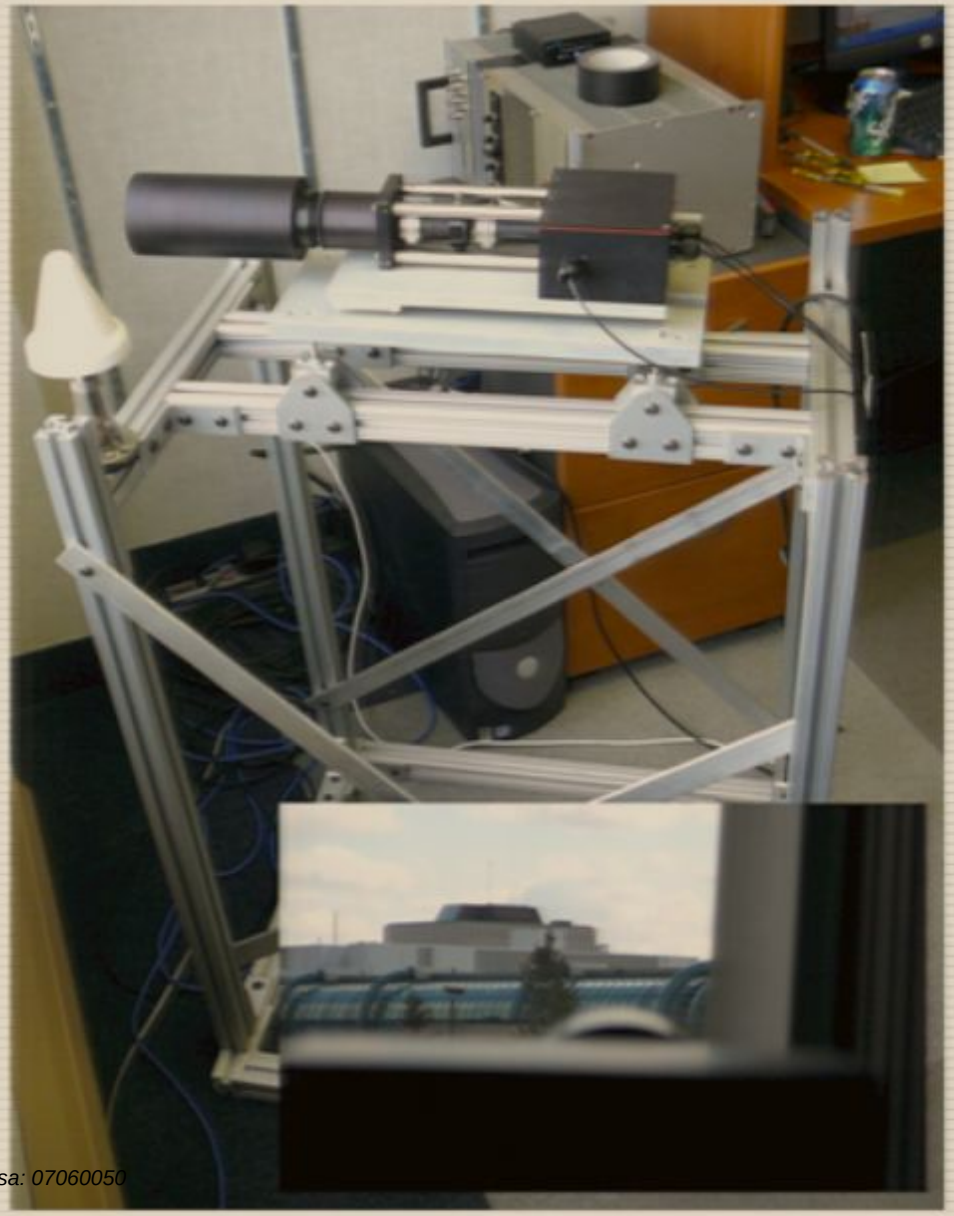


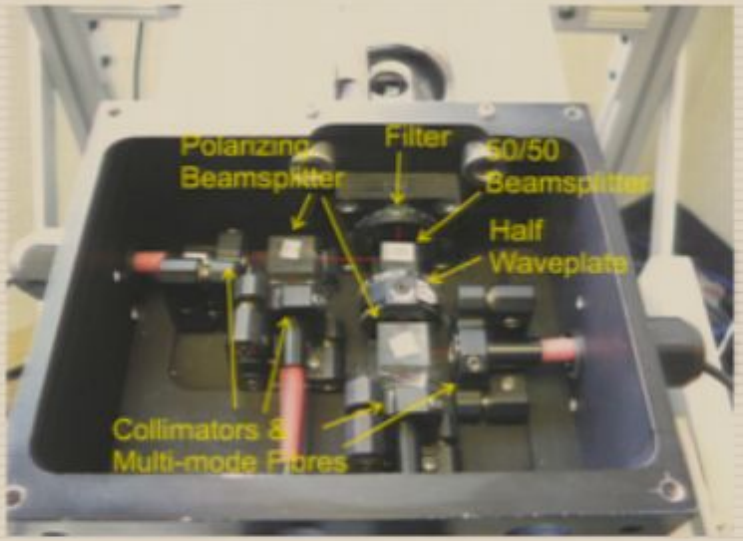
Entangled Photon Source on 6th floor of CEIT



Sender telescopes on roof of CEIT

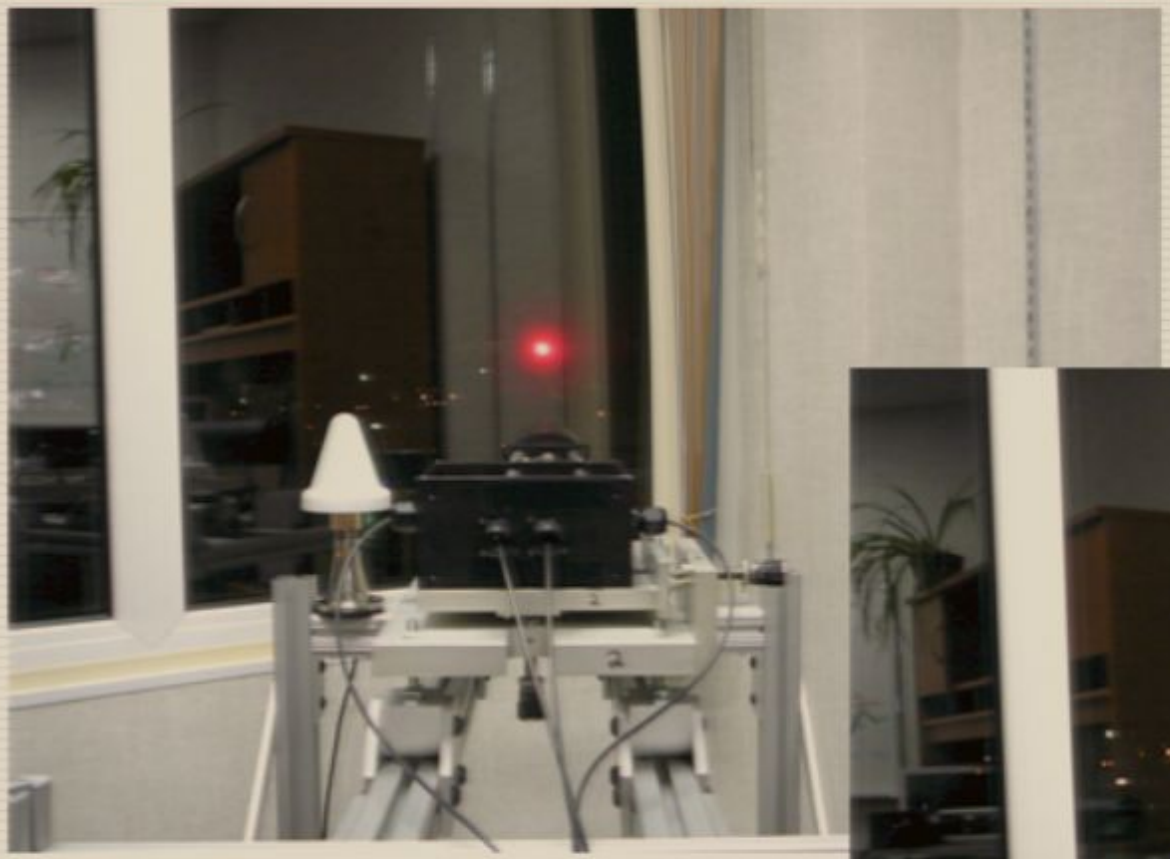
Alice's receiver station at BFG





Experimental Results

Aligning Alice at night at BFG



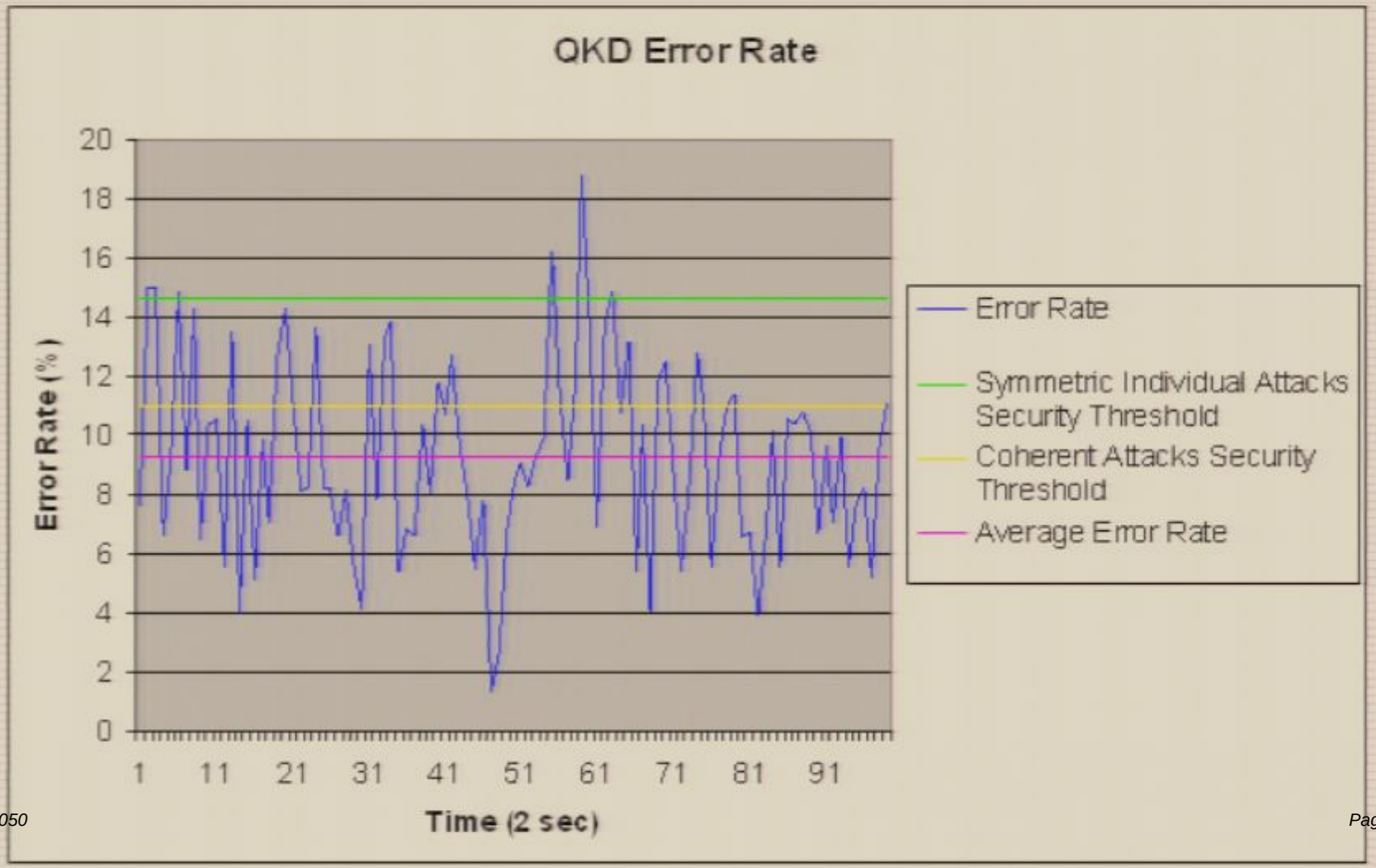
Fine Tuning Alice's Alignment

- With a ~7.1% link efficiency, Alice gets ~8,556 singles counts and ~750 coincidence counts per second

Movie

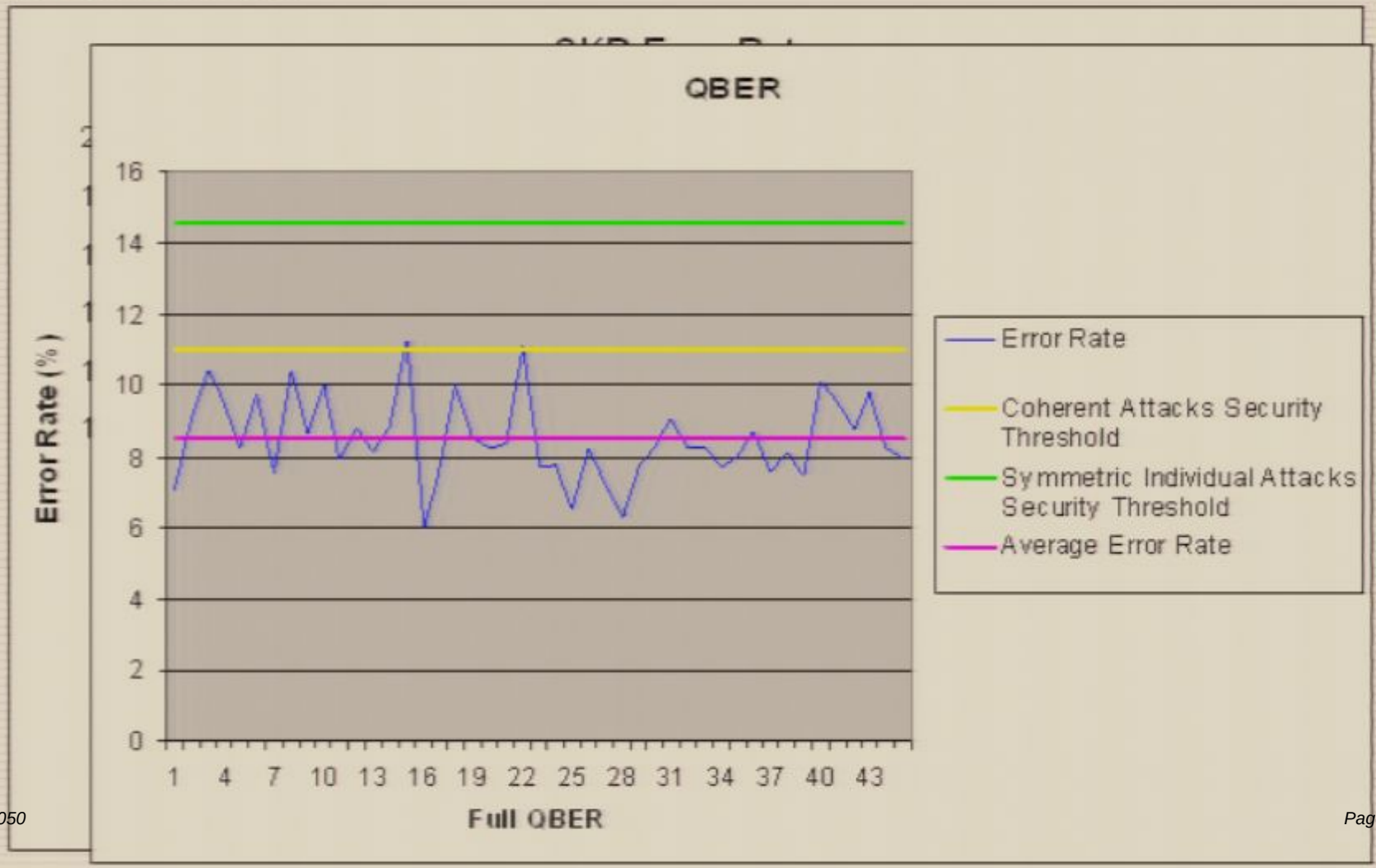
Experimental Results - QKD

- An average error rate of 9.29% ±0.33% was found over 3 minutes and 20 seconds of data collection

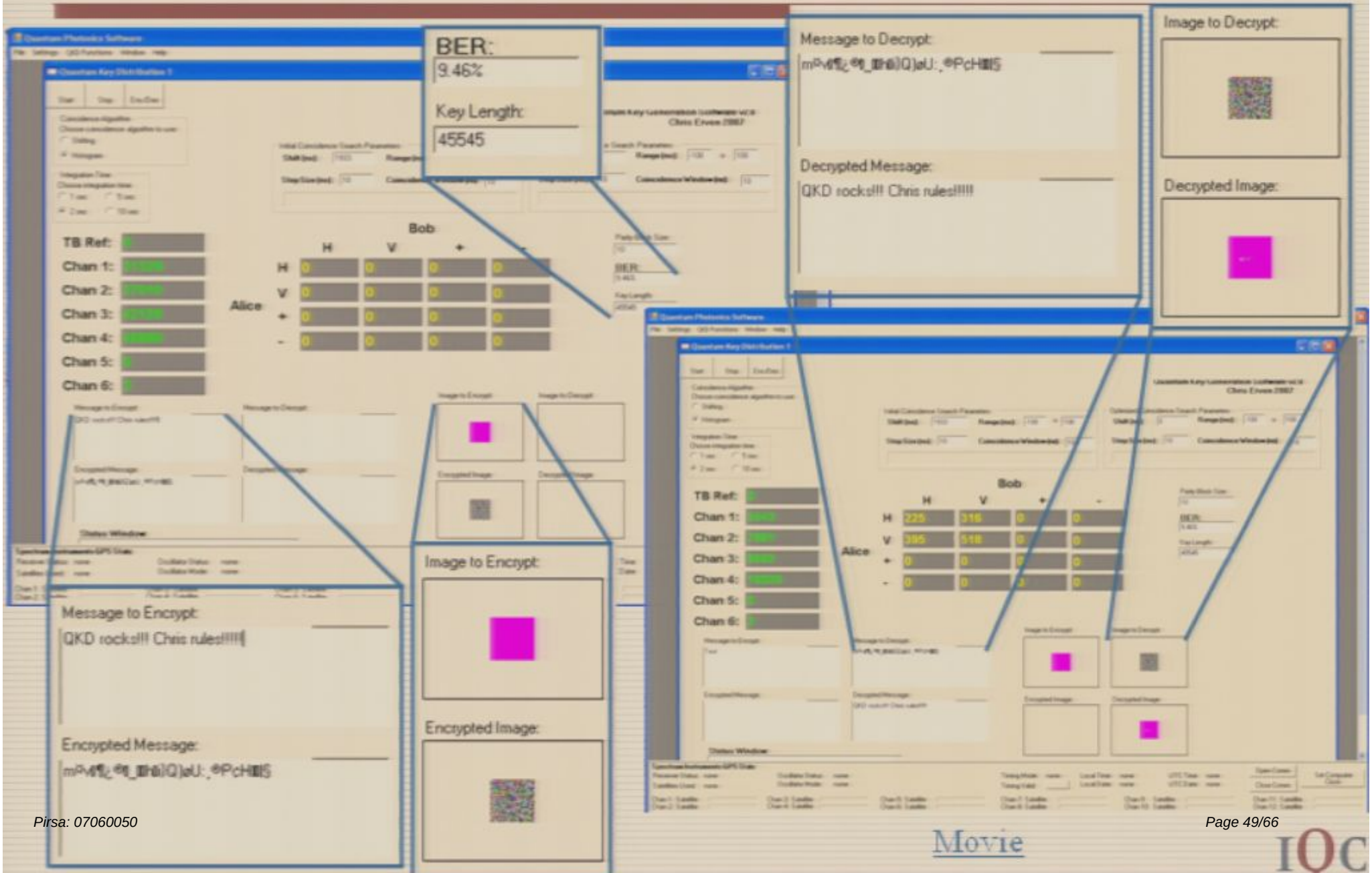


Experimental Results - QKD

- An average error rate of 9.29% ±0.33% was found over 3 minutes and 20 seconds of data collection



Experimental Results - QKD



Experimental Results - QKD

- Before error correction
  - Alice's Key

    10100011100000011111110011000010110001000110010000011110110000001101111100100111111
    10010011000101000010001101011101100001010010101011101101100010101001000001000110111
    11100111101010000010110010101101100100001101000001111011111110110010001011010100001 0
    10111010010100001100010110011111001010110010000010100

  - Bob's Key

    10100011100000011111110011000011110001000110101000001111011000001110111110010011111
    10010011000101000010001101010011000010101101010011011010000101010011000010001101110
    11100111101000000010110010101101100100011101000001111011111110111010001011101000011
    10111010010100001100010100111110010101100000000100100...

- After error correction and privacy amplification
  - Alice's Key

    11011111100010010101101000010100001001111110110111010010111101110001010010101010111
    10110001101111111000101010111101110100010000001110001000011110111010001111001101001
    01111110010101110000110111000010000100001010100001011011000111001001110101100111100
    ...

  - Bob's Key

    11011111100010010101101000010100001001111110110111010010111101110001010010101010111
    10110001101111111000101010111101110100010000001110001000011110111010001111001101001
    01111110010101110000110111000010000100001010100001011011000111001001110101100111100
    ...

Bell Inequality

Let's play with the following quantity

$$QS + RS + RT - QT = (Q+R)S + (R-Q)T$$

Either $(R-Q)T = 0$ or $(Q+R)S = 0$

And we can see that $QS + RS + RT - QT = \pm 2$

Now let's cast this in a statistical light

$$E(QS + RS + RT - QT) = \sum_{qrst} p(q,r,s,t) \cdot (qs + rs + rt - qt)$$

$$\leq \sum_{qrst} p(q,r,s,t) \cdot 2 = 2$$

Equivalently

$$E(QS + RS + RT - QT) = E(QS) + E(RS) + E(RT) - E(QT)$$

So we end up with the Bell inequality (actually CHSH inequality)

$$E(QS) + E(RS) + E(RT) - E(QT) \leq 2$$

Alice
Q = ±1
R = ±1

Bob
S = ±1
T = ±1

Experimental Results – Bell Measurement

- The CHSH inequality (Bell inequality generalized for actual experiments) reads

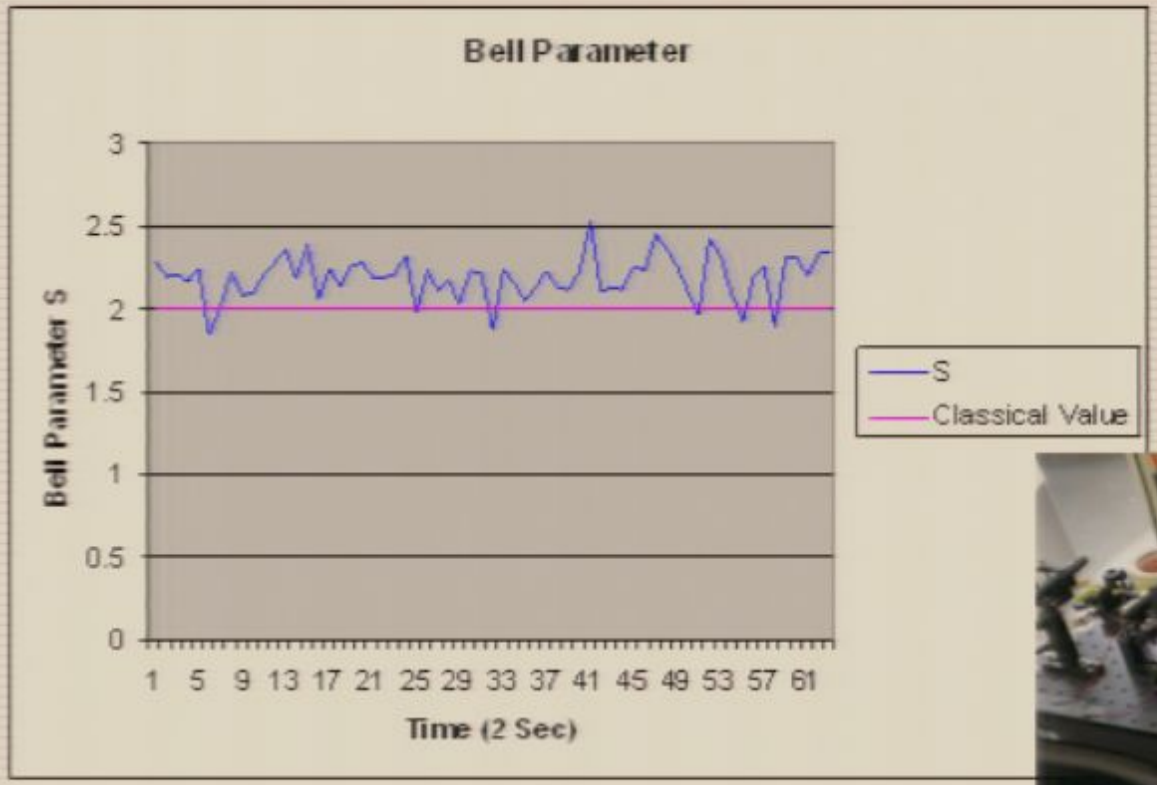
$$S(\alpha,\alpha',\beta,\beta') = \left|E(\alpha,\beta) - E(\alpha',\beta)\right| + \left|E(\alpha,\beta') + E(\alpha',\beta')\right| \leq 2$$

where

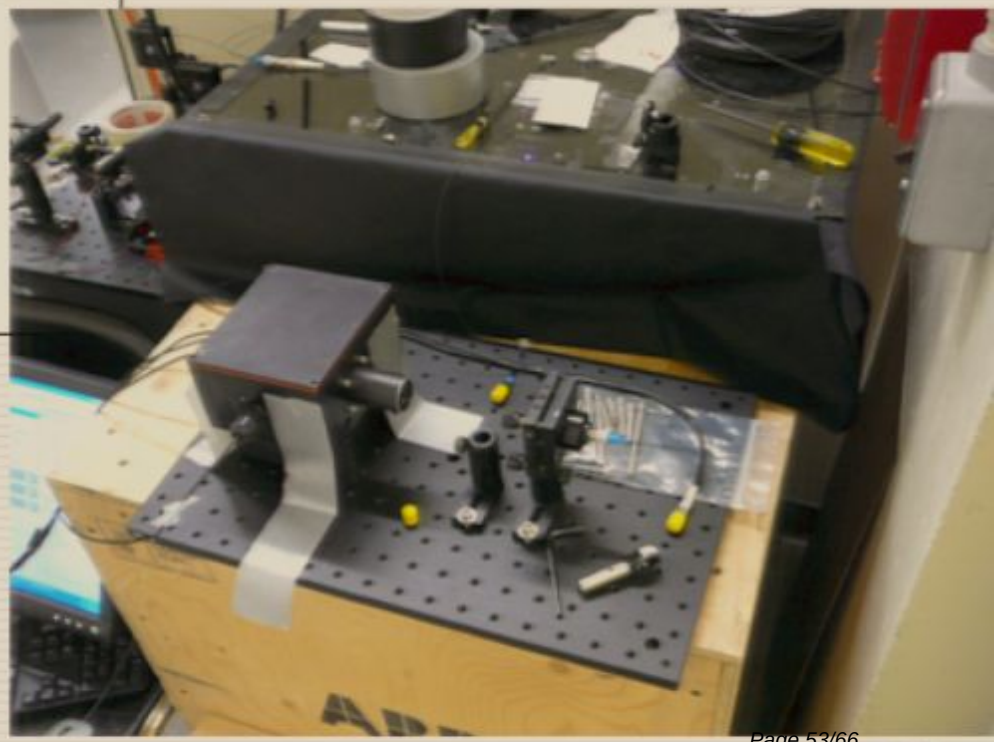
$$E(\alpha,\beta) = \frac{[C_{++}(\alpha,\beta) + C_{--}(\alpha,\beta) - C_{+-}(\alpha,\beta) - C_{-+}(\alpha,\beta)]}{N}$$

- Average Bell parameter of $S = 2.19 \pm 0.017$ was found over 3 minutes and 20 seconds of data collection

Experimental Results – Bell Measurement



Movie



Future Work

- Automation of the system and add alignment lasers to source board
- Develop improved entangled photon sources
- Investigate the use of adaptive optics to improve link efficiency
- Implement an Entanglement Witness for security
- Run 24 hours a day to investigate problems which arise
- Implement other Quantum Key Distribution and Quantum Communication protocols (3 state protocol, entangling the space-time metric, etc)
- Get the second link to PI working!

Back to Bob

Entangled State

$$|\leftrightarrow\rangle|\updownarrow\rangle - |\updownarrow\rangle|\leftrightarrow\rangle$$

$$= |\nearrow\rangle|\nwarrow\rangle - |\nwarrow\rangle|\nearrow\rangle$$

Back to Bob

Back to Bob

Back to Bob

Back to Bob

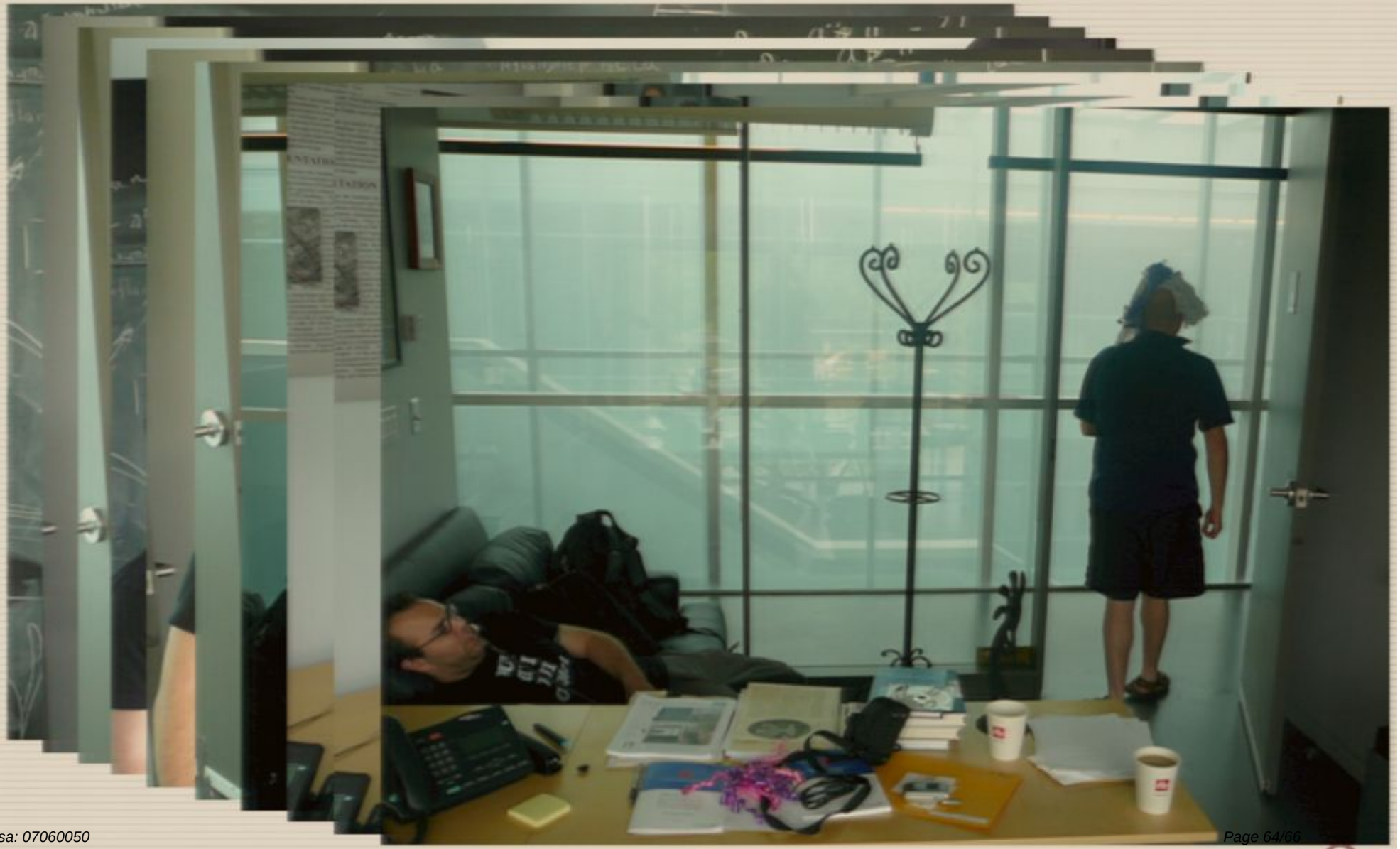
Back to Bob

Back to Bob

Back to Bob

Back to Bob

Back to Bob



Back to Bob

Future Work

- Automation of the system and add alignment lasers to source board
- Develop improved entangled photon sources
- Investigate the use of adaptive optics to improve link efficiency
- Implement an Entanglement Witness for security
- Run 24 hours a day to investigate problems which arise
- Implement other Quantum Key Distribution and Quantum Communication protocols (3 state protocol, entangling the space-time metric, etc)
- Get the second link to PI working!