Lecture 1: A taste of experimental quantum information techniques

Christian Kurtsiefer

Asher Peres International School, Chowder Bay @ Sydney, Nov 2008
Quantum physics does not happen in Hilbert space - quantum physics happens in the lab.

Misquoted? Don't know the exact reference but certainly a view of Asher Peres I subscribe to
Overview

- Photons as qubits
  - obvious things one can do in quantum information
  - what is commonly understood by a photon?
  - manipulate qubits
  - what really works well: detectors, pair sources
  - what also works: pair (sometimes multi) photon sources
  - Hamilton operators are useful!!

- Quantum key distribution schemes as the usual quantum info suspects
  - basic ideas: BB84
  - Bell inequalities to evaluate knowledge of eavesdropper
  - a practical implementation
  - some dreams and problems
want distinguishable things representing qubits with possible entanglement in system state:

\[ |\Psi\rangle_{tot} = \sum_i c_i |\Psi_{1,i}\rangle \otimes |\Psi_{2,i}\rangle \otimes |\Psi_{3,i}\rangle \otimes |\Psi_{4,i}\rangle \]
What is...a photon?

Highly recommended read:
Photons...?

- Definition via detection: photoelectric effect localizable in space/time, no energy eigenstates

- Definition via cavity mode excitation clean energy eigenstate labelling, very hard to observe

- Definition via spontaneous emission localizable in time/origin, well-defined preparation scheme “single photon sources” rely on that

- Definition via total energy in ~monochromatic field over hbar
What one can do with photons...

...in quantum information?

- transport light
- encode qubits...without loosing the superposition states

**polarization**

| ↑ | H |
| ↓ | V |

**time bin**

| ↑ | early |
| ↓ | late |

**optical path**

| ↑ | rail 0 |
| ↓ | rail 1 |
Easy: single qubit operations

- 1-qubit rotation

$$|\psi\rangle \xrightarrow{\lambda/2} |\psi\rangle$$

$$|\psi\rangle = \begin{pmatrix} \cos 2\varphi & -\sin 2\varphi \\ -\sin 2\varphi & -\cos 2\varphi \end{pmatrix} |\psi\rangle$$

- arbitrary 1-qubit operation

- measurement

- state preparation
Why are these easy operations?

- Inherit all the phase and amplitude manipulation abilities from classical optics / electrodynamics

\[
\begin{align*}
|\psi\rangle & \xrightarrow{\lambda/2} |\psi\rangle \\
|\psi\rangle & = \begin{pmatrix}
\cos 2\varphi & -\sin 2\varphi \\
-\sin 2\varphi & -\cos 2\varphi
\end{pmatrix} |\psi\rangle
\end{align*}
\]

- Birefringent materials, polarization states of light
POVMs in the lab....

Bloch / Stokes vectors corresponding to an optimal measurement scheme for polarization qubits

optical implementation by embedding in larger Hilbert space

Convergence in an experiment
What is hard?

- universal 2-qubit operations, require large optical nonlinearity

### Diagram

- hopeless with typical bulk nonlinearities
- possible with atoms close to resonance:

<table>
<thead>
<tr>
<th></th>
<th>A, B</th>
<th>A', B'</th>
</tr>
</thead>
<tbody>
<tr>
<td>0,0</td>
<td>0,0</td>
<td></td>
</tr>
<tr>
<td>0,1</td>
<td>0,1</td>
<td></td>
</tr>
<tr>
<td>1,0</td>
<td>1,0</td>
<td></td>
</tr>
<tr>
<td>1,1</td>
<td>(1,1) e^{i\phi}</td>
<td></td>
</tr>
</tbody>
</table>

work by S. Harris & friends in Stanford:
M. Lukin, Harvard:

atomic clouds
atoms in fibers
Detecting photons

- Use photoelectric effect: Convert electromagnetic field into a charge
  
  ![Diagram](image)

- detect an electron becomes an irreversible process in a very short time
Single photon detectors

• Photomultiplier
  low-medium quantum efficiency @IR...red, well understood
  can be fast

• Avalanche photodiodes above breakdown
  QE about 20-50% (manufacturer quotes 70%),
  repetition rate ~1MHz

• Superconducting detectors
  very high QE (>95% for some), photon number resolving,
  currently slow response rate

• (PIN photodiodes for continuous variables)
  not suitable for single photoelectron counting, high noise at
  low frequencies, up to very high quantum efficiency (>99%)
Single photon detectors 2

properties:

- quantum efficiency at operational wavelength (0.1..99%)
- timing jitter (30...500 ps)
- dark counts (0...20...100 000 cps)
- dead time (10ns...1us)
- ugly artefacts: afterpulses, selective blindability
- (intensity-dependent) delays
- gating needs
- temperature requirements (50mK...room temp)
Avalanche photodetector

- passive quenching topology:
Lower temperature to limit dark count rate...

-15 °C
'Making' photons

- spontaneous emission from atom-like systems
- cascade decays for making pairs
- parametric conversion in optical nonlinearities

Single Photon Sources

• making single photons at random times:

  spontaneous emission from
  atoms / color centers / quantum dots / single molecules

• making single photons deterministically (and sequences)

  use pulsed excitation,
  cavities to enforce emission in one mode via Purcell effect
Cascade Decays 2

- indistinguishable decay paths
  
  $(0,0) \rightarrow (1,1) \rightarrow (0',0)$ and
  $(0,0) \rightarrow (1,-1) \rightarrow (0',0)$

leads to polarization correlation of the photons:

$$|\Psi\rangle = \frac{1}{\sqrt{2}} (|\sigma^+ \sigma^-\rangle - |\sigma^- \sigma^+\rangle)$$

singlet Bell state $|\Psi^-\rangle$

Atomic Cascade Decays

Nonlinear optical processes: 3-wave mixing, 4-wave mixing:

response of a medium:

\[ P = \varepsilon_0 (\chi E + \chi^{(2)} E^2 + \chi^{(3)} E^3 + \ldots) \]

- Kerr nonlinearity
- refractive index, birefringence
- second harmonic generation
- parametric conversion
• making sometimes pairs of photons at random/fixed times

\[ \chi^{(2)} \]

pump laser

high fidelity maximally entangled photon pair states

• making combinations of 2/4/6.....photon events at fixed times:

\[ \chi^{(2)} \]
The first (?) PDC pair source

- correlation between detection times – makes us talk about pairs

\[ \lambda \]

\( \text{TIME DELAY } \tau \text{ IN CHANNEL 1 (NANOSECONDS)} \)

\( \text{COINCIDENCE RATE } R_c (\text{SEC}^{-1}) \)

\[ \text{D.C. Burnham, D.L. Weinberg, Phys. Rev. Lett. 25, 84 (1970)} \]
Photon pairs form PDC 3

- 'spatial' correlations:
  - coincidences show up for particular detector positions
- indicates momentum conservation

Type-II SPDC fluorescence
Entangled photon sources

- Use non-collinear type-II parametric down conversion

Two indistinguishable decay paths lead to

\[
|\Psi^-\rangle = \frac{1}{\sqrt{2}} (|HV\rangle - |VH\rangle)
\]

\[
= \frac{1}{\sqrt{2}} (|+-\rangle - |--\rangle)
\]

P.G. Kwiat et al., PRL 75, 4337 (1995)
Look at a particular wavelength range

Type-II SPDC fluorescence
**SPDC, quantitatively**

- Free electromagnetic field:
  \[
  \hat{H}_F = \frac{\epsilon_0}{2} \int \hat{E}^2(\vec{r}) + c^2 \hat{B}^2(\vec{r}) \, d^3 r
  \]

- Linear susceptible material
  \[
  \hat{H}_0 = \frac{\epsilon_0}{2} \int \chi \hat{E}^2(\vec{r}) + c^2 \hat{B}^2(\vec{r}) \, d^3 r
  \]

- With nonlinear material:
  \[
  \hat{H} = \frac{1}{2} \int \hat{E} \cdot \hat{P}(\vec{r}) + \epsilon_0 c^2 \hat{B}^2(\vec{r}) \, d^3 r
  \]
  \[
  = \hat{H}_0 + \frac{\epsilon_0}{2} \int \hat{E} \chi^{(2)} : \hat{E}^2(\vec{r}) \, d^3 r =: \hat{H}_0 + \hat{H}_I
  \]
Choose fields

- Pump is treated as classical field (non-depleted):

\[
\vec{E}_p(\vec{r}, t) = E_0 \vec{\epsilon} \left[ g(\vec{r}) e^{i \omega_p t} + g^*(\vec{r}) e^{-i \omega_p t} \right]
\]

- amplitude

- mode function
**Target modes**

- Electrical field operator

\[
\hat{E}_{s,i}(\vec{r}) = i E_{s,i} \bar{\epsilon} \left[ g(\vec{r}) \hat{a}(t) - g^*(\vec{r}) \hat{a}^+(t) \right]
\]

- Pump field
- Signal mode
- Idler mode

- Mode function
- Operator component

normalization
Typical mode functions

- Plane waves:
  \[ g(\vec{r}) = e^{i \vec{k} \cdot \vec{r}} \]
  conceptually nice, not really implemented in experiments

- Plane waves with a Gaussian envelope
  \[ g(\rho, z) = e^{ikz} e^{-\rho^2/w^2} \]
  typical laser beams and light that propagates in optical fibers (approx)
Normalize operator...The Works

- Get the magnetic field operator

\[
\hat{B}_{s,i}(\vec{r}, t) = \frac{1}{i \omega} E_{s,i} \left[ \nabla \times (\vec{\varepsilon} \, g(\vec{r})) \hat{a}(t) + \nabla \times (\vec{\varepsilon} \, g^*(\vec{r})) \hat{a}^+(t) \right]
\]

- Free field should look like harmonic oscillators:

\[
\hat{H}_0 = \frac{\varepsilon_0}{2} \int_V \left[ \hat{E}^2(\vec{r}) + c^2 \hat{B}^2(\vec{r}) \right] dV = \sum_{\text{modes } j} \hbar \omega_j (\hat{a}_j^\dagger \hat{a}_j + \frac{1}{2})
\]

you need dispersion here:

\[
c^2 k^2 = \omega^2 \quad \text{for plane waves}
\]

you get

\[
E_{s,i} = \sqrt{\frac{\hbar \omega_j}{2 \varepsilon_0 V}}
\]

for plane waves
Simplify $H_I$

$$\hat{H}_I = \frac{\varepsilon_0}{2} \int \hat{E}_p (\vec{r}, t) \chi^{(2)} \hat{E}_s (\vec{r}, t) \hat{E}_i (\vec{r}, t) \, d^3 r$$

- eight terms, integral only over mode functions:

$$\hat{H}_I = \sum_{n, m} \frac{\varepsilon_0}{2} E_0 E_{s_n} E_{i_m} \left( \hat{\epsilon}_p \chi^{(2)} \hat{\epsilon}_{s_n} \hat{\epsilon}_{i_m} \right) \times$$

$$\left[ \int_V g_P (\vec{r}) g_{s_n} (\vec{r}) g_{i_m} (\vec{r}) \, d^3 r \times \hat{a}_{s_n} (t) \hat{a}_{i_m} (t) e^{i \omega_p t} \right] + 7 \text{ more terms}$$

- constants
- mode indices
- spatial aspect
- interaction volume
- operator character
- + time dependencies
Phase matching

\[ S := \int_V g_P(\vec{r}) g_{s_n}(\vec{r}) g_{i_m}(\vec{r}) \, d^3 r \]

- Plane waves:
  \[ S = (2\pi)^3 \delta_{xyz}(k_P + k_s + k_i) \]

- Finite size of interaction thickness:
  \[ S = (2\pi)^2 \delta_{xy}(k_P + k_s + k_i) \times a \, \text{sinc} \left[ (k_{z,P} + k_{z,s} + k_{z,i}) a / 2 \right] \]
Phase matching 2

\[ S := \int_V g_P(\vec{r}) g_{sn}^*(\vec{r}) g_{im}^*(\vec{r}) \, d^3r \]

- plane waves:
  \[ S = (2\pi)^3 \delta_{xyz}(k_P - k_s - k_i) \]

- finite size of interaction thickness:
  \[ S = (2\pi)^2 \delta_{xy}(k_P - k_s - k_i) \times \]
  \[ a \text{sinc} \left[ (k_{z,P} - k_{z,s} - k_{z,i}) a / 2 \right] \]

approximate momentum conservation

for terms with \( \hat{a}_s \hat{a}_i \)
So now we have...

\[ \hat{H}_I = A \left( \hat{a}_s^+ \hat{a}_i^+ e^{-i\omega_p t} + \hat{a}_s \hat{a}_i e^{+i\omega_p t} \right) \]

......and we know \( A \) quantitatively

Where do we go from here on?

- consider asymptotic states (vacuum fields -> pair states)

\[ |\Psi_f\rangle = |1_s, 1_i\rangle = \hat{a}_s^+ \hat{a}_i^+ |0\rangle \]

- do Fermi's golden rule for rates from the vacuum

\[ |\Psi_i\rangle = |0\rangle \]

...brings energy conservation
Rate details

• for fixed target wave index $k_s$

$$ R(k_s) = \frac{2\pi}{\hbar} \left| \langle \Psi_i | \hat{H}_I | \Psi_f \rangle \right|^2 \rho(\Delta E) $$

• total rate in all possible $k$s: (Gaussian beams, collinear modes of waist $w_s=w_i=w_p$):

$$ R_T = \frac{4 d^2 a P \omega_p}{9 n_s n_i n_p \varepsilon_0 \pi w_p^2 (n_i-n_s) c^2} $$

d: effective nonlinearity
a: crystal thickness
n: refractive indices
P: pump power

typically ~5000 pairs/sec/mW for 2mm thick BBO in type-II
An efficient pair source

- Choose a target wavelength which is suitable for detectors
- couple target modes in single mode optical fibers
- Remove residual distinguishability between photons due to birefringence
Match angular dispersion

- Choose an optical bandwidth $\Delta \lambda$
- Choose collection angle of fiber modes to $\Delta \theta = \Delta \lambda \frac{d\theta}{d\lambda}$
- Restrict pump mode to collection region

Pair and single rates

- high brightness by mode matching, observed pair/single ratio: 28%
Entanglement Quality

- Visibility of polarization correlations:
  HV: 98.2%, ±45deg: 96.3%

- Violation of a CHSH-type Bell inequality:
  $S = 2.6989 \pm 0.0034$ (204 $\sigma$ in 1sec/point)
Other experimental tests

- Visibility of Polarization correlation >99% in all bases
- Leggett-type inequalities for (nonlocal) hidden variable models

Practical pair source

Blue diode-laser as pump source, BBO as nonlinear crystal

- 24,000 s$^{-1}$ detected pairs from 40 mW pump @ 407nm in single mode fibers at 810/818 nm, 2mm BBO crystal
- polarization correlation visibility in 45° basis: 92%
Much better implementations

Colinear down conversion, periodically poled materials

F. Wong et al., MIT


P. Trojek, H. Weinfurter, arxiv:0804:3799

Geneva group: waveguide sources

- Up to 1000 times brighter than non-colinear sources
- Polarization correlation visibility in 45° basis > 99%
Summary

- Make single qubits and qubit pairs
- Manipulate and transport photonic qubits
- Fundamental tests of quantum mechanics
  test Bell-type inequalities & friends
- Quantum communication
  quantum cryptography
Time for Coffee.....

Thank you!

http://qoptics.quantumlah.org/lah/

CQT Graduate program:
http://cqtphd.quantumlah.org
Lecture 2: Aspects of Quantum Cryptography

Christian Kurtsiefer

Asher Peres International School,
Chowder Bay @ Sydney, Nov 2008
Quantum 'cryptography'

- better: quantum key distribution
- even better: quantum key growing

- BB84 protocol
- Ekert protocol
- Device independent key distribution
**BB84 protocol**

**Prepare & measure protocols (BB84 & friends/derivatives):**

- Uses error fraction to estimate eavesdropper's knowledge
- Discussion over classical channel (basis, sifting)
- Error correction, privacy amplification

- Single photon source
- Quantum channel
- EO modulators
- PBS
- Detectors

• uses error fraction to estimate eavesdropper's knowledge
Encoding information....

- ....works also with other perpendicular polarizations.....

- ....but you need correct measurement basis:

<table>
<thead>
<tr>
<th>prepare</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>measure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Heisenberg uncertainty principle:
random results
Error detection / correction

- Some errors are due to imperfect devices, detectors, background light etc.
- Some errors indicate an eavesdropping attempt
- Correct errors by discussing parity bits over blocks openly:

  **ALICE:** 0111 0101 0101 0110 1010 0111 0101 .......

  **BOB:** 0110 0101 0111 1110 1010 0111 0101 .......

- **A→B:** p=1  p=0  p=0  p=0  p=0  p=1  p=0 .......

- **B→A:** ERR  OK  ERR  ERR  ERR  OK  OK  OK .......

Other encoding techniques

- Encoding qubit in relative phase between two packets

  \[ \phi_a = 0, \pi/2, \pi, 3\pi/2 \]

- Replace fiber pair by time structure (early / late)

  \[ \phi_b = 0, \pi/2 \]

  equivalent to polarization encoding
Consecutive measurements

- same basis: always same outcome

- different bases

random outcome at first PBS
Estimate Eve's knowledge

- Raw key with errors: $N_r$ bits

- Quantum bit error ratio (QBER): $\eta$

- Number of bits leaked to an eavesdropper $N_e$

$$N_e = N_r \left( h(\eta) + h(\eta) \right)$$

possible knowledge of an eavesdropper revealed in (optimal) due to measurements error correction

binary entropy: $$h(\eta) = -\eta \log_2 \eta - (1-\eta) \log_2 (1-\eta)$$
Estimate Eve's knowledge

I(A:B) after error correction

depends on the attack model (individual attack); for *infinite* key length and (!) single photons
Privacy amplification

- compress raw key to the information advantage vs. Eve.

\[
\begin{bmatrix}
0 \\
1 \\
0 \\
1
\end{bmatrix} = \begin{bmatrix}
0 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1
\end{bmatrix} \times \begin{bmatrix}
1 \\
0 \\
1 \\
1 \\
1 \\
0
\end{bmatrix}
\]

Eve may know this

- All information leaked to Eve (attacks + error correction) has to be considered

**Tricky:** finite key length may make privacy amplification more difficult – \( \sim 10^7 \) to \( 10^{10} \) bits
BB84 original implementation

C. Bennett, F. Bessette, G. Brassard, L. Savail, J. Smolin
J. Cryptology 5, 3 (1992)
Imperfect 'single photons'

- use faint coherent pulses instead of single photons

\[ p(n) = \frac{\lambda^n}{n!} e^{-\lambda} \quad \text{for} \quad \langle n \rangle = 0.1 \]

\[ p(0) = 90.48\% \quad p(1) = 9.05\% \quad p(n>1) = 0.47\% \]

- much simpler to prepare than true single photons:

- potentially insecure: photon number splitting attack
  --- > decoy state protocol

A Prepare & Send problem:

...needs lots* of trusted random numbers!

- Do you trust your random numbers?

* Mbit/sec for kbit/sec key
Quantum Random numbers

- use beam splitters and single (post-selected) photons

\[ \text{J.G. Rarity et al., J. Mod. Opt. 41, 2345 (1994)} \]
\[ \text{T. Jennewein et al., Rev. Sci. Inst. 71, 1675 (2000)} \]

- need to remove bias, two detectors
Quantum RNG II

- extract Poissonian photon statistics

- 20 Mbit/s
Preparation of polarized photons

- Make use of good intrinsic polarization of laser diodes

![Diagram of polarized photons](image)

**basis** **value**

**spatial filter**
BB84: Spectral attack

Don't measure polarization, but e.g. color:
The Hilbert Space in your system is larger than it appears

H V - +

asymptotic average information leakage: <2%
Polarization measurement

- Replace active basis choice by passive choice in a beam splitter

Bridging distances

Even further...

- use decoy states to reveal an eavesdropping attempt in a high loss regime
Go Global

- Use satellites as trusted relays between distant locations

- ....but why should you trust it?
QKD with photon pairs: BBM92

Quantum correlations & measurements on both sides

- no trusted random numbers for key
- direct use of quantum randomness for measurement basis

public discussion (sifting, key gen / state estimation)

error correction, privacy amplification
Practical pair source

Blue diode-laser as pump source, BBO as nonlinear crystal

- 24,000 s\(^{-1}\) detected pairs from 40 mW pump @ 407 nm in single mode fibers at 810/818 nm, 2 mm BBO crystal
- polarization correlation visibility in 45° basis: 92%
NUS campus test range

receiver

transmitter

1.5 km
Receiver unit

alignment laser

receiving telescope

polarization analyzer passively quenched Silicon APD
- QE ~50%
- ~1000s$^{-1}$ dark cnt rate

spatial filter (150 µrad)
Scintillation in atmosphere

Telescope dia 76mm

95% power diameter ~60mm

(40 mm FWHM)
Identified raw coincidences between close and remote receiver

(time of day (21.5.-22.5.2006))

(true coincidences)

(accidental coinc x10)

(transmitter telescope pointing changes)

(with interference filter 5nm FWHM, 50% peak transmission)
....and after The Works:

- CASCADE error correction with ~6000 bit packets
- assume incoherent attack strategy for privacy amplification
- average efficiency of EC/PA: >57%
- average final key rate: 650 bits/sec
- residual error rate ~10^{-6} due to a stupid error
No interference filter

- use a RG780 long pass filter to suppress visible light
- average final key rate 850 bits/sec

(data taken 1.6.2006)
Atmospheric absorption

- representative vertical atmosphere layer (corresponds to ~11 km air on ground)
Optical fibers as 'channel'

- Use existing telecom infrastructure
- independent of environment
- high transmission:
  - 800nm: 2dB/km (T=63% in 1km)
  - 1310nm: 0.2dB/km (T=63% in 10km)
  - 1550nm: 0.35dB/km (T=44% in 10km)
- stress birefringence and geometric phases are time dependent:
Birefringence compensation

- Probe fiber birefringence via two passes with Faraday mirror

- Basis of “Plug & Play” or autocompensation schemes in commercial QKD systems (id quantique, NEC)

- Bridging ~100 km

N. Gisin & team, GAP optique, Geneva
D. Bethune / W. Risk, IBM Almaden
A. Karlsson, KTH Stockolm
NEC
Compare figures of merit

- BB84 raw key rate:
  \[ r = \frac{f_0 \times \mu \times \eta_d}{2 \times T} \]
  \( \downarrow \) channel transmission
  \( \uparrow \) primary send rate
  \( \uparrow \) detector efficiency

- Probability for a background event:
  \[ P_D = d \times \tau \]
  \( \uparrow \) detector dark count rate
  \( \uparrow \) detection time window
  Si: \( 10^{-7} \)
  InGaAs: \( 10^{-5} \)

- Detector-induced bit error ratio
  \[ QBER = \frac{P_D \times f_0}{r} = \frac{2 \times P_D}{\mu \times \eta_d \times T} \]
Entanglement based protocols

Find eavesdropper not via errors, but via testing entanglement: Ekert91 – type and tomographic protocols

 maximal entanglement between A and B

 reduced entanglement between A and B
**Bell inequality I**

Correlation between setting $i, j$: 
$$E(i,j) := \frac{n(i,j) + n(\bar{i}, \bar{j}) - n(i, j) - n(\bar{i}, \bar{j})}{n(i,j) + n(\bar{i}, \bar{j}) + n(i, j) + n(\bar{i}, \bar{j})}$$

Combined correlation function: 
$$S := E(1,1') + E(1,2') + E(2,1') - E(2,2')$$

If there is a local hidden parameter $\lambda$ (= knowledge of $E$) governing the measurement outcomes of $A$ and $B$, then: 
$$|S| \leq 2$$
Bell inequality II

For proper settings 1, 2, 1', 2' and state $|\Psi^-\rangle$: $S = \pm 2\sqrt{2}$

- Estimate quantitatively the knowledge of Eve of raw key between A and B from S:
  $$I_E(S) = h\left(1 + \frac{\sqrt{S^2/4 - 1}}{2}\right)$$

- Assume “fair sampling” between key measurement and Bell test

- No fingerprint problems of photons due to side channels

E91 Implementation

- use almost same kit:

\[
\begin{align*}
1, 1' (V) & \quad 3 (67.5°) \\
3' (+45°) & \quad 5 (22.5°) \\
2, 2' (H) & \quad 4 (-22.5°) \\
6 (-67.5°) & \quad 4' (-45°)
\end{align*}
\]

- \{H,V; H',V'\} coincidences \quad \text{key generation}

- \{H,V,+,+-;H'',V'',+,+-\} coincidences \quad \text{CHSH Bell test}

- low QBER with existing simple source
Field results (1.4km range)

- typical data run (with tropical rainfall inbetween)
For non-lossy detectors and a measurement basis decision at “free will” of the observers:

No assumptions on devices and source is necessary to get an upper bound for eavesdropping!

Field usage...

PDC pair source & sender

- System gets simpler and more robust

Receiving side

- Open source: http://code.google.com/p/qcrypto

Detector breakdown signature

- detection scenario
- hot carrier recombination spectrum
- attack scenario
- approx 40 photons/sr in Si APD

Timing channel attack I

Photon from quantum channel

BS \(\lambda/2\) PBS APD

PBS APD

Projection optics

Signal conditioning

Timing basis

Public information

Secret bit
Classical timing information carries fingerprint of detectors:

small detector imbalances may tell Eve a lot!
Timing channel attack – The Cure

- Make sure no detail timing information is revealed.

Alternative cures (costly for background):
- coarser quantized timing information
- add timing noise

Nastier attacks:
V. Makarov
Trondheim
H.K. Lo, Toronto
Time for Coffee.....

Thank you!

http://qoptics.quantumlah.org/alah/

CQT Graduate program:
http://cqtphd.quantumlah.org