The Abdus Salam
International Centre for Theoretical Physics

United Nations
Educational, Scientific
and Cultural Organization

International Atomic
Energy Agency

SMR.1738 - 23

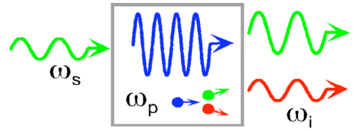
WINTER COLLEGE
on
QUANTUM AND CLASSICAL ASPECTS
of
INFORMATION OPTICS

30 January - 10 February 2006

Fiber-optic Quantum Communication and Applications

Prem KUMAR

Dept.Elec.& Comp.Engineering
Northwestern University
2145 N. Sheridan Road
IL 60208-3118 Evanston
USA

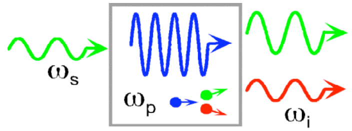


Fiber-optic Quantum Communication and Applications

Prem Kumar
Northwestern University

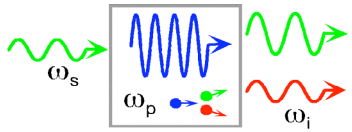
Winter College on
Quantum and Classical Aspects of Information Optics
ICTP, Trieste, Italy
February 9, 2006

Topics for Lecture 3



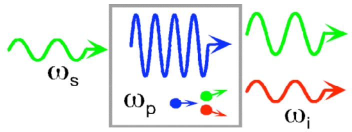
- Fiber nonlinearity for quantum communication
- Entanglement generation in fibers
- Quantum cryptography with fiber systems
- Keyed communication in quantum noise.
  - Cryptographic objective: direct data encryption
  - Cryptographic objective: key generation

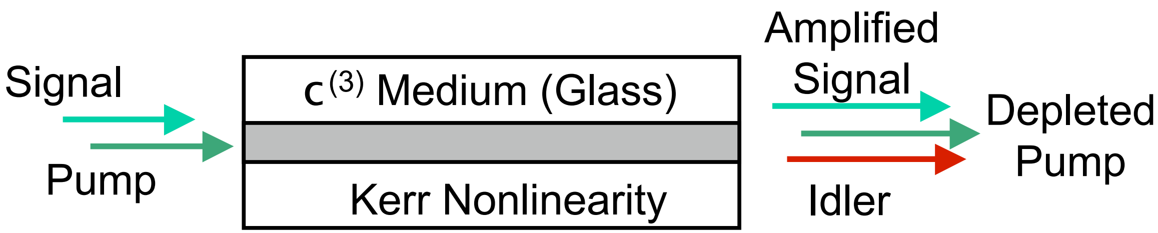
Our Motivation for Using Fibers

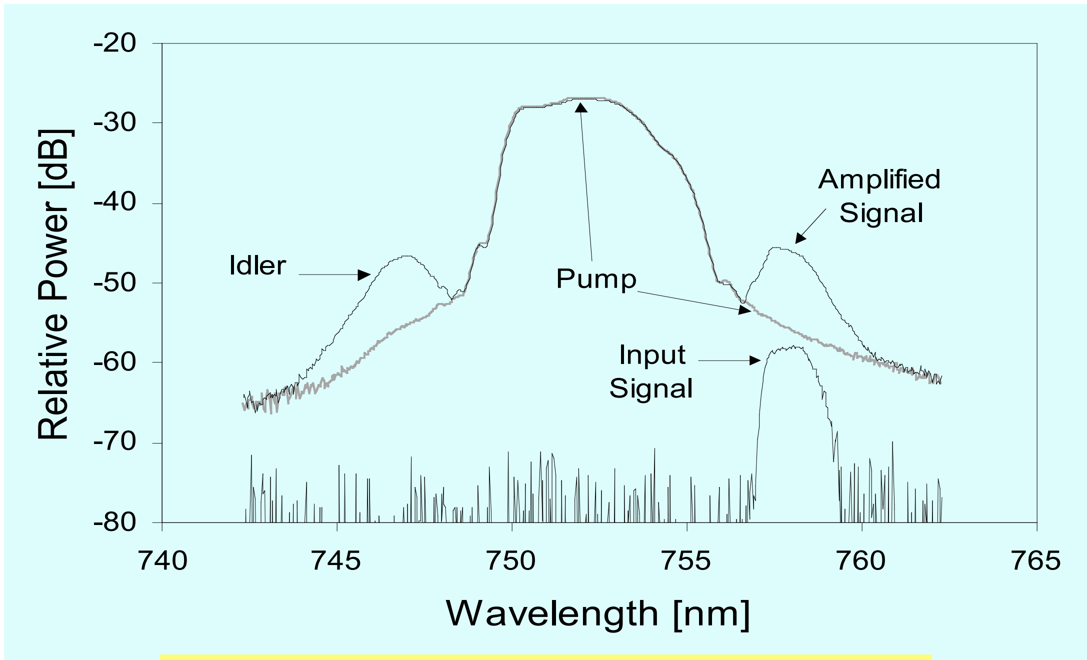


- Realistic long-distance quantum communication must integrate with existing optical-fiber networks
- Fiber offers several advantages over $c^{(2)}$:
  - Excellent modal purity, highly desirable for schemes requiring multiple quantum interactions
  - Possible to wavelength multiplex several entangled channels on existing fiber plant
  - Avoids coupling photons from $c^{(2)}$ crystals into fiber
  - Long interaction lengths possible, owing to high quality of commonly available optical fibers
- Side benefit: Allowing us to investigate fundamental limits of practical optical communication technology

Four-Wave Mixing and Parametric Fluorescence in Optical Fiber



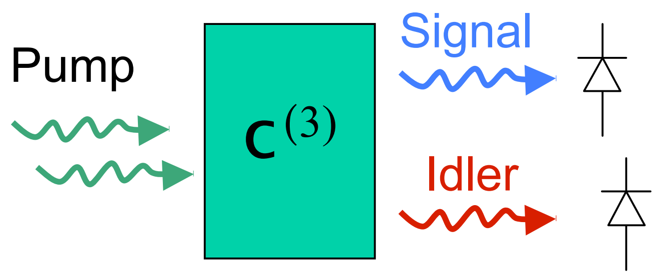




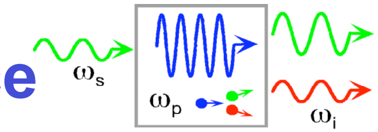
Sharping et al., Opt. Lett. ***26****, 1048 (2001)*

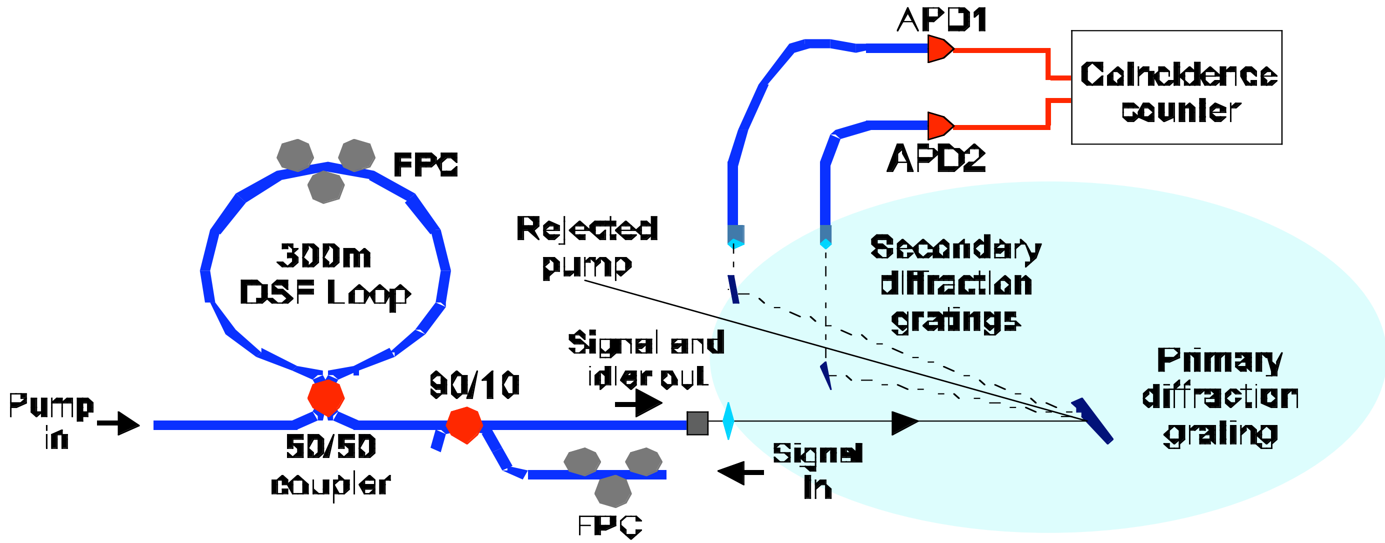
Quantum Mechanically:

- FWM is nondegenerate optical parametric amplification (OPA), as in $c^{(2)}$ crystals
- Signal and idler photons are created in pairs
- *They should exhibit entanglement properties similar to signal and idler photons created in $c^{(2)}$ parametric down-conversion*



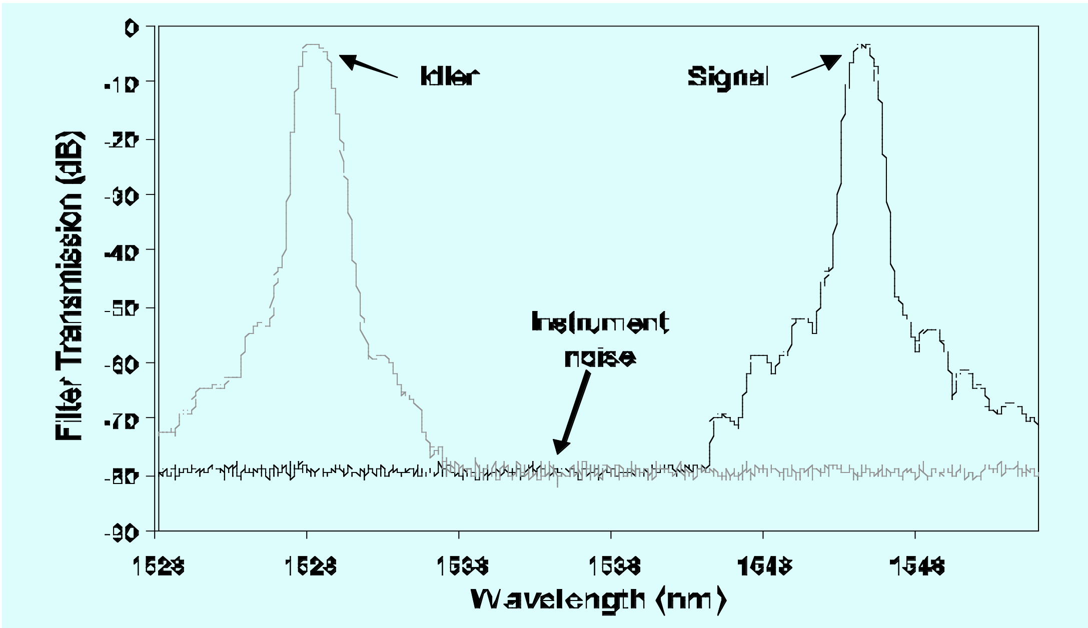
Photon Counting of Parametric Fluorescence



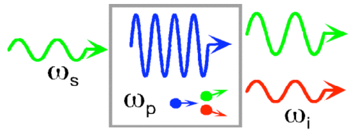


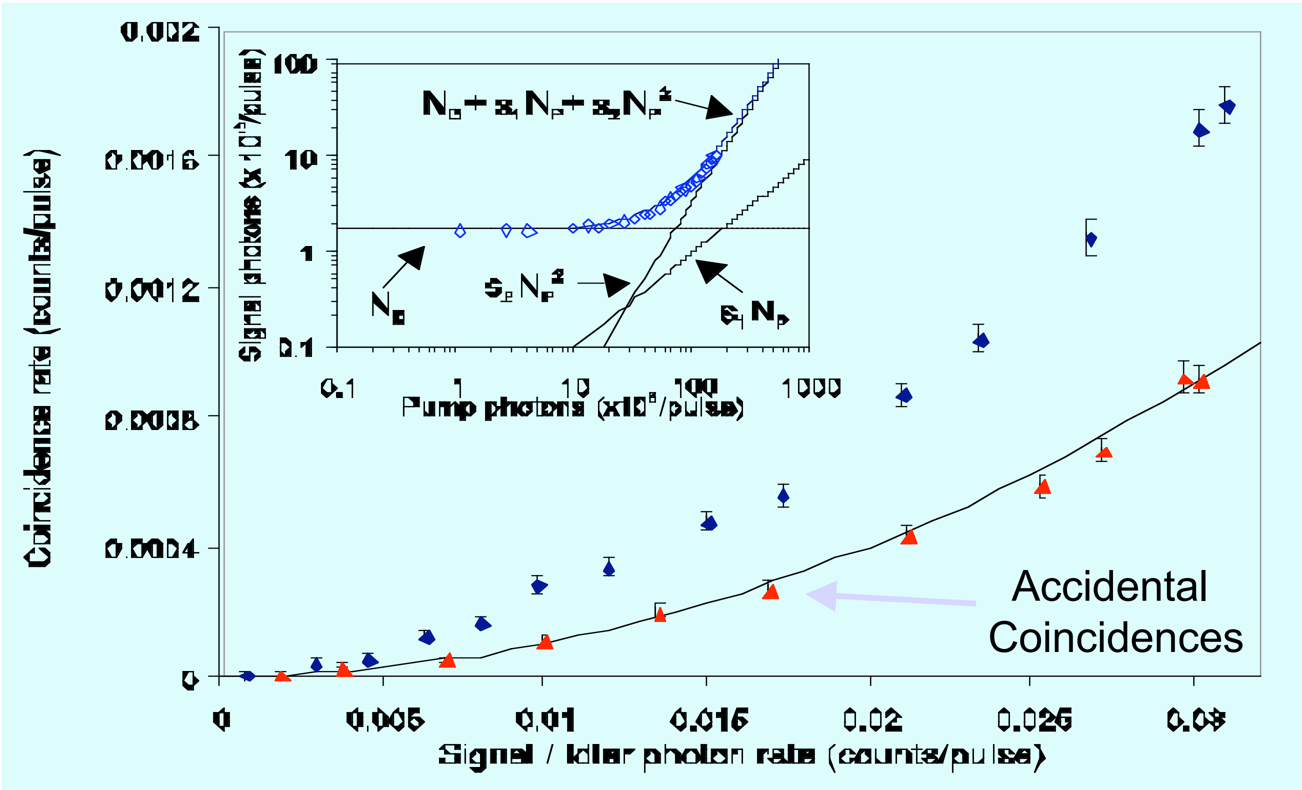
Double Grating Filter

- Pump pulse contains ~10^8 photons
- Interested in detecting 0.01 photons / pulse
- Therefore, 100 dB rejection of pump photons is required
- > 30dB rejection by Sagnac loop helps a great deal



Coincidence Counting Results

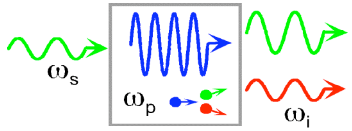




- We tested the parametric fluorescence at the single photon level
- The counted photon number depends quadratically on the injected pump photon number

Fiorentino, Voss, Sharping, and Kumar, IEEE Photon. Technol. Lett. ***14****, 983 (2002)*

- We measure coincidences for signal and idler photons generated by one pump pulse
- Coincidence rate is greater than that measured for two adjacent pulses
- The latter fit well with the theory for two independent pump sources



How do we create Polarization Entanglement?

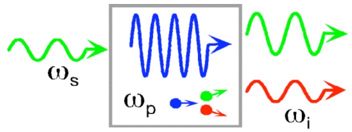
Isotropic nature of Kerr nonlinearity gives

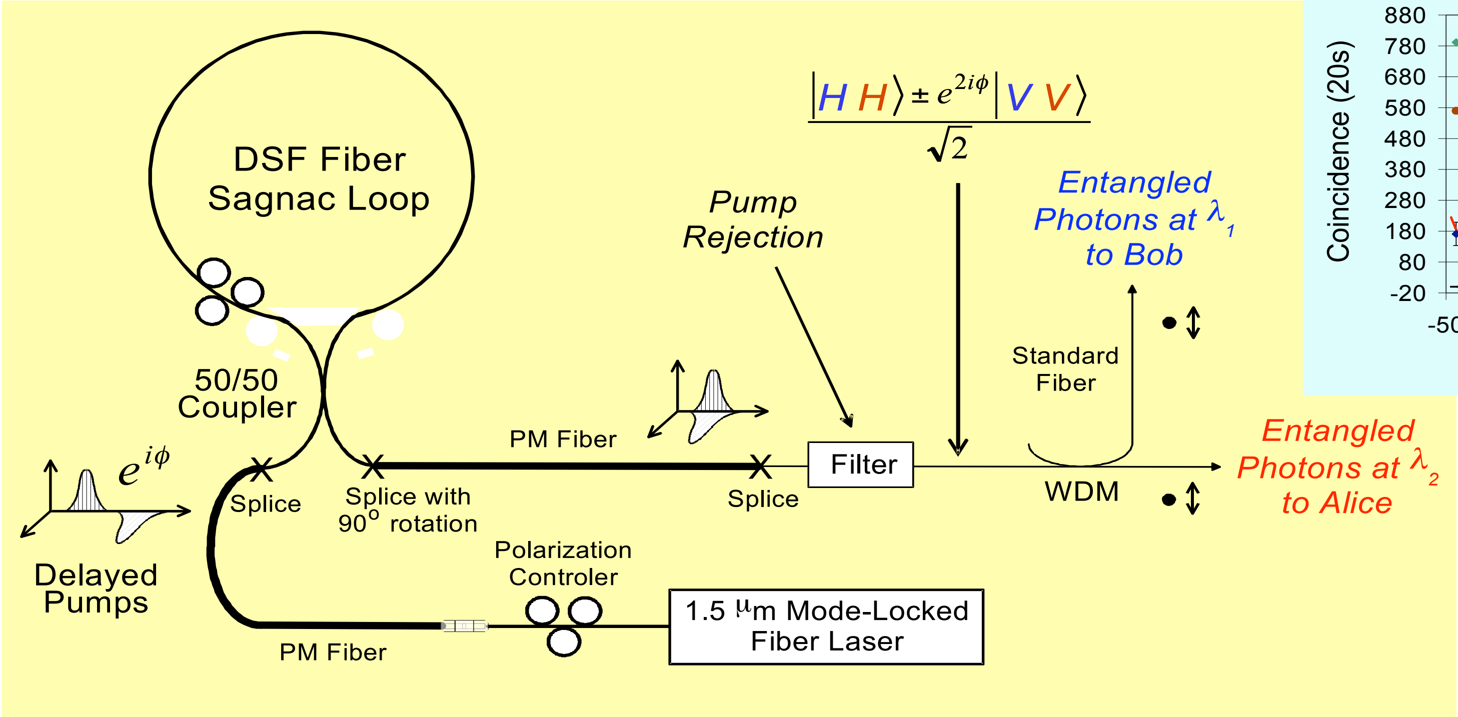
$$|H\,H\rangle \quad \text{or} \quad |V\,V\rangle$$

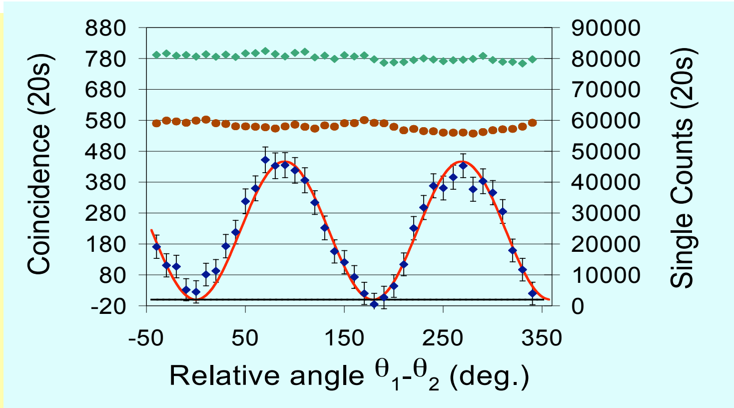
How to get:

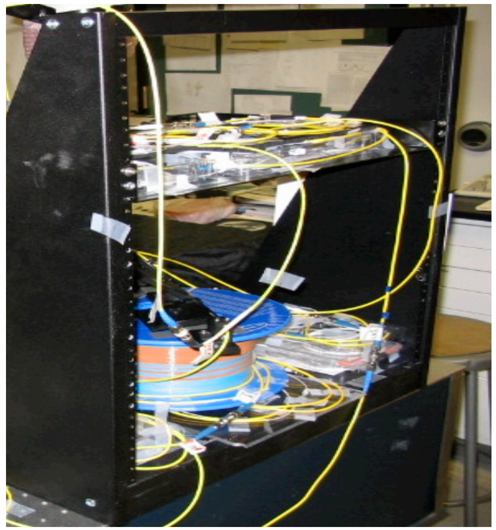
$$\frac{|H\,H\rangle \pm e^{2i\phi}|V\,V\rangle}{\sqrt{2}}$$

Fiber Source of Polarization-Entangled Photons

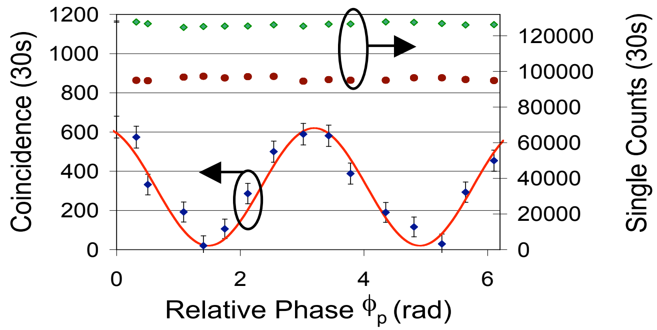


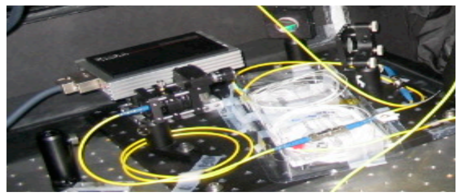






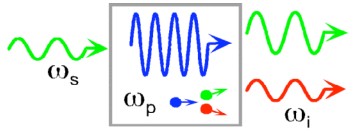
Bell State	***S***	**Violation**
H H + *V V*	2.75 ± 0.077	10 σ
H H – *V V*	2.55 ± 0.070	8 σ
H V + *V H*	2.48 ± 0.078	6 σ
H V – *V H*	2.64 ± 0.076	8 σ

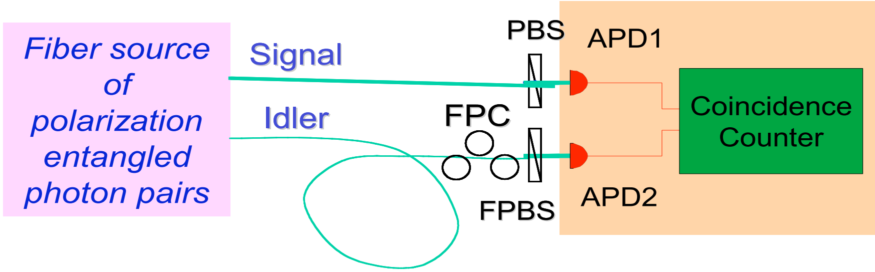




X. Li *et al.*, *PRL* **94**, 053601 (2005).

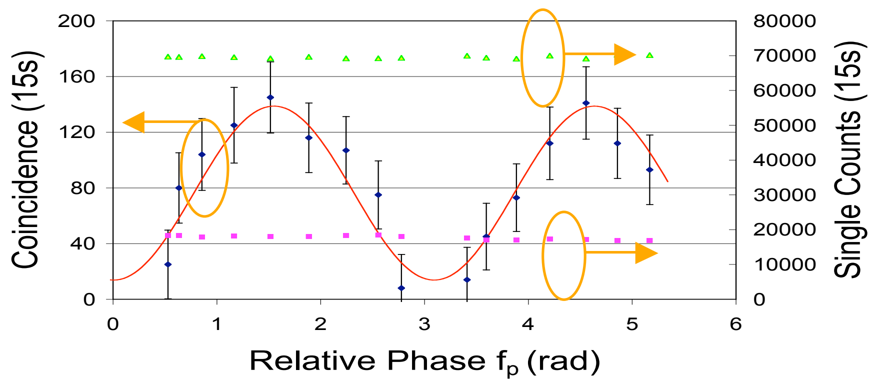
Quantum Memory and Distribution of Polarization-Entangled Photons





25Km Fiber Spool (Corning LEAF)

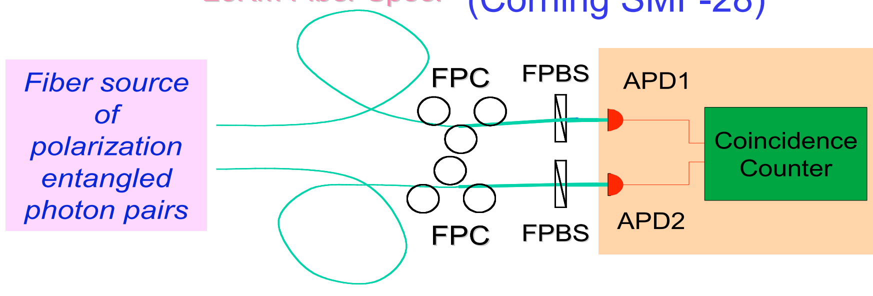
V=80%



$\theta_1 \approx \theta_2 \approx$ +/– 45°, scanning ϕ_p

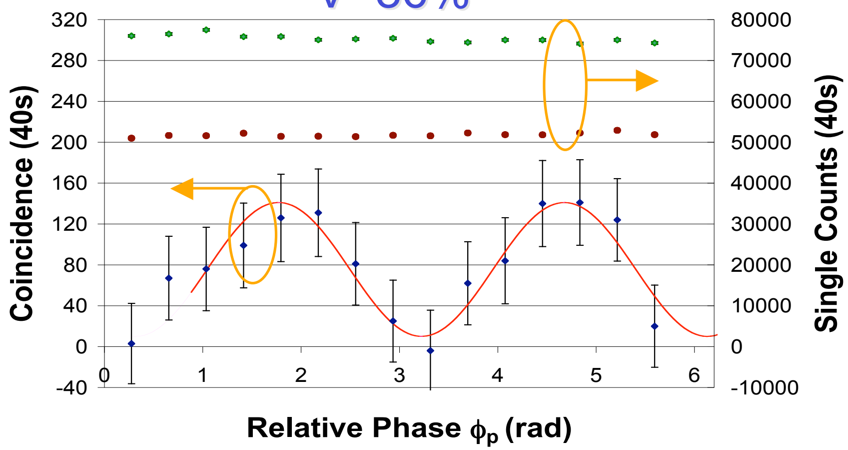
- Pump power in each polarization: 0.55mW average
- Average production rate of correlated photon pairs: about 0.1 pairs/pulse

25Km Fiber Spool (Corning SMF-28)



25Km Fiber Spool

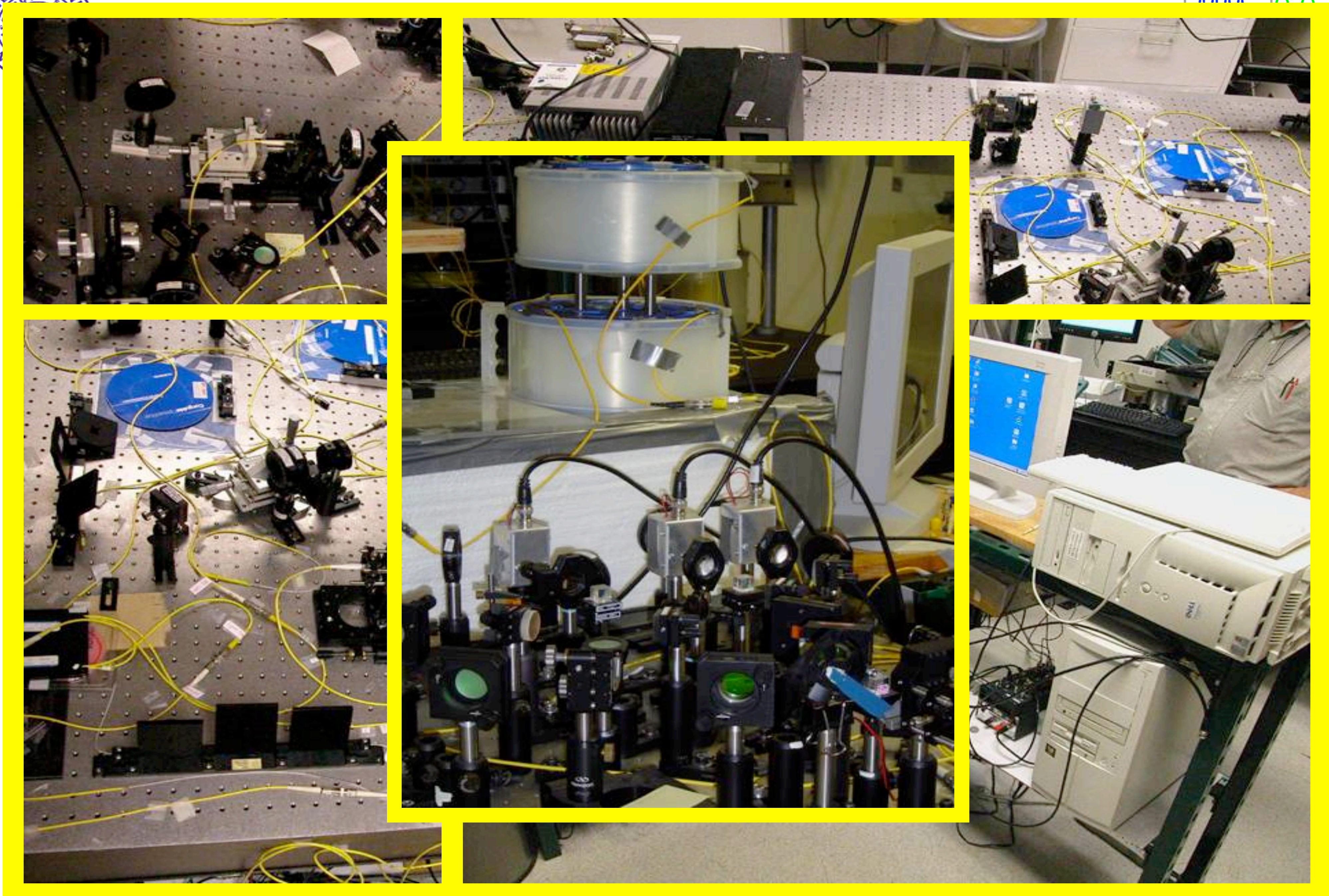
V=86%

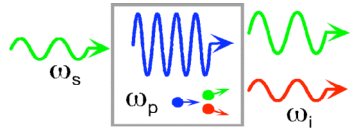


$\theta_1 \approx \theta_2 \approx$ +/– 45°, scanning ϕ_p

- Pump power in each polarization: 0.78mW average
- Average production rate of correlated photon pairs: 0.15pairs/pulse

X. Li, P. L. Voss, J. Chen, J. E. Sharping, and P. Kumar, Optics Letters **30**, 1201 (2005).

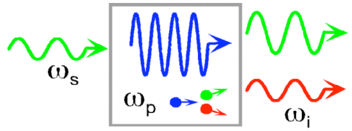




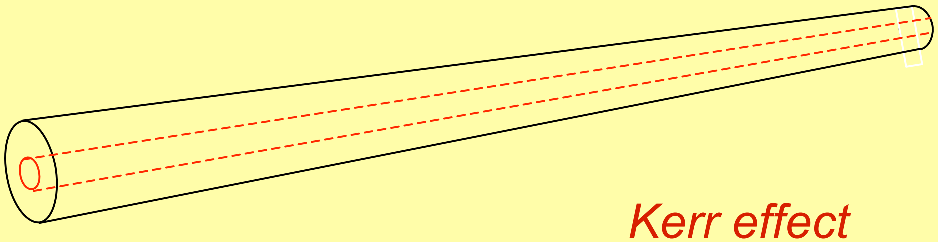
What is the cause and nature of the observed background photons?

Evidence from the excess noise figure of fiber-optical parametric amplifiers being developed for telecom systems suggests the reason to be the Raman effect.

Nonlinear Optics in Fiber



Glass as a c(3) Medium



Kerr effect

- Small core → high intensity
- Large interaction length
- Excellent mode matching
- Low loss for some λ's
- Doping is possible
- Dispersion
- Relatively small $\chi^{(3)}$

$$\frac{\partial A_p}{\partial z} + \frac{\alpha}{2}A_p + i\frac{\beta_2}{2}\frac{\partial^2 A_p}{\partial T^2} = i\gamma(|A_p|^2 A_p)$$

(Pump SPM: $i\gamma(|A_p|^2 A_p)$)

$$\frac{\partial A_{s(i)}}{\partial z} + \frac{\alpha}{2}A_{s(i)} + d\frac{\partial A_{s(i)}}{\partial T} + i\frac{\beta_2}{2}\frac{\partial^2 A_{s(i)}}{\partial T^2} = i\gamma\left[|A_p|^2 A_{s(i)} + A_p^2 A_{i(s)} * \exp(i\Delta k z)\right]$$

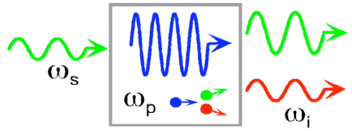
(XPM: $|A_p|^2 A_{s(i)}$; Four-Wave Mixing: $A_p^2 A_{i(s)} * \exp(i\Delta k z)$)

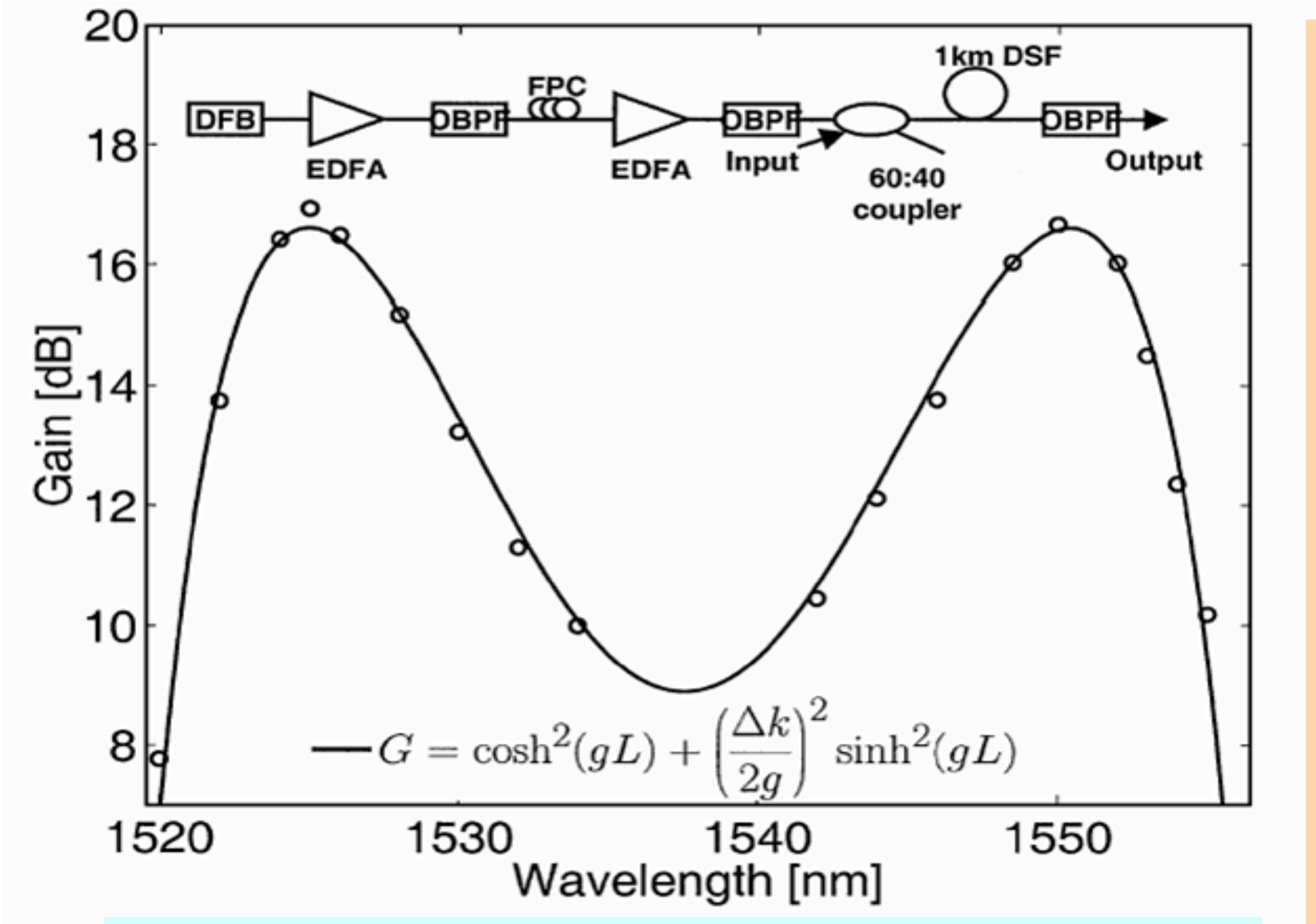
$$2\omega_p = \omega_s + \omega_i \qquad \Delta k = 2k_p - k_s - k_i \qquad \gamma = \frac{n_2\omega_p}{A_{eff}c}$$

Phase Matching: $\Delta k = 2k_p - k_s - k_i$

Nonlinear Coefficient: $\gamma = \frac{n_2\omega_p}{A_{eff}c}$

Fiber Optical Parametric Amplifier (FOPA): An Example of a PIA



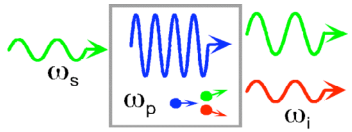


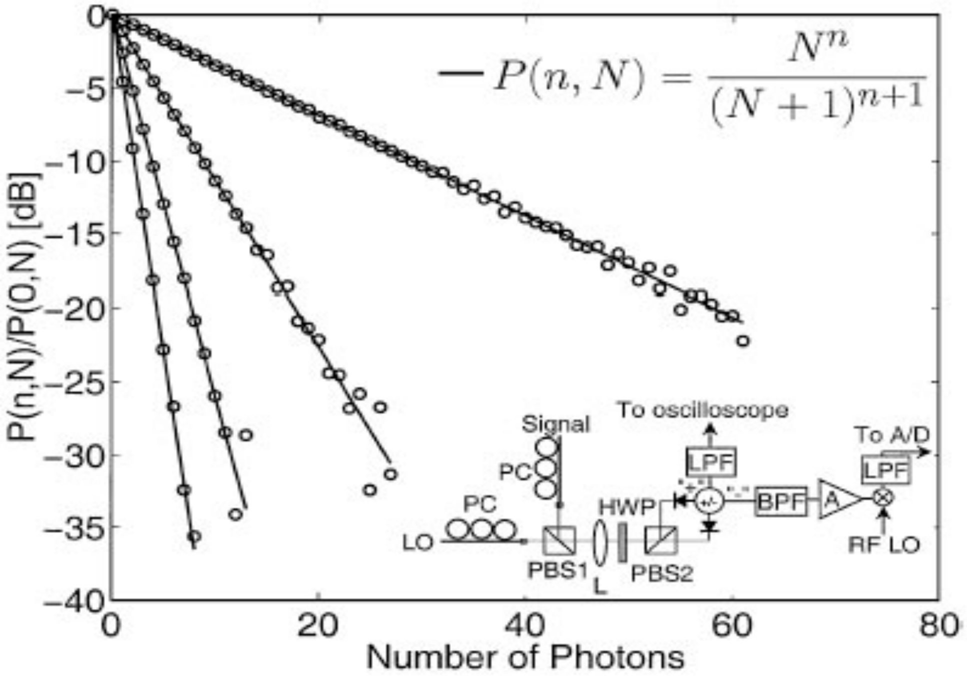
$$g = \sqrt{\left[(\gamma P_p)^2 - \left(\frac{\delta k}{2}\right)^2\right]}$$

$$\delta k = 2\gamma P_p + (k_s + k_i - 2k_p) \approx 2\gamma P_p + \beta_2(\omega_s - \omega_p)^2$$

- 1 km linear FOPA configuration
- Gain as high as 20 dB
- 1537.5 nm pump
- 1.3 W pump peak power
- 700 ns pump pulses
- 8 kHz pump pulse rate
- CW signal

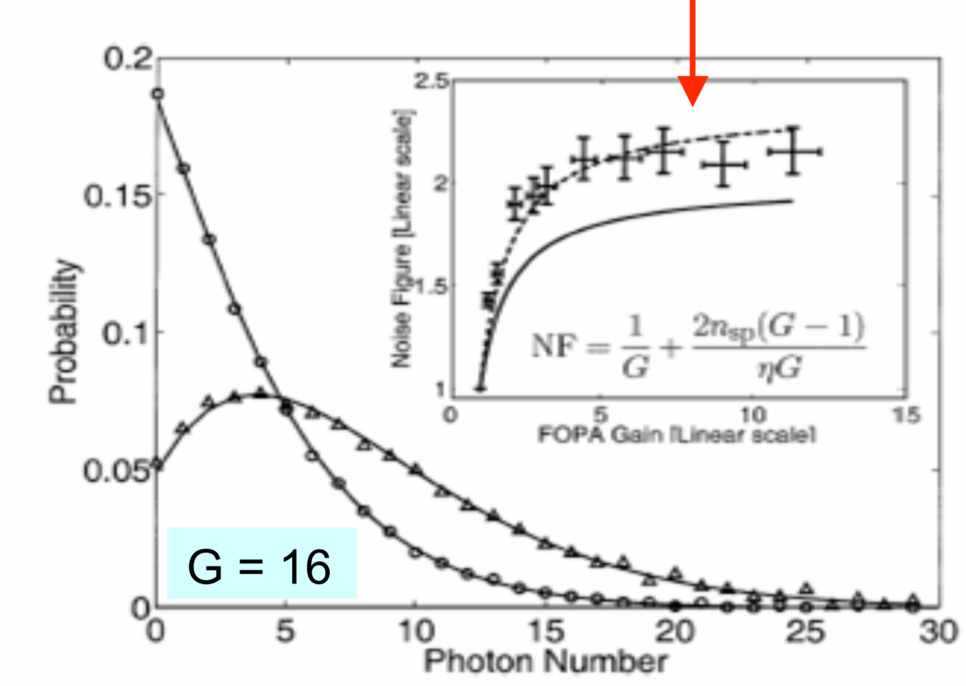
Measurement of the Photon Statistics and Noise Figure of a Fiber PIA





P. L. Voss, R. Tang, and P. Kumar, *Optics Letters*, Vol. 28, 2003, pp. 549.

Some excess noise is found on the amplified signal.

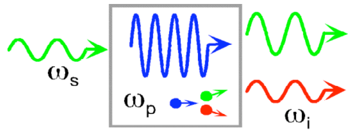


$$\hat{i}(\Omega) \propto \hat{X}(\psi) = \hat{X}\cos(\psi) + \hat{Y}\sin(\psi)$$

$$\hat{E} = \hat{X} + i\hat{Y} = \frac{e^{i\psi}\hat{E}(-\Omega) + e^{-i\psi}\hat{E}(\Omega)}{\sqrt{2}}$$

No fitting parameters are used.

NF Limit Due to Raman Effect



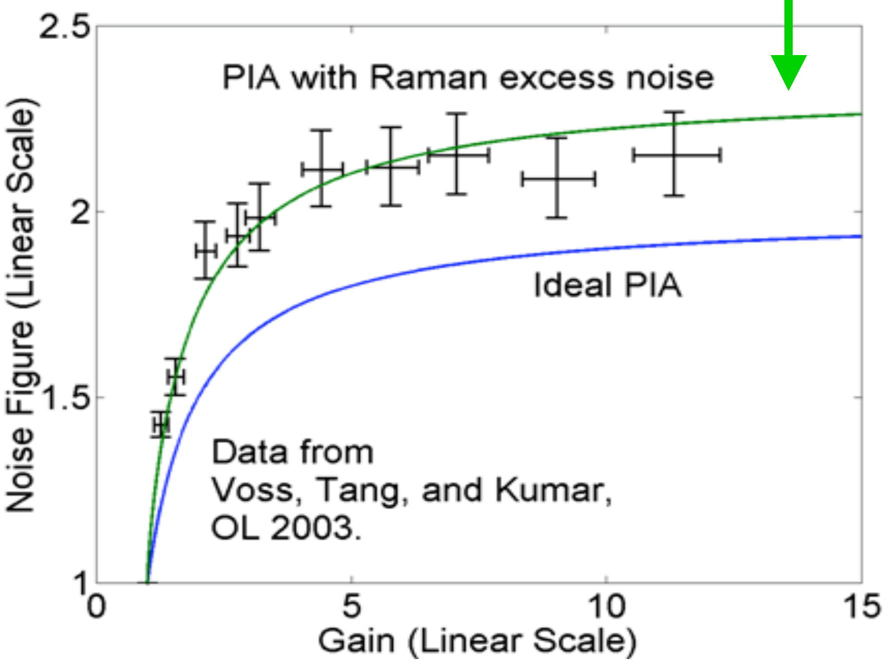
Voss and Kumar, "Raman-noise induced noise-figure limit for $\chi^{(3)}$ parametric amplifiers," *Optics Letters*, Vol. 29, 2004, pp. 445–447.

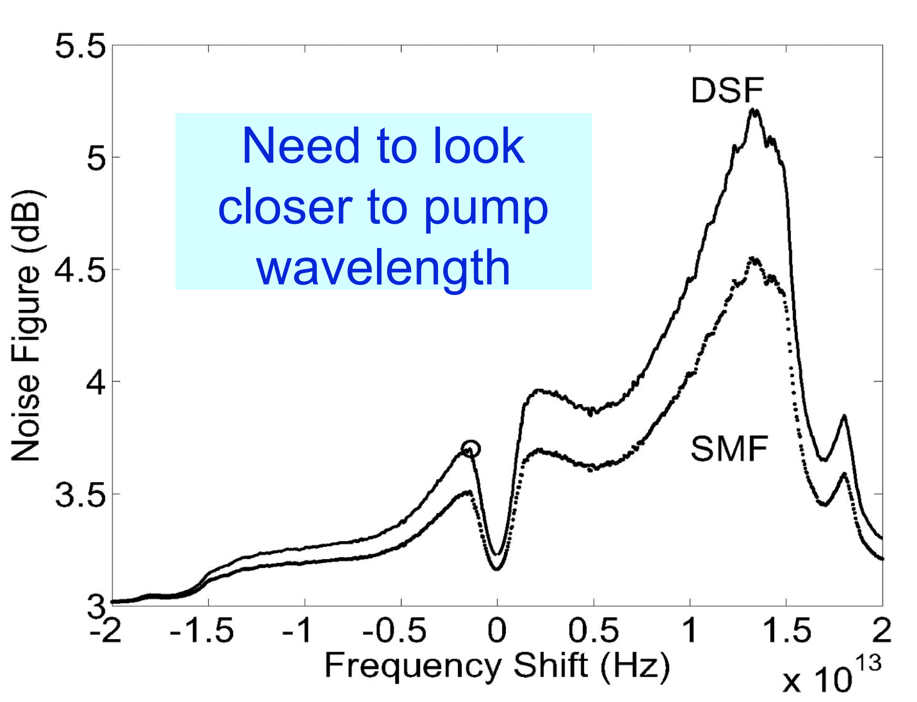
- Addition of Raman noise can be treated analytically

$$\hat{a}_s(z) = \mu_s(z)\,\hat{a}_s(0) + \nu_s(z)\,\hat{a}_a^\dagger + c_{s1}(z)\,\hat{t}_1^\dagger$$
$$\hat{a}_a(z) = \mu_a(z)\,\hat{a}_a(0) + \nu_a(z)\,\hat{a}_s^\dagger + c_{a1}(z)\,\hat{t}_1 + c_{a2}(z)\,\hat{t}_2$$

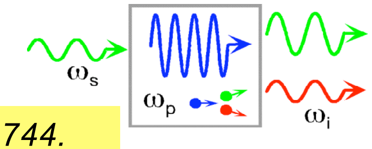
Excess noise terms due to Raman effect

- **Matches PIA noise figure data with no fitting parameters**



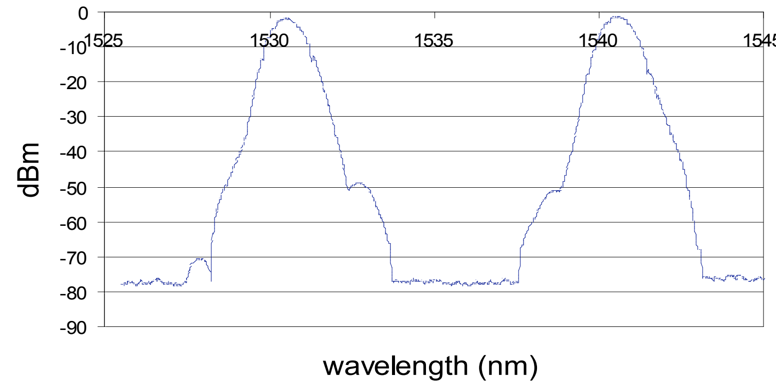


Correlated Photon Pairs with Low Background

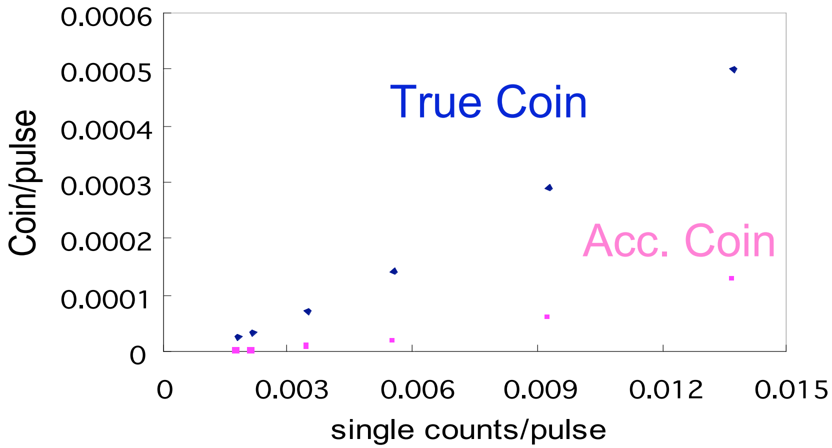


X. Li, J. Chen, P. L. Voss, J. E. Sharping, & PK, Optics Express, Vol. 12, No. 16, 2004, pp. 3737–3744.

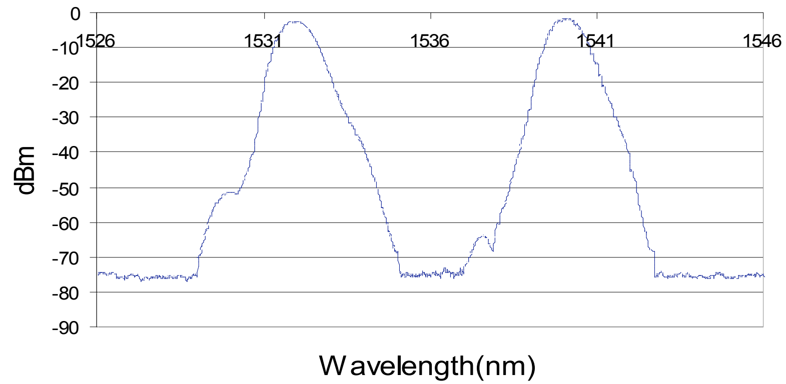
λ_p = 1535.5nm, λ_s = 1530.5nm, λ_i = 1540.5nm



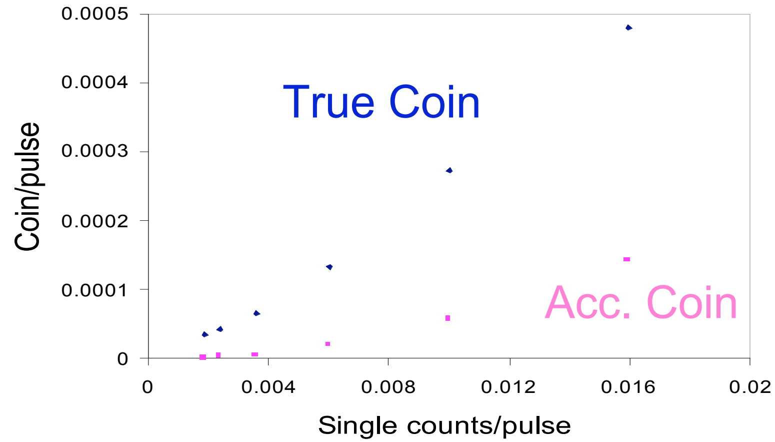
Spectrum of double grating filter



λ_p = 1536nm, λ_s = 1532, λ_i = 1540nm



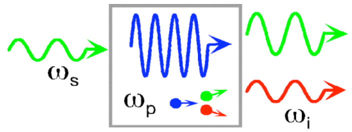
Spectrum of double grating filter



Spontaneous Raman scattering is suppressed

$$\frac{Coin_{True}}{Coin_{Acc}} > 10$$

Raman Photons vs. Temperature



Stokes → n+1

Anti-Stokes → n

Bose Population Factor:

$$n = \frac{1}{\exp\left(\frac{h\,\Delta\nu}{kT}\right) - 1}$$

$$\Delta\nu = \frac{C}{\lambda^2}\Delta\lambda \quad : \Delta\lambda = 4.8 \text{ nm}$$

At T =300 K (room);

S → 10.8

AS → 9.8

At T =195 K (dry-ice);

S → 7.2

AS → 6.2

At T =77 K (LN_2);

S → 3.16

AS → 2.16

Raman Photon Reduced Factor(RF) compared to 300 K: →

$$S_{RF}(195K) = \frac{10.8}{7.2} = 1.5$$

$$AS_{RF}(195K) = \frac{9.8}{6.2} = 1.6$$

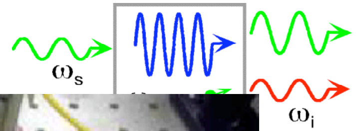
$$S_{RF}(77K) = \frac{10.8}{3.6} = 3.0$$

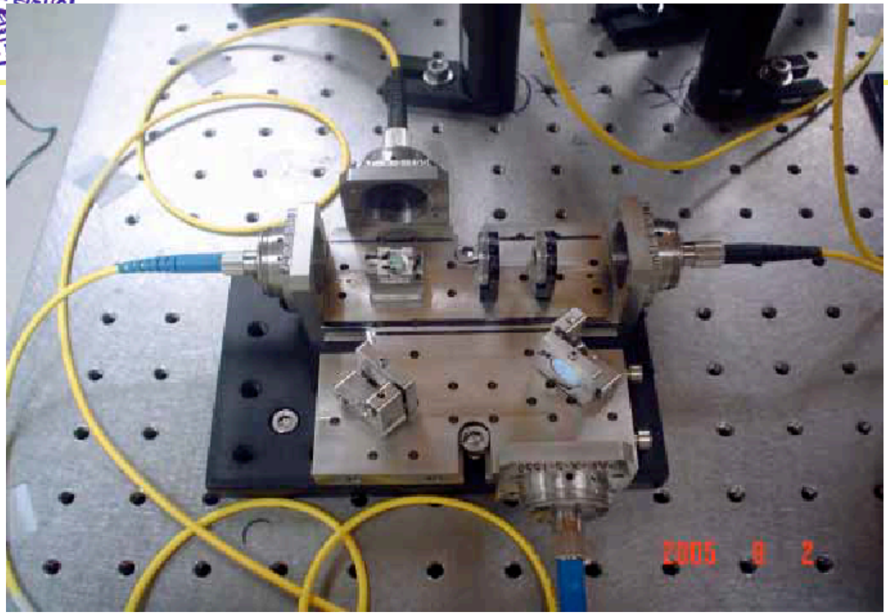
$$AS_{RF}(77K) = \frac{9.8}{2.16} = 4.5$$

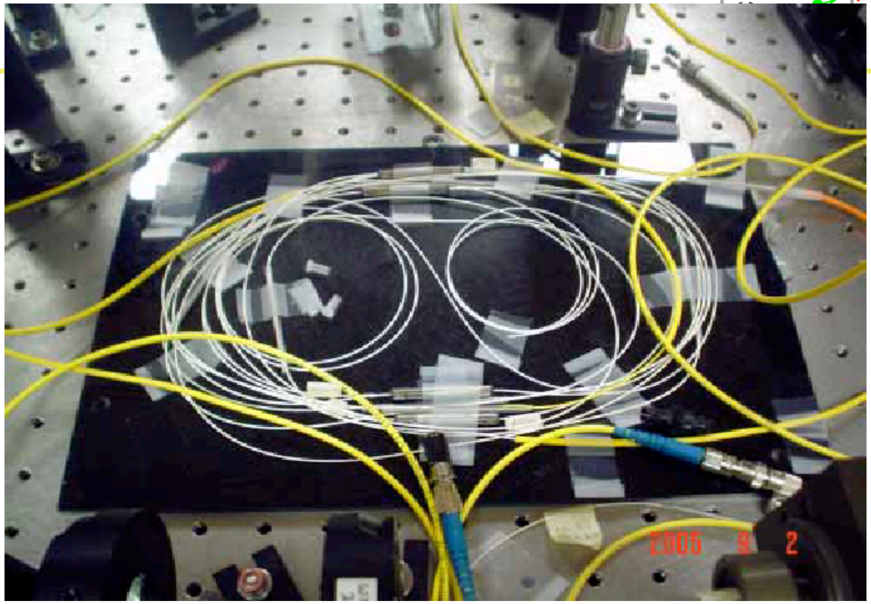
Ratio (300 K) = 28/1

Ratio (195 K) = 28/(1 /1.6) = 48.

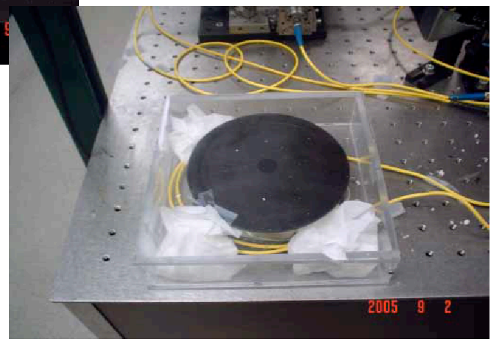
Ratio (195 K) = 28/(1/4.0) = 112.


ωs
ωi

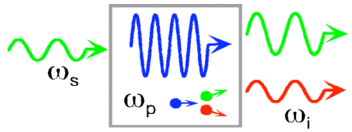

2005 9 2


2005 9 2

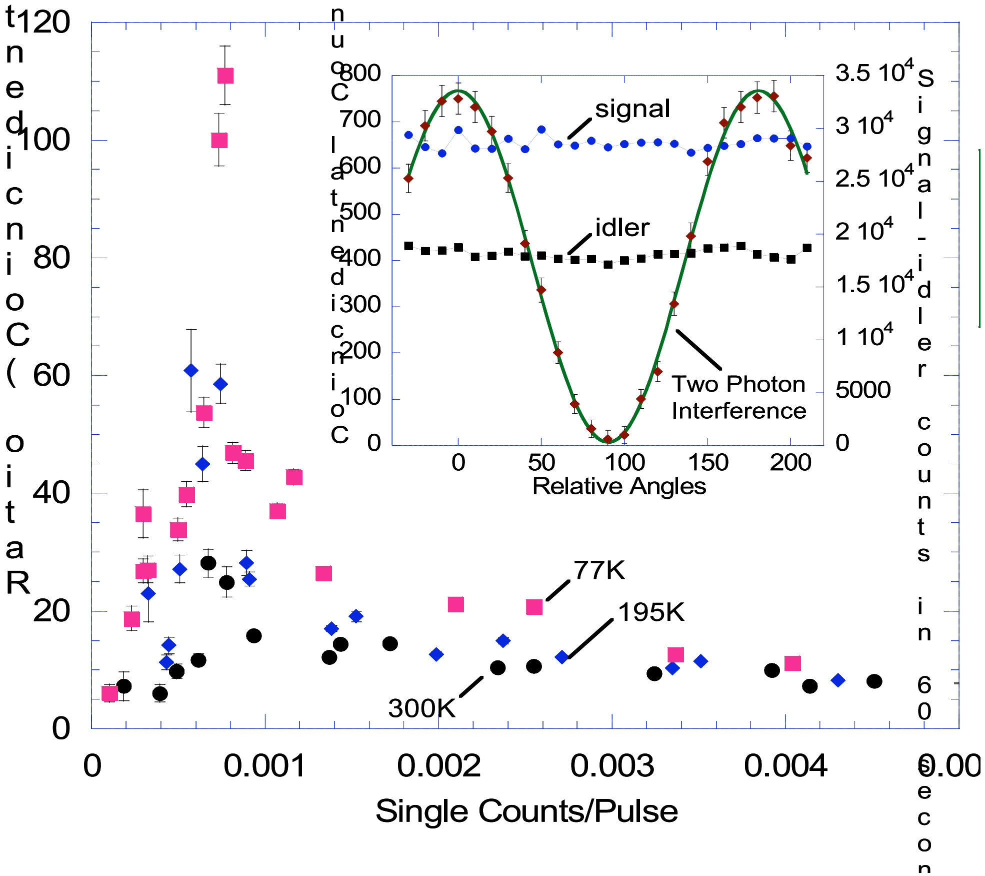

2005 9 2

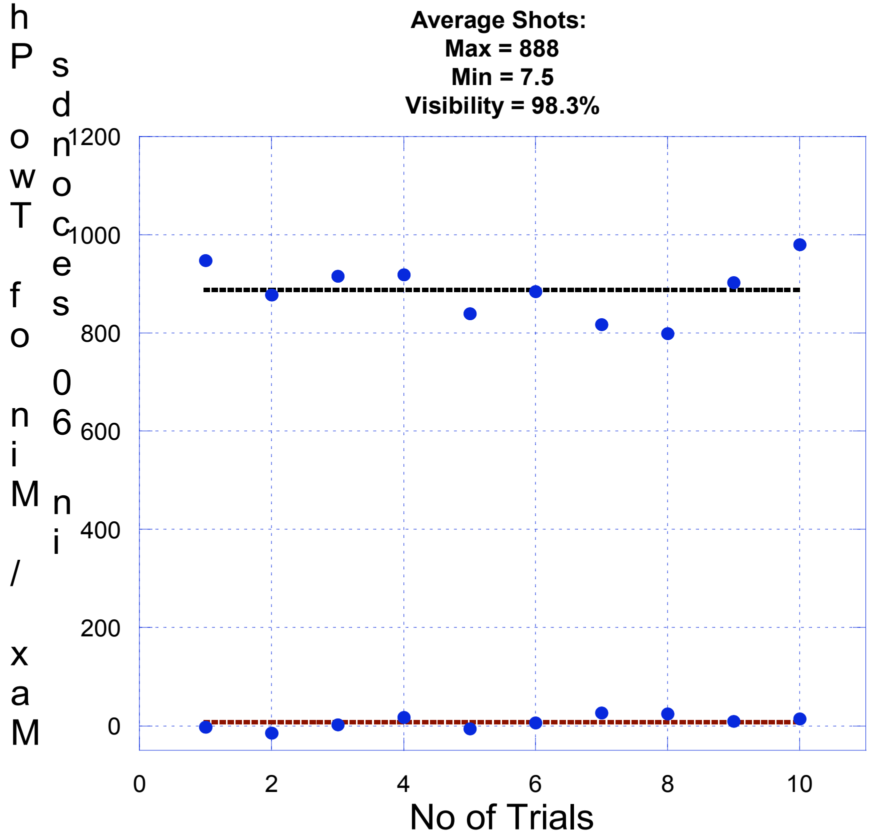

2005 9 2

Observation of High Purity Entanglement



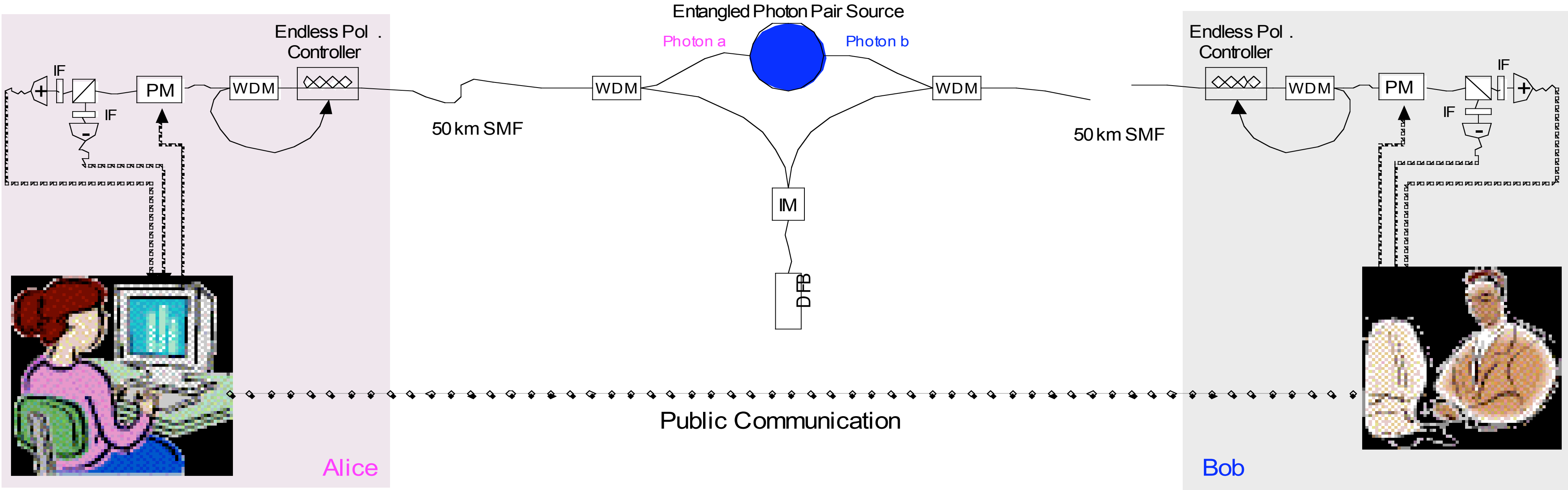
Average visibility > 98%; meets the ARDA roadmap criteria





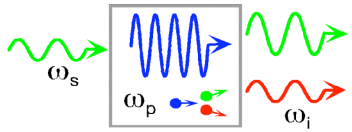
Presented as a postdeadline paper to FiO'2005, Tucson, AZ

System Under Development at NU



- The telecom band (around 1550 nm) polarization entangled photon pair source delivers photon *a* to Alice and photon *b* to Bob.
- The auxiliary DFB laser light is chopped into pulses which do not overlap with photon *a* and photon *b* in time. Its wavelength is several nm away from photons *a* and *b*.
- The commercially available endless polarization controllers compensate the polarization fluctuations by monitoring the polarization state of the auxiliary light.
- Alice and Bob's polarization modulators (their principle axis are 45° to the system's principle axis) apply the modulation according to randomly chosen measurement bases.

Data Encryption with the BB84 / Ekert Protocols



- Protocols allow two parties to remotely agree on a string of binary random numbers known only to each other (a cryptographic key)
- The parties use the key either with mathematical encryption algorithms such as 3DES or AES or with Vernam Cipher (one-time pad)
- Mathematical encryption algorithms are **not proven to be secure** and may have difficulty keeping up with the data rates on high-speed optical networks
- One-time pad is **proven** to be information theoretically secure on public channels, but it requires one key bit for every data bit → data rate = key generation rate

Best results to date: ~20km at ~1kbps → Rate-distance ~0.02Mbps-km

AlphaEta Direct Data Encryption Protocol

M **agreed-upon bases choices with**

$M >> \sqrt{n}$

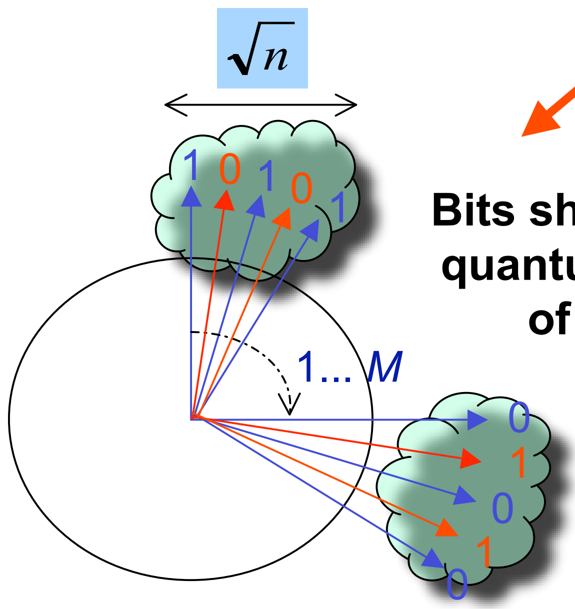
n **= number of photons per bit**

Alice and Bob use a short secret key

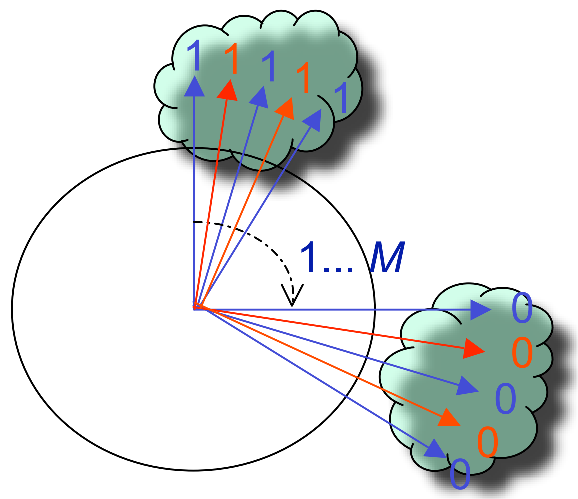
Alice ⟶ **Bob**

Irreducible Quantum noise protects data from Eve

Use of secret key unveils the shroud for Bob

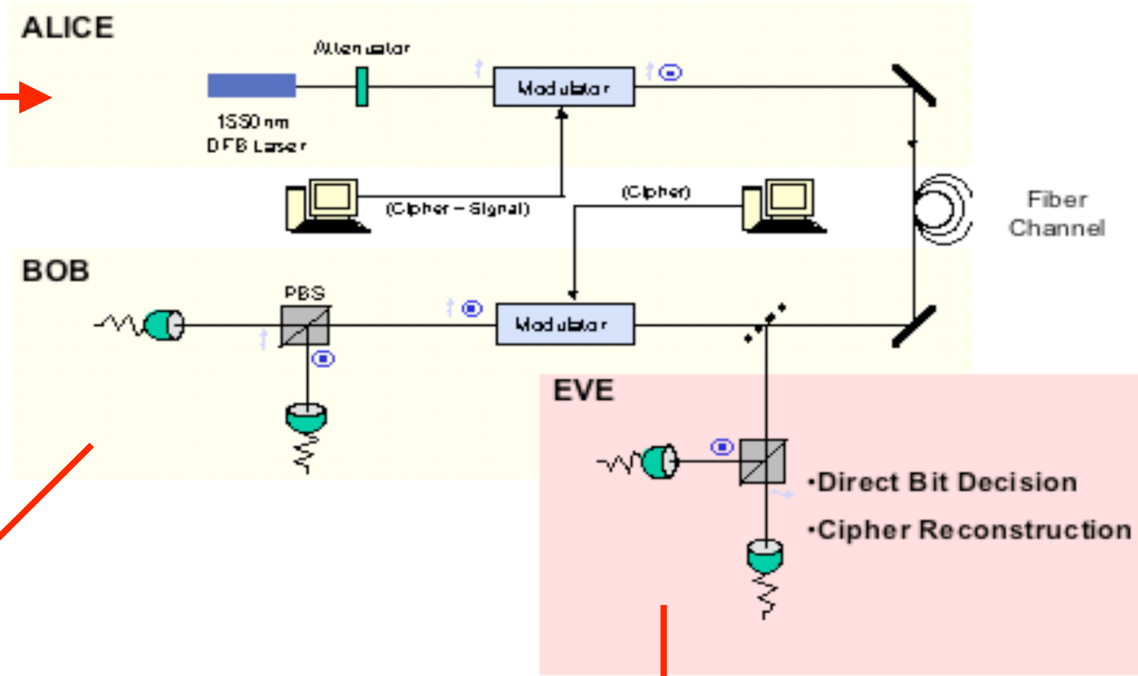


Bits shrouded in quantum-noise of light



Lab Demonstration of Difference Between Bob' s and Eve's Measurements

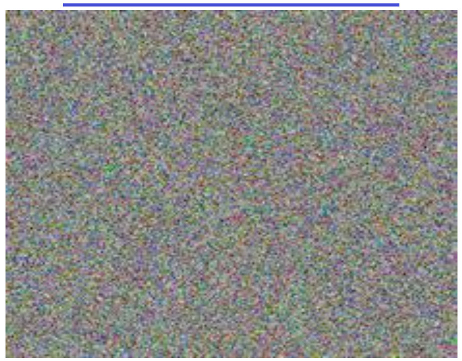
Original Data:



Alice to Bob:

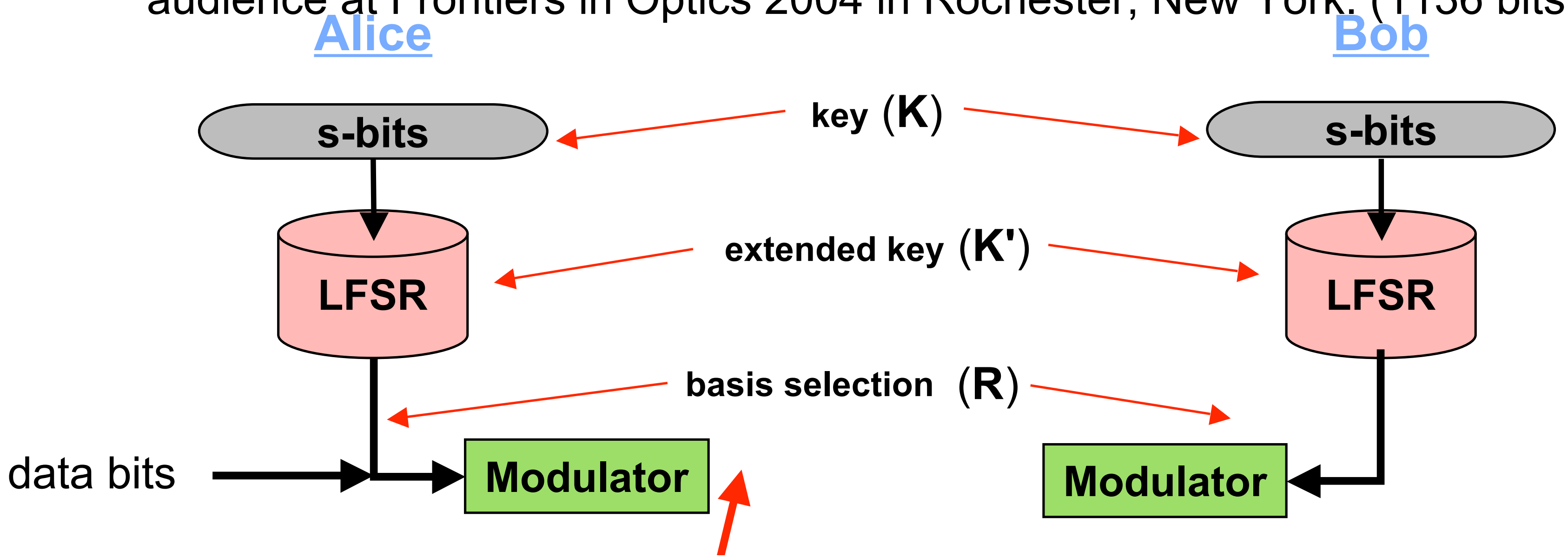
Alice to Eve:

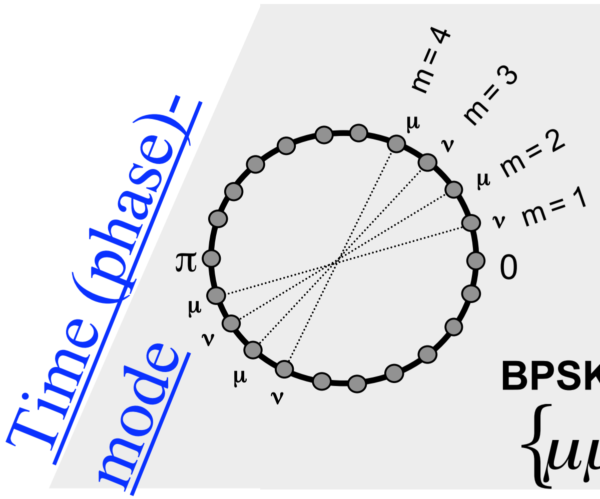
Eve with a random key



Quantum Data Encryption (QDE) Protocol

I want to thank the organizers for inviting me to speak before this distinguished audience at Frontiers in Optics 2004 in Rochester, New York. (1136 bits)





M bases (2M phase states), *m*:[0,M-1]

$$\left|\psi_m^{(\mu)}\right\rangle = \left|\alpha\, e^{i\theta_m}\right\rangle$$

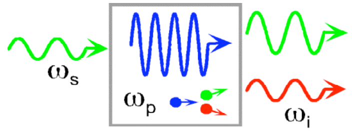
$$\left|\psi_m^{(\nu)}\right\rangle = \left|\alpha\, e^{i(\theta_m+\pi)}\right\rangle$$

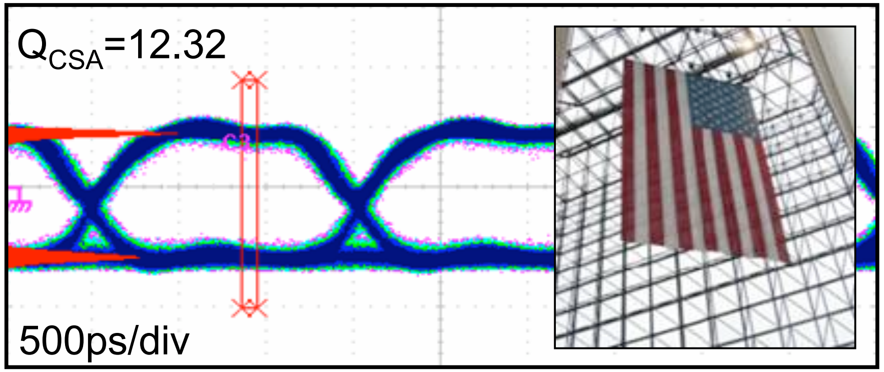
BPSK logical encoding:

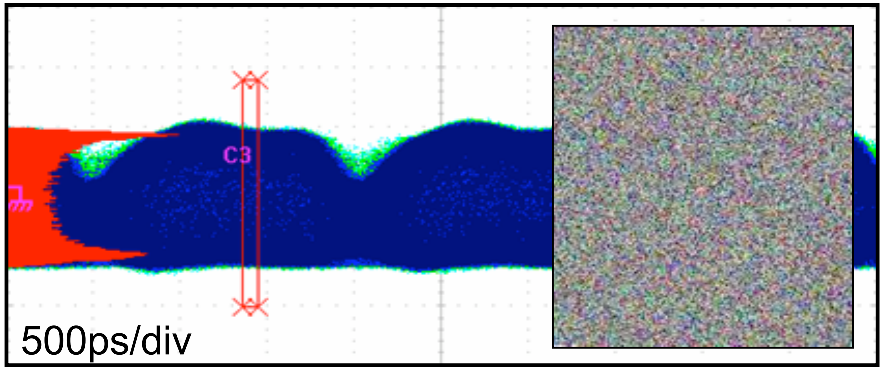
$$\{\mu\mu, \nu\nu\} \rightarrow L1 \quad \{\mu\nu, \nu\mu\} \rightarrow L0$$

E. Corndorf, G. Barbosa, C, Liang, H. Yuen, and P. Kumar, *Optics Letters* 28, 2040 (2003); CLEO'04 postdeadline paper.

Bob's and Eve's Eye Patterns, 200km







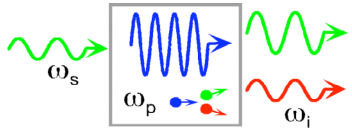
- 200km in-line amplified line
- 650Mbps data rate
- 2^{15}-bit PRBS
- M = 2,047
- -25dBm (~40,000 ph/bit) at launch

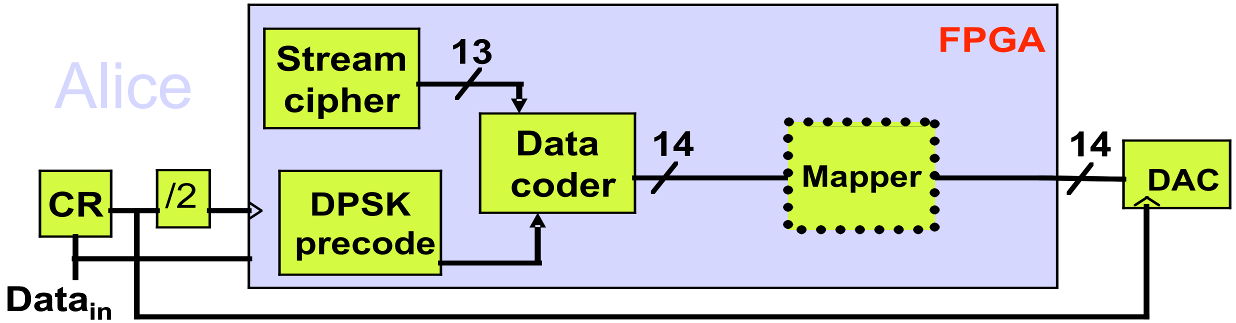
E. Corndorf, G. Kanter, C. Liang, and P. Kumar, CLEO'04 postdeadline paper; to appear in PTL.

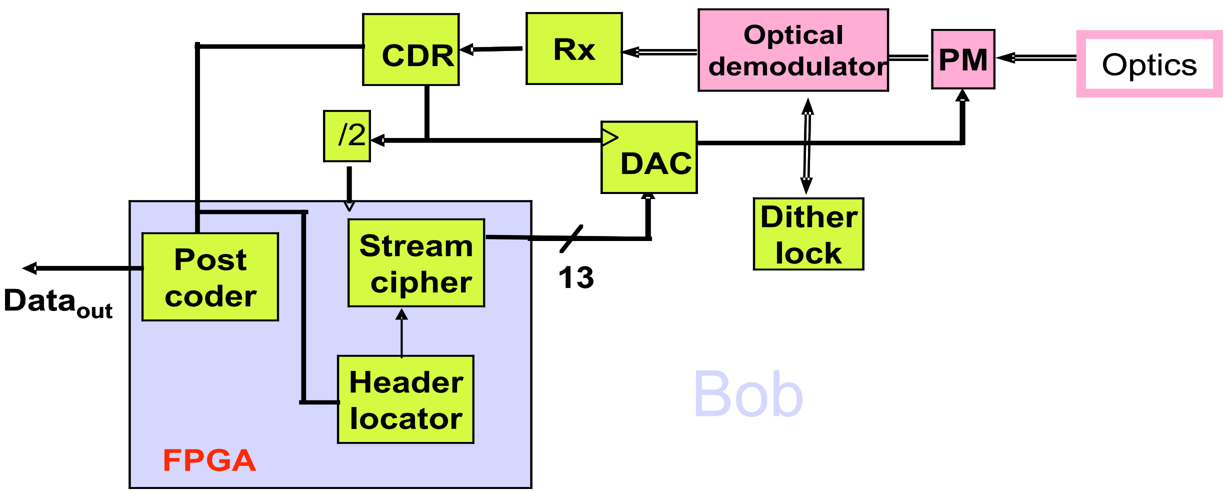
- Eve located at source (Alice)
- Simulated by Bob with incorrect secret key
- Eve's PDF is uniform

- *Bursty*, not streaming!
- No clock recovery, common clock!

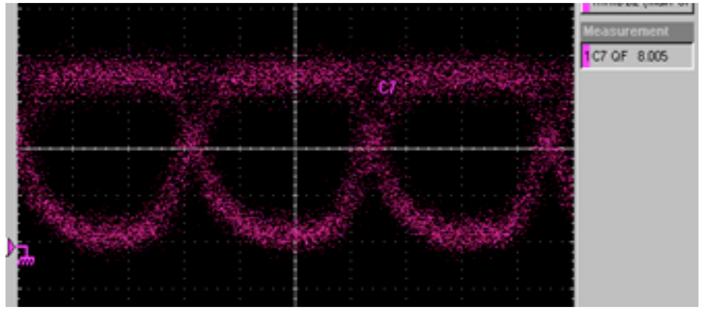
622 Mbps Streaming System



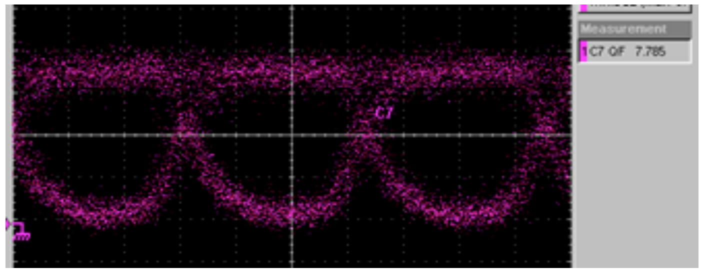




Bob's Eye: DPSK data without encryption

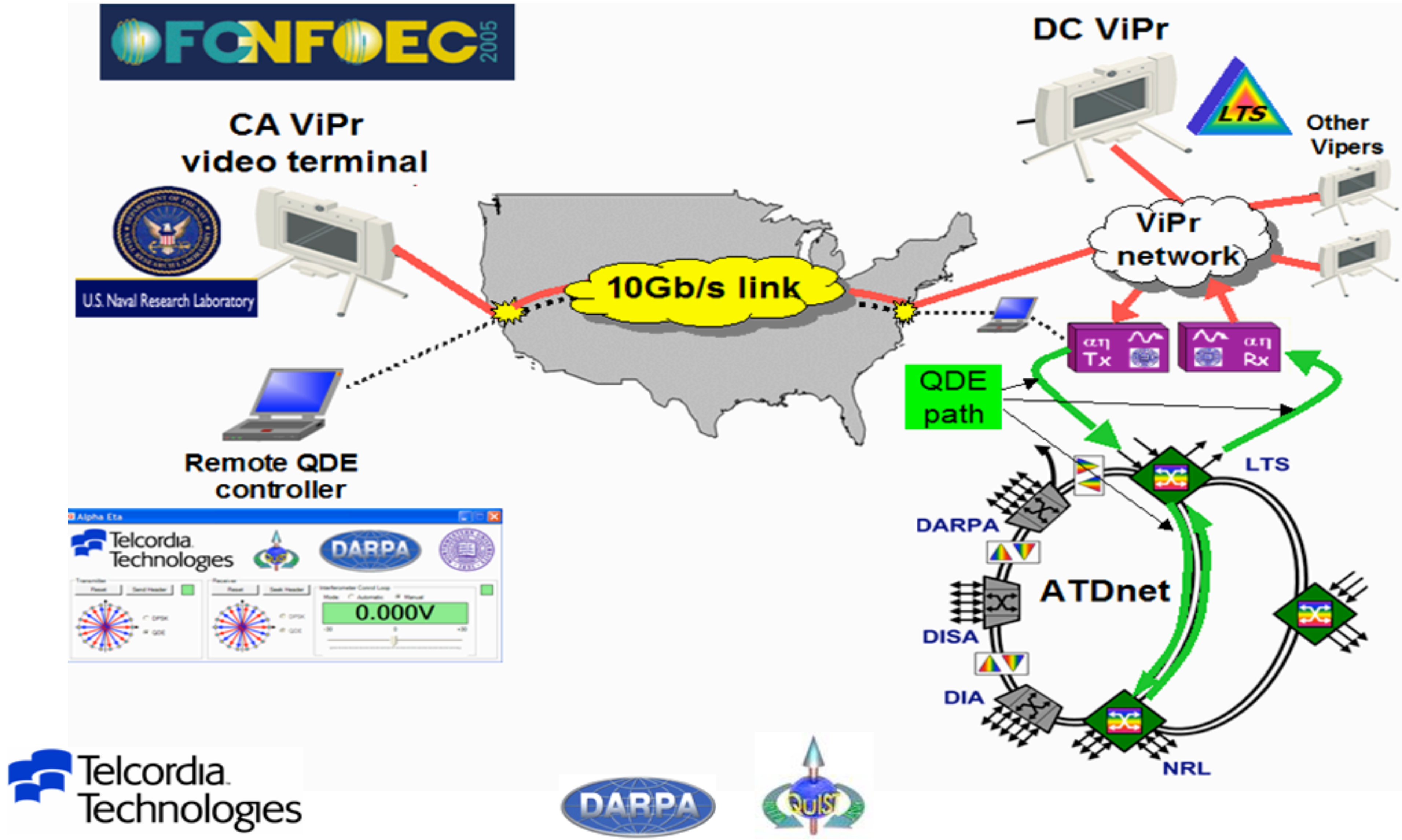


Bob's Eye: DPSK data with encryption & decryption with recovered clock

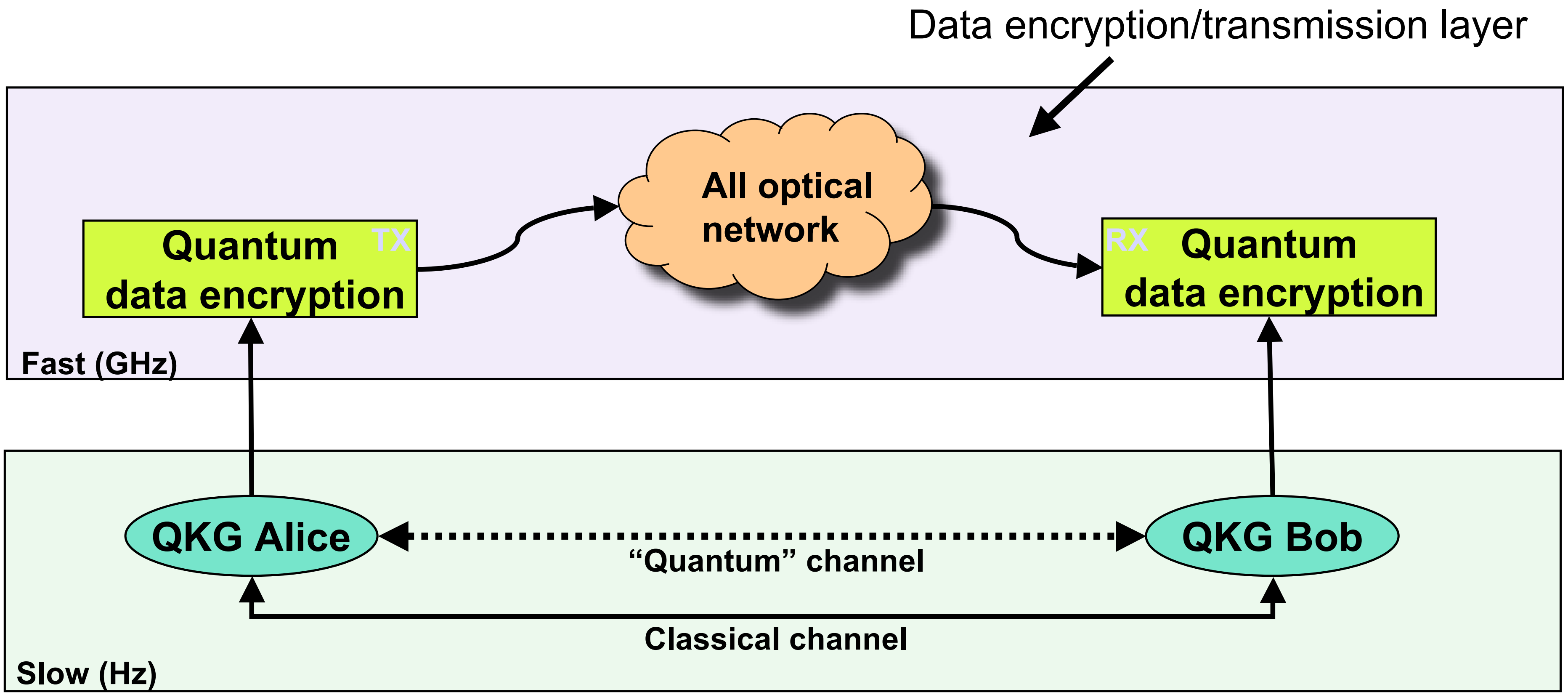


Only 0.2dB encryption penalty

Quantum Data Encryption over ATDnet in Washington, DC



Physical Layer Security over WANs



Key server layer:

- With proposed satellite up-down link
- Potentially 100-200 km apart with KCQ or fiber generated entanglement (recent NU work) using BB84 type protocols