Does QKD fit to the WDM world?

Misha Brodsky[1]

Jungmi Oh [1], *Cristian Antonelli*[1]

1: AT&T Labs, 2: University of L'Aquila

Quantum Information Technology Workshop, WS9
ECOC 2009

1

One-time pad or Vernam Cipher

UNITED STATES PATENT OFFICE.

GILBERT S. VERNAM, OF BROOKLYN, NEW YORK, ASSIGNOR TO AMERICAN TELEPHONE AND TELEGRAPH COMPANY, A CORPORATION OF NEW YORK.

SECRET SIGNALING SYSTEM.

1,310,719. Specification of Letters Patent. Patented July 22, 1919.

Application filed September 13, 1918. Serial No. 253,962.

2

Need for Quantum Networks

Why QKD has not yet been widely adopted?
- Solution to important but *NOT* the most important issue
- 100% security is *NOT* needed
- PtP ➔ scales as N^2 for N users
- Limited reach

Suggestions
- Focus on different application: key management?
- Reconfigurable multi-user networks: entanglement?

Example
Central station creates entangled pairs (C-band wide) and distributes them to end-users

Brodsky and Feuer
US Patent Applications 12/008,952; 12/008,926

3

Wavelength Selective Switch

WSS: 1 input → 2,4,8 output device
incoming spectrum → WDM channels
distributes WDM channels to its output fibers

Commercially available, being widely deployed

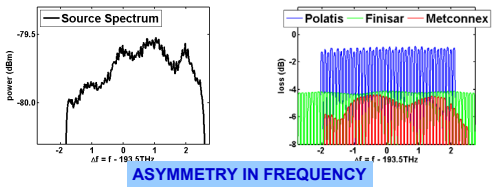
Key players: Polatis, Finisar, Capella, JDSU etc

Which one is good for your network?

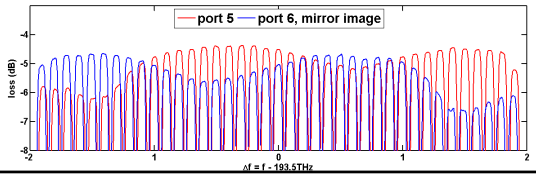
4

Potential Issues

WAVELENGTH DEPENDENT SPECTRA AND LOSS



ASYMMETRY IN FREQUENCY



5

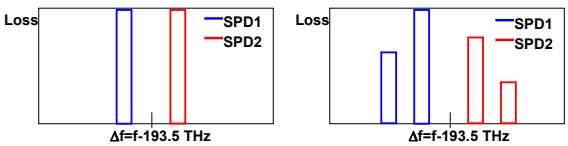
Criteria - Coincidence Rates

Useful for QKD system designer/operator, but calculations could be tricky

$$P_{coin} \approx \mu \times \eta_1 \times \eta_2 \times t_1 \times t_2$$

μ, η_1, η_2 **not known, change → calibration needed**

t_1, t_2 **are poorly defined due to wavelength dependence**



6

Formal Treatment for Coincidence

Fraction of input spectrum $P(\omega)$ that reached detector through the filter:
Fraction of input spectrum $P(\omega)$ that contribute to coincidence:

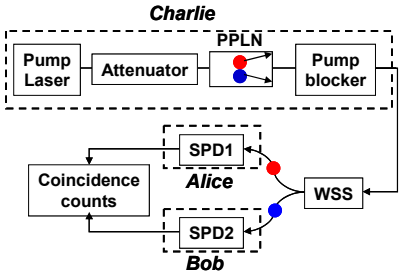
$$P_{1,2} = \int_0^\infty |H(\pm\omega)|^2 P(\omega) d\omega \qquad P_p = \int_0^\infty |H(\omega)|^2 |H(-\omega)|^2 P(\omega) d\omega$$

after some algebra …

$$P_{coin} = 1 - exp(-\mu \times P_1 \times t_1\eta_1) - exp(-\mu \times P_2 \times t_2\eta_2) + exp(-\mu \times (P_1 \times t_1\eta_1 + P_2 \times t_2\eta_2 - P_p \times t_1\eta_1 \times t_2\eta_2))$$

7

Setup

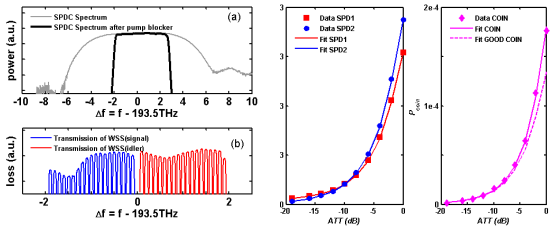


8

Test 1
In-situ system calibration (μ, η_1, η_2)

9

Counts and Coincidence



Simultaneous measurements of $P_{1,2}$ and P_{coin} ➔ μ, η_1, η_2.

Agrees well in independent measurements

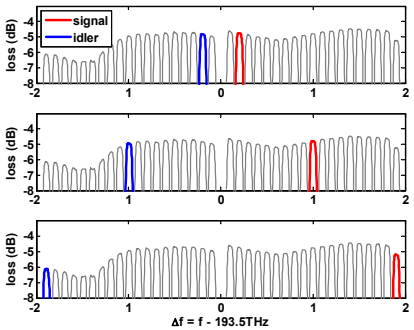
High power (multiple pairs)

10

Test 2
Coincidence across C-band

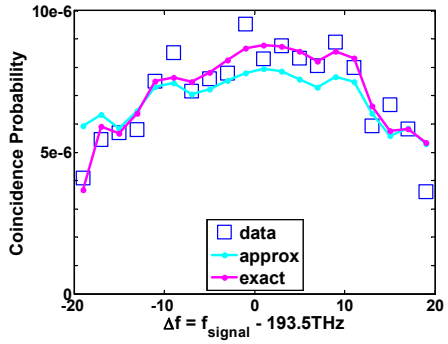
11

WSS Configurations



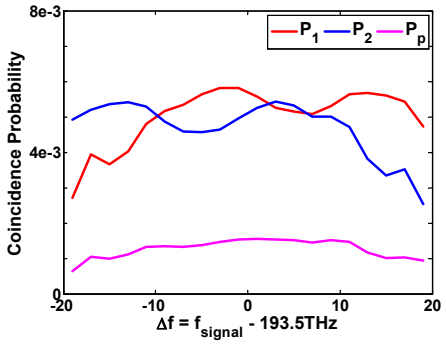
12

Coincidence



13

Integrals

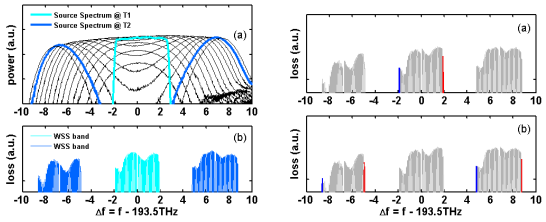


14

Test 3
Bandwidth provisioning
coincidence for S & L bands

15

Bandwidth Provisioning for Quantum Channels



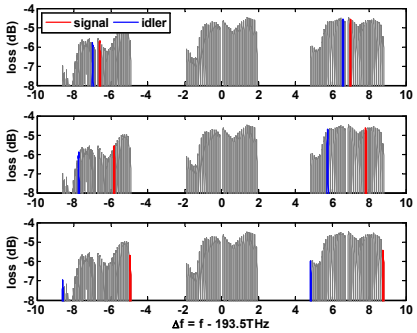
Why it is interesting?
To facilitate fiber sharing between strong telecom and weak QKD channels

Why it is possible?
Phase matching condition in PPLN determines the entangled pair spectrum

AWG transmission is quasi periodic in frequencies and spans several bands

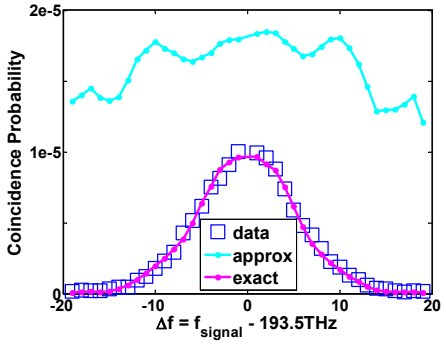
16

WSS Configurations



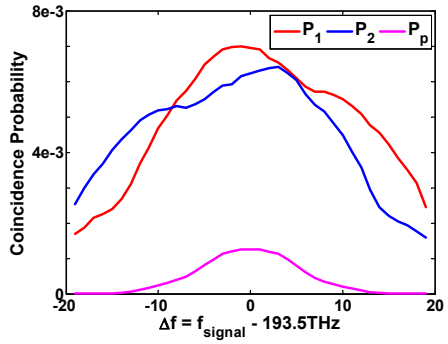
17

Coincidence



18

Integrals



19

Summary

Need for multi-user networking

Application of WSS

Coincidence rates based on photon statistics
- Formal expression
- In-situ system calibration (μ, η_1, η_2)
- Coincidence across C-band
- Bandwidth provisioning, coincidence for S & L bands

Thank you !

20