High-Speed Quantum Key Distribution Using Integrated Photonics

Dirk Englund

Columbia University in the City of New York

QUANT2012

Institute for Pure and Applied Mathematics

Aug. 28

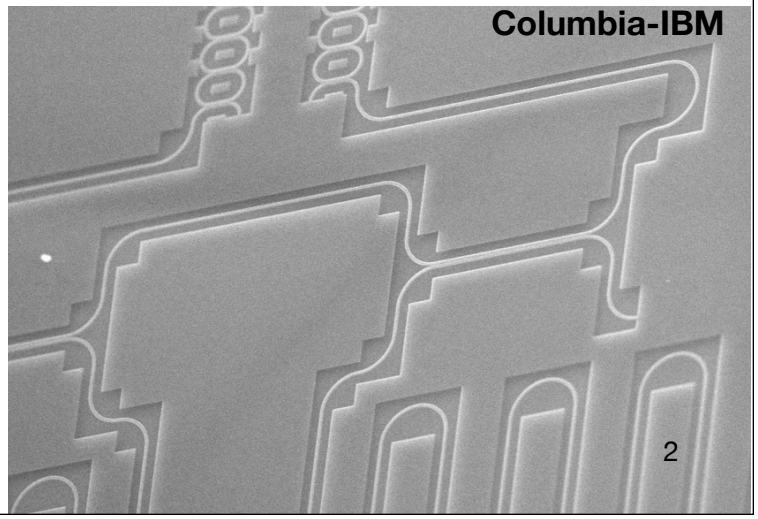
Major Collaborators:

- Solomon Assefa, IBM
- Jeffrey Shapiro, MIT
- Franco Wong, MIT

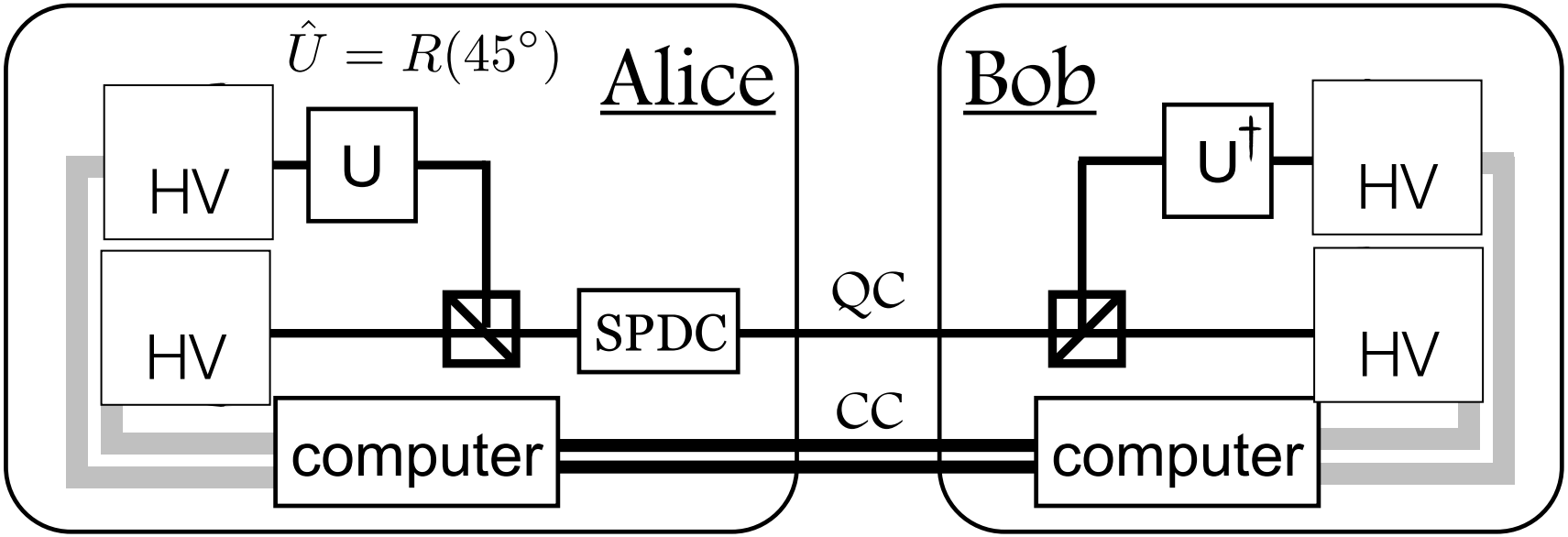
Outline

- **I. High-dimensional quantum key distribution using dispersive optics**
- Given a limited photon budget, can we improve key rate using high-dimensional Hilbert space of photons?
  - Can use many d.o.f., hyperentangled states (eg Kwiat group), ..
- Use spectral and temporal correlations to maximize secure key capacity
- Dispersive optics QKD: require only linear optics, including second-order dispersive elements, and only two single photon detectors for participants Alice and Bob

- **II. Quantum Silicon Photonics**
- Building quantum information processing systems in the silicon on insulator (SOI) platform
- Active control & electronics integration



Polarization-based QKD with entangled photons



Bennett, Brassard, Mermin, PRL 1992

$$|\Psi\rangle \propto |H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B \rightarrow {}_A\langle H|\Psi\rangle \propto |H\rangle_B$$
$${}_A\langle H|\hat{U}|\Psi\rangle = {}_A\langle D|\Psi\rangle \propto |D\rangle_B$$

P_{coinc}	Alice HV	Alice AD
Bob HV	1	1/d~0.5
Bob AD	1/d~0.5	1

Protocol:

1. Alice and Bob measure randomly in mutually unbiased bases (MUB)
2. They publicly compare bases for each photon (but not measurement results!)
3. They record results where they measure in the same basis.

QKD in fiber networks

•Polarization: $|\Psi\rangle \propto |H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B$

•d=2 Hilbert space
•Polarization modes aren't good eigenstates in fiber

•Time: $|\Psi\rangle \propto |t_1\rangle_A |t_1\rangle_B + |t_2\rangle_A |t_2\rangle_B$

•**Time & frequency - good eigenstates for fiber and free space**
•Telecom optimized to deal with frequency and time
•High-dimensional Hilbert space

$$|\Psi\rangle \propto |t_1\rangle_A |t_1\rangle_B + |t_2\rangle_A |t_2\rangle_B + |t_3\rangle_A |t_3\rangle_B + |t_4\rangle_A |t_4\rangle_B \cdots$$

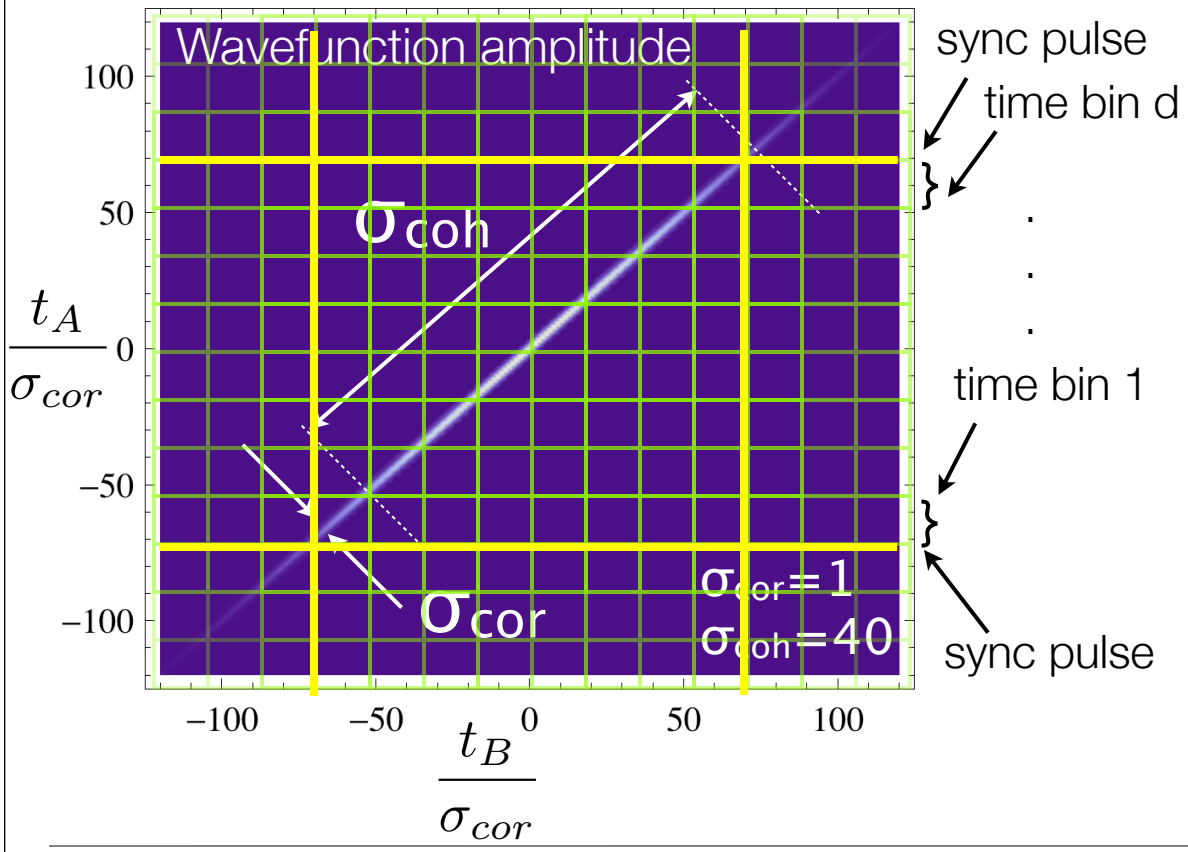
•Khan, Howell PRA 2006
•Khan, Broadbent, Howell PRL 2007
•Qi, Opt. Lett. 2006
•Bechmann-Pasquinucci *et al.,* PRA 2000
•Marcikic *et al.,* PRL 2004
•Mower *et al.,* arxiv 2011

Generating temporally entangled states

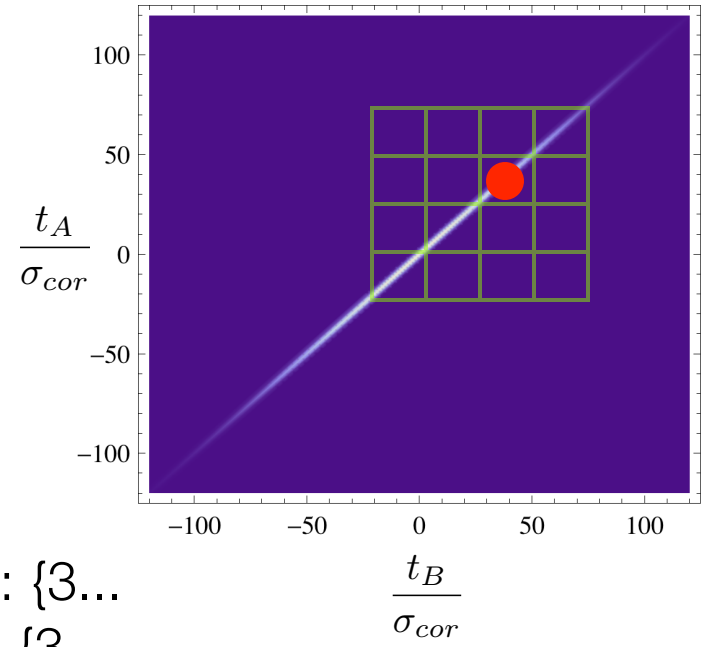
Spontaneous parametric down conversion (SPDC):

laser field → $\chi^{(2)}$ → entangled photon pairs

$$|\Psi\rangle = \int\int \exp\left[-\frac{(t_A - t_B)^2}{4\sigma_{cor}^2}\right] \exp\left[-\frac{(t_A + t_B)^2}{16\sigma_{coh}^2}\right] |t_A t_B\rangle \, dt_A t_B$$



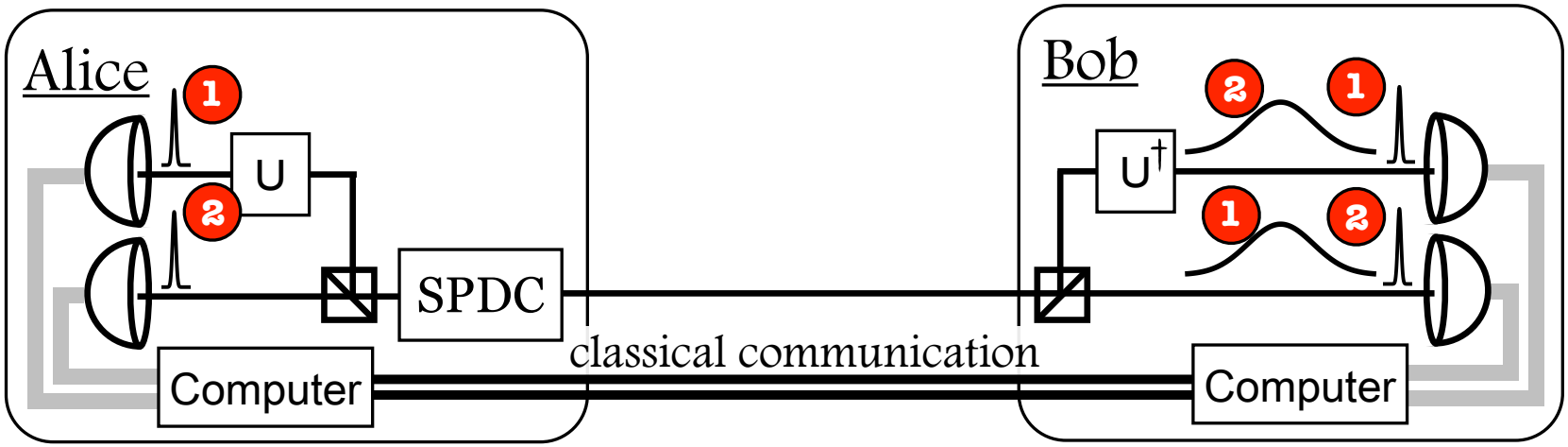
Building the key:



Alice: {3...

Bob: {3...

Mutually unbiased bases



- Requirements on unitary transformation U:

  Spread a time state over all time states in a frame/alphabet
  Preserve correlations if Alice and Bob both apply

$$|\langle T_{iA}T_{jB}|\,\Psi_{AB}\rangle|^2 = \delta_{ij}$$

$$|\langle T_{iA}T_{jB}|\,\hat{U}_A \otimes \hat{U}_B\,|\Psi_{AB}\rangle\,|^2 = \delta_{ij}$$

$$|\langle T_{iA}T_{jB}|\,\hat{I}_A \otimes \hat{U}_B\,|\Psi_{AB}\rangle|^2 = \frac{1}{d}$$

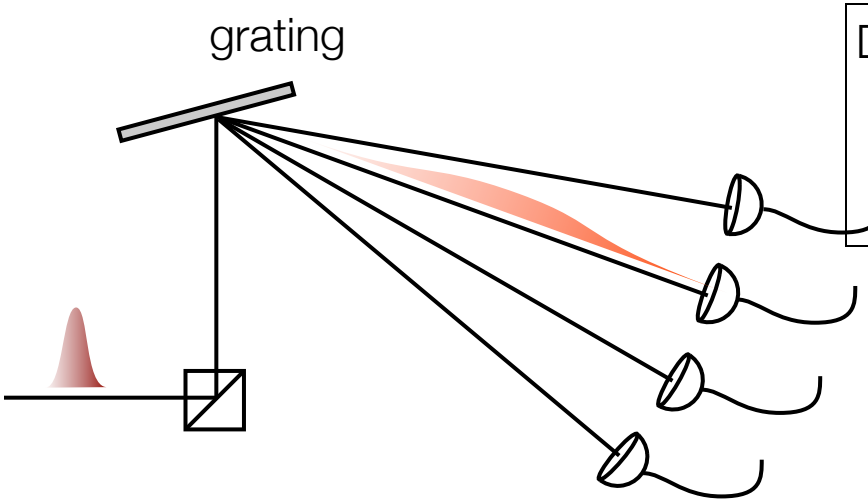
$$|\langle T_{iA}T_{jB}|\,\hat{U}_A \otimes \hat{I}_B\,|\Psi_{AB}\rangle|^2 = \frac{1}{d}$$

Creating the right transformation

Seek a conjugate basis:

$$|t_0\rangle \propto \int e^{it_0\omega}\,|\omega\rangle\,d\omega$$

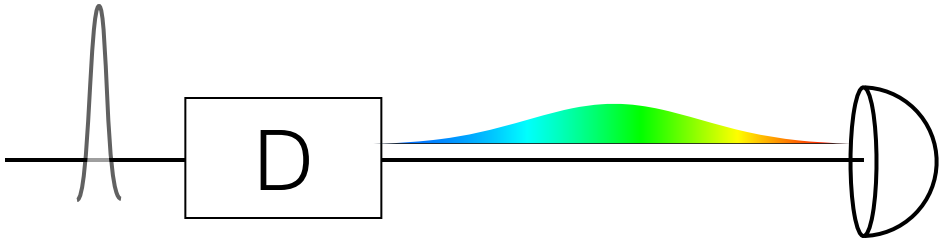
$$|\omega_0\rangle \propto \int e^{it\omega_0}\,|t\rangle\,dt$$



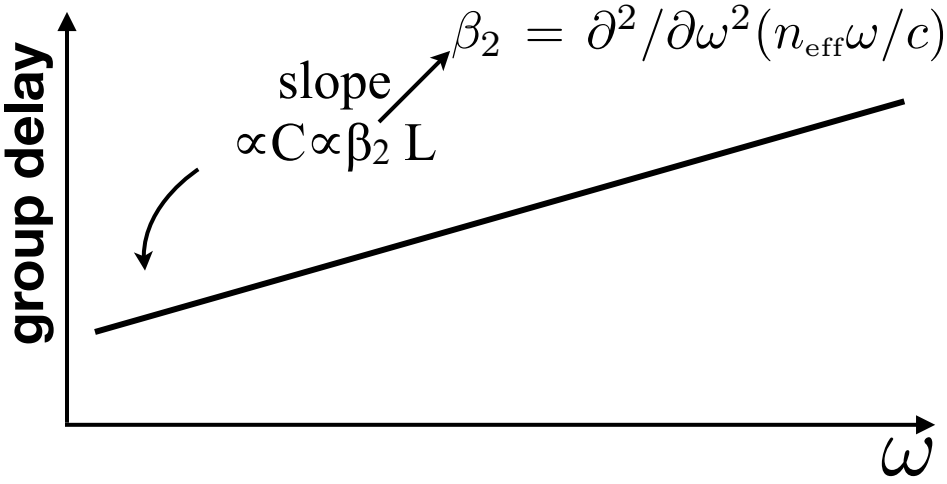
Drawbacks:
1. Cost
2. Noise (limits rate and transmission length)

- Qi, Opt. Lett. 2006
- Mower *et al.*, arxiv 2011

Second-order dispersion:



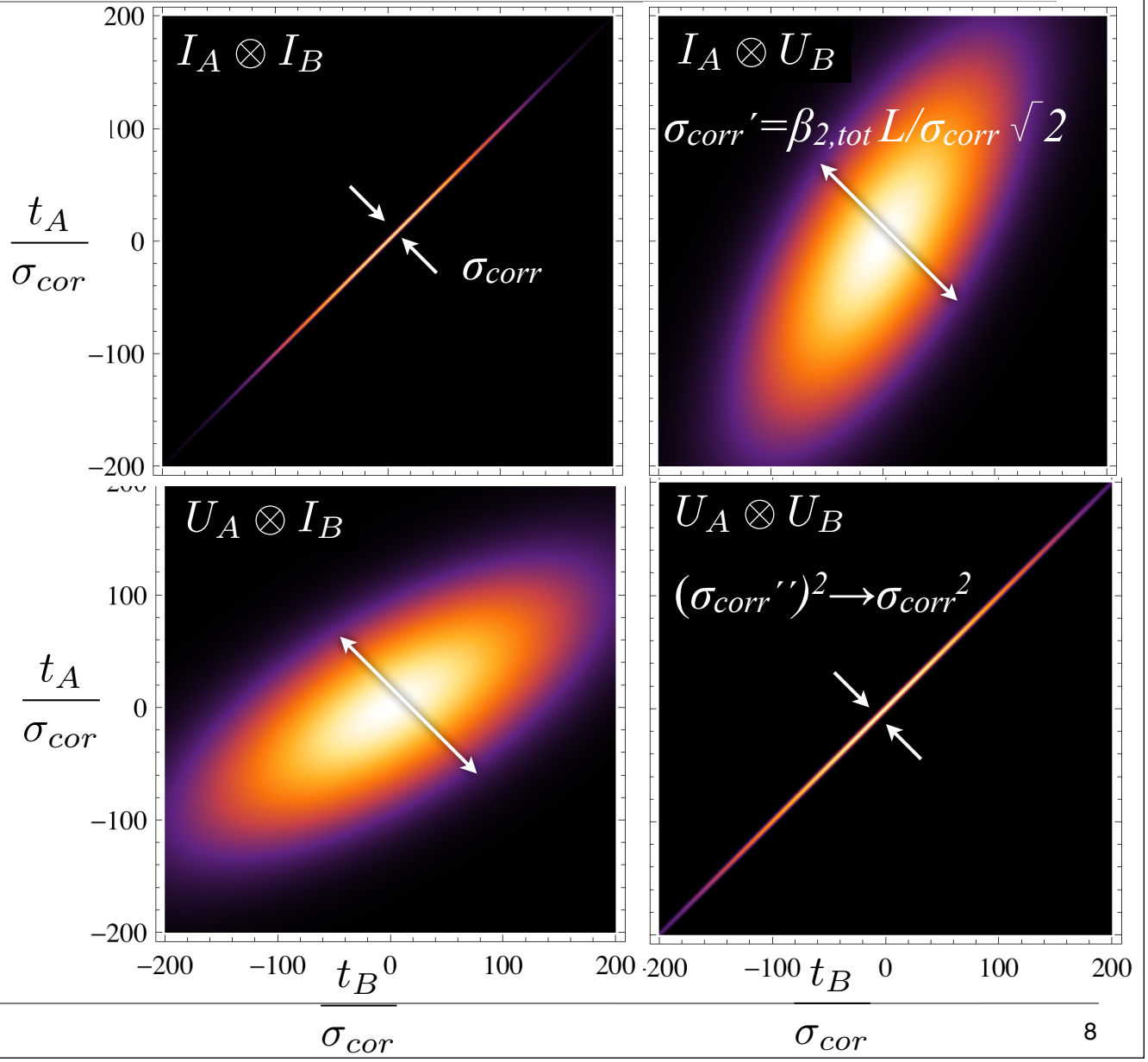
$$G(\omega) \propto e^{iC\omega^2}$$



The effect of dispersion on biphoton correlations

Coincidences:

P_{coinc}	I_A	U_A
I_B	~1	~1/d
U_B	~1/d	~1



Additional questions:

1. Are two bases sufficient?
2. When are the correlations sufficiently reduced?

Security for DO-QKD

$$\Delta I = \beta I(A,B) - \chi(A,E)$$

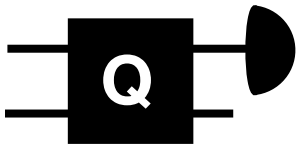
Secret-key capacity

Reconciliation efficiency

Mutual information

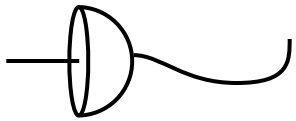
Holevo information

Holevo information - bound on Eve's information given 'general coherent attack'



Calculated from the covariance matrix[2]

Mutual information - Alice and Bob make time-of-arrival measurements



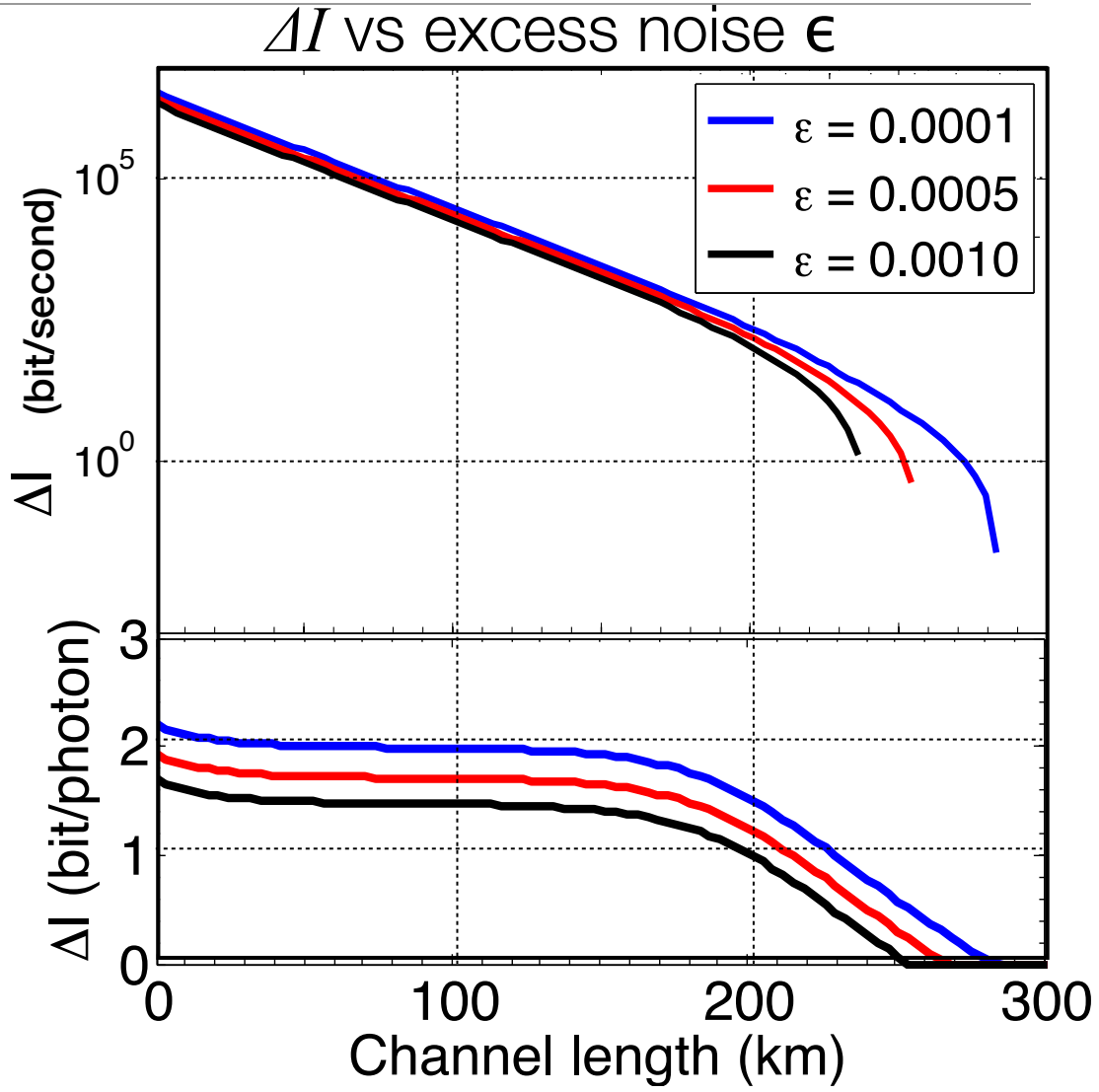
Secret-key capacity - Information advantage of Alice and Bob over Eve after error correction and privacy amplification

•Holevo Probl. Peredachi Inf. 1973

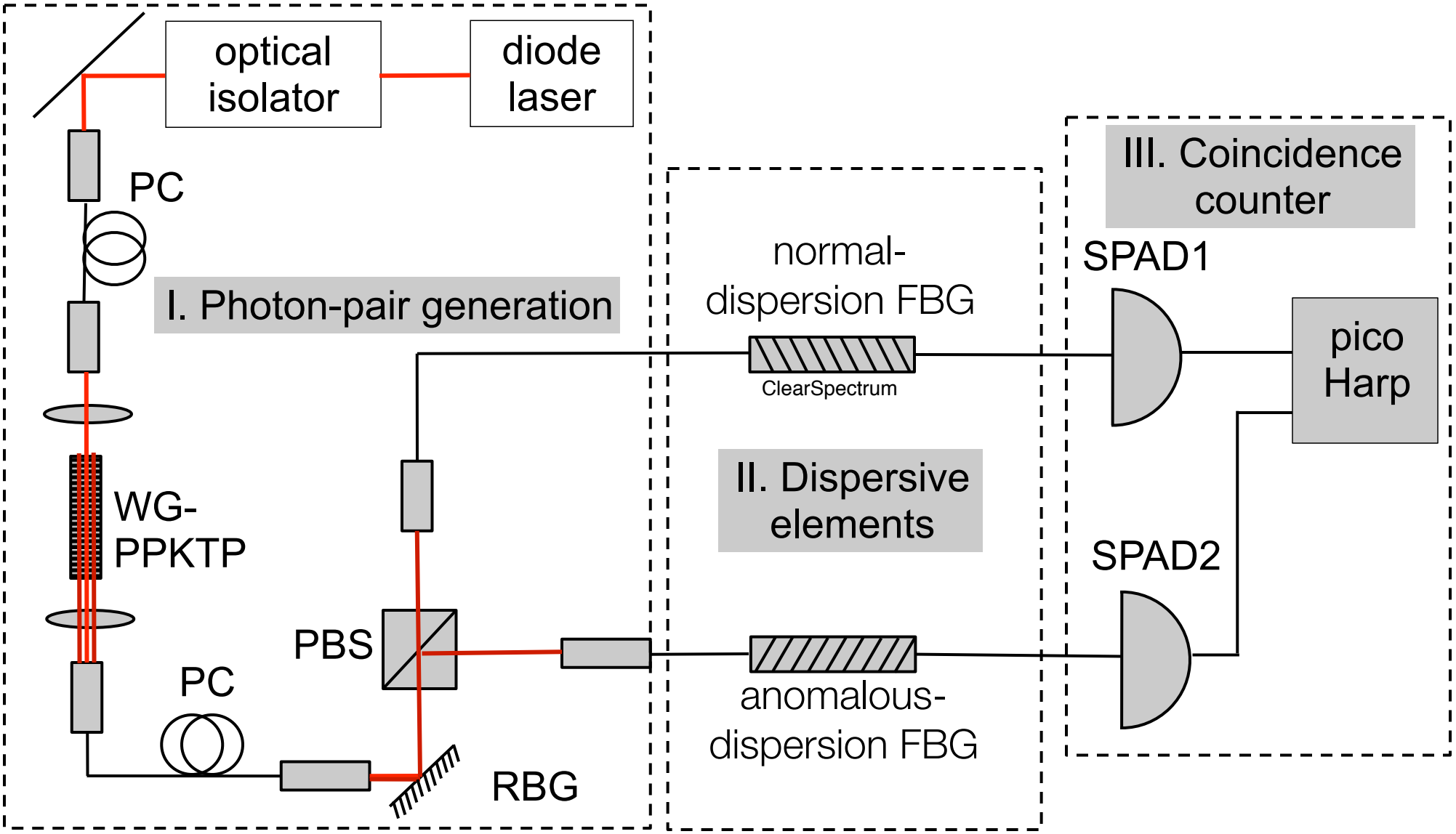
•[2]Weedbrook *et al.,* Rev. Mod Phys. 2012

Preliminary Analysis of security for DO-QKD

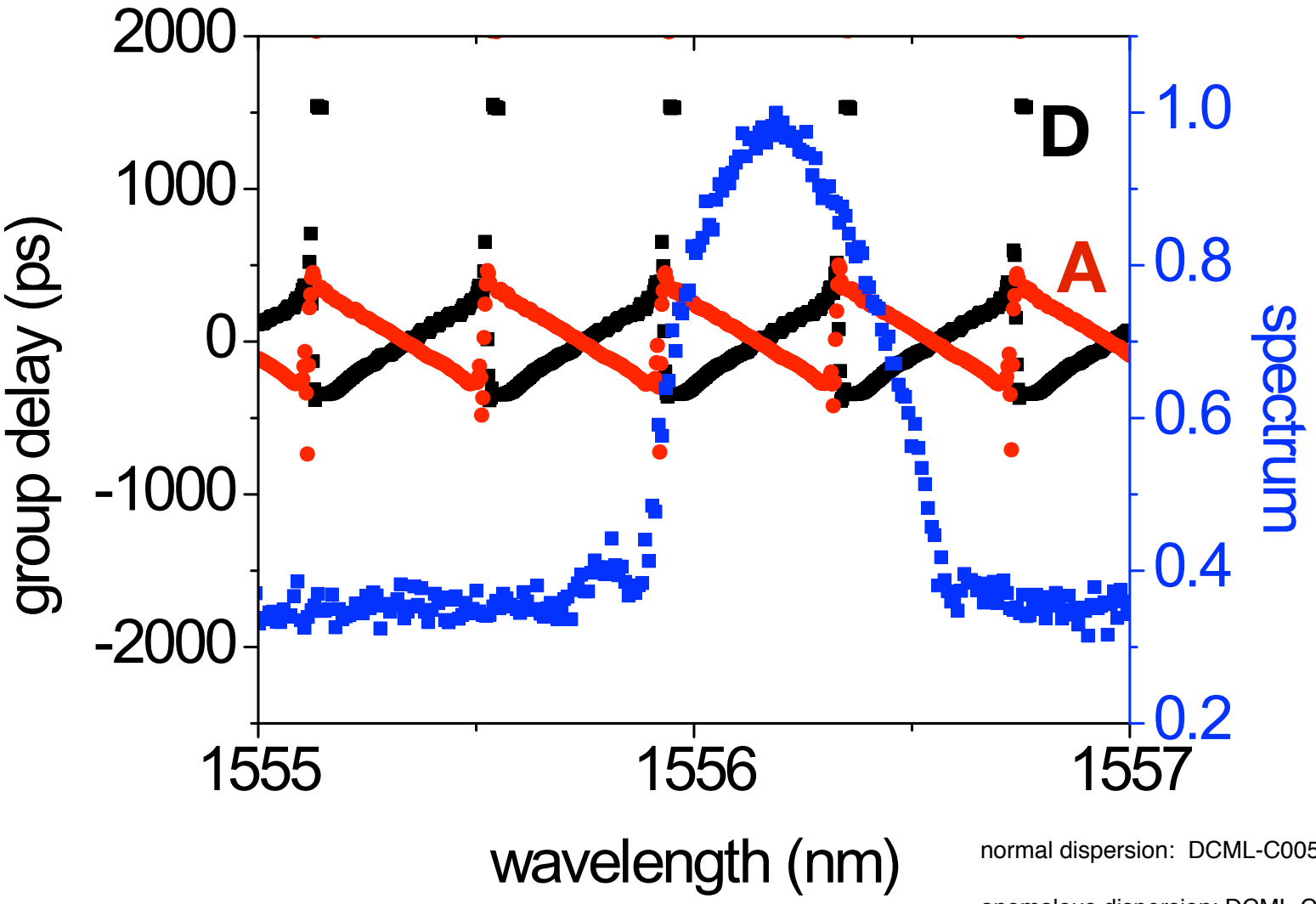
Parameter	Value
T_α	200 ps
d	20
σ_{coh}	100 ps
σ_{cor}	1 ps
J	1 ps
P_D	10^{-5}
λ	0.01
$\beta_2 L$	10,000
β	0.8
α	0.2 dB/km



Experimental Setup



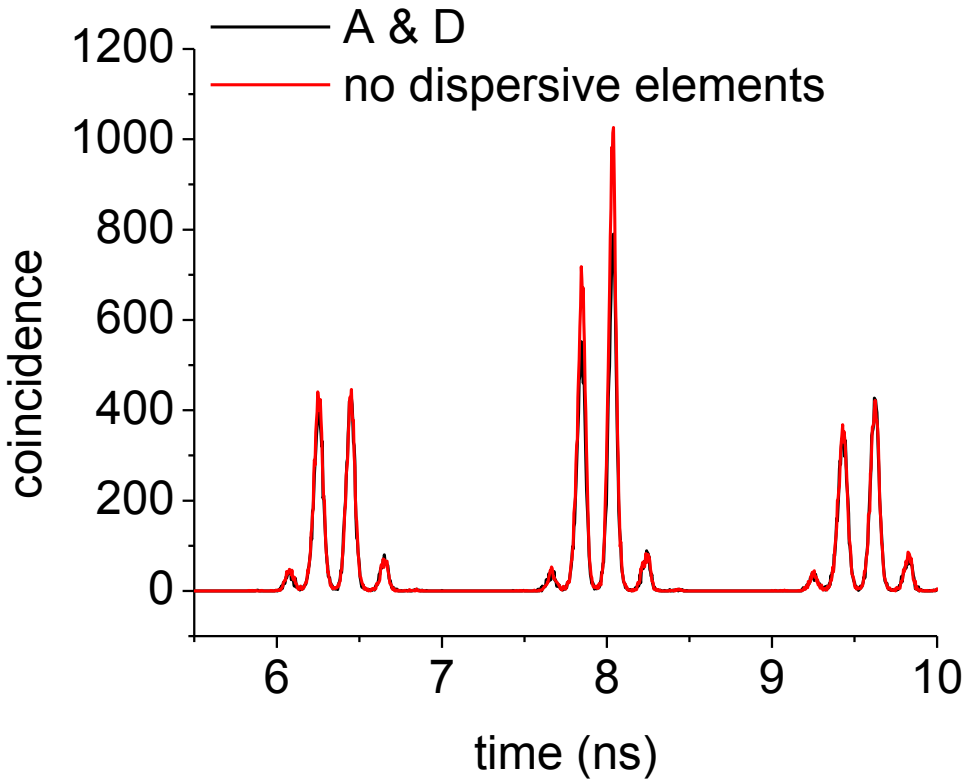
Dispersive elements

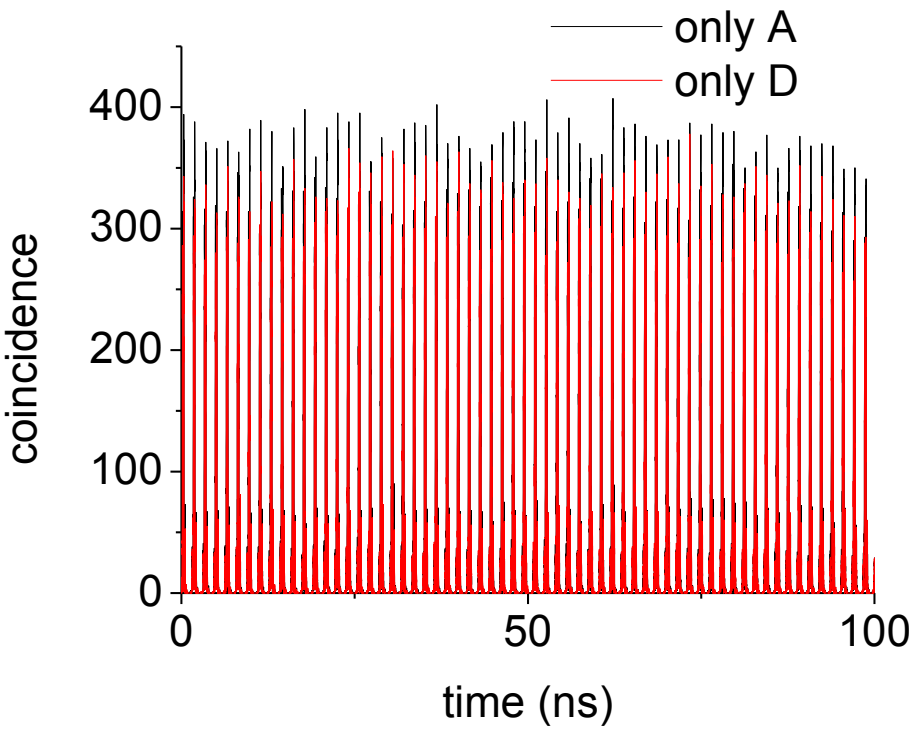


normal dispersion: DCML-C0050+100k-AB080

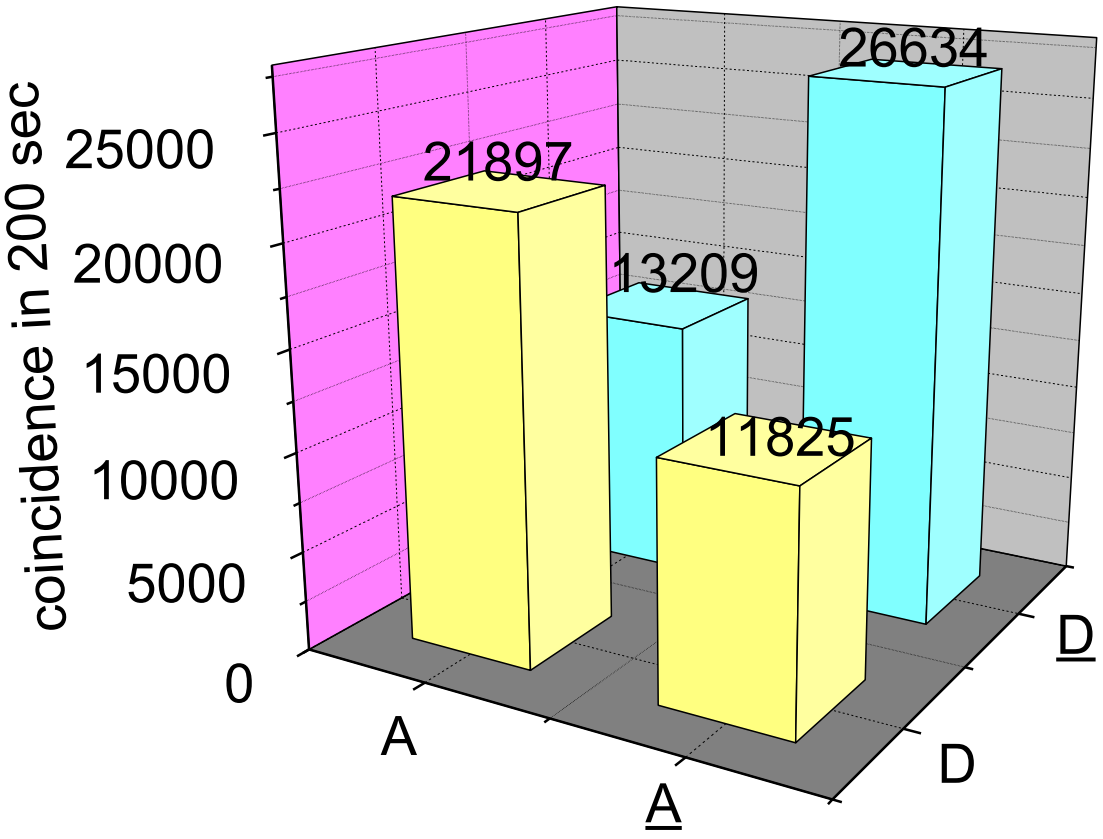
anomalous dispersion: DCML-C0050-100k-AB080

Results


A & D
no dispersive elements
coincidence
time (ns)
1200
1000
800
600
400
200
0
6
7
8
9
10


only A
only D
coincidence
time (ns)
400
300
200
100
0
0
50
100

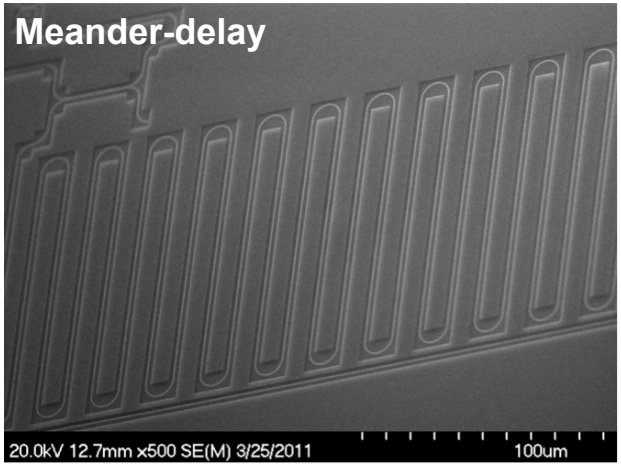
Experiment

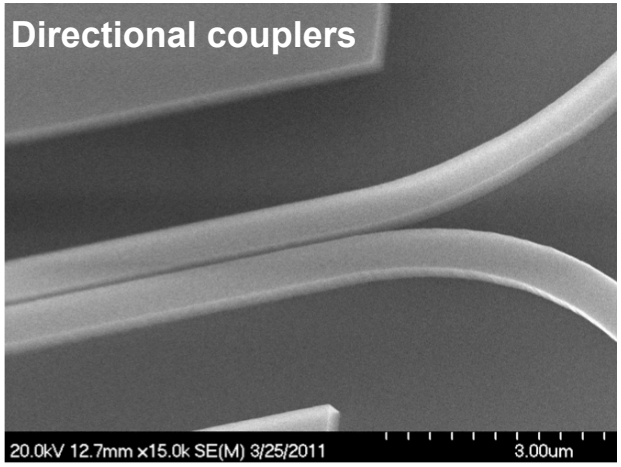


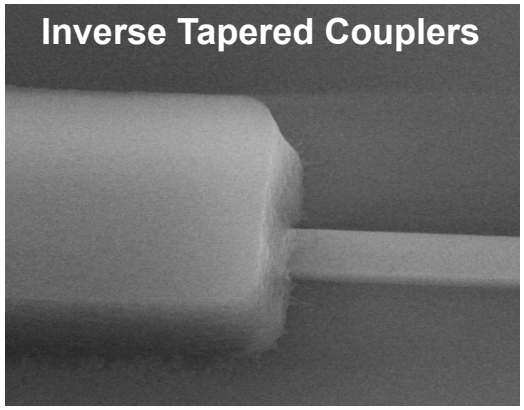
(including dark counts)

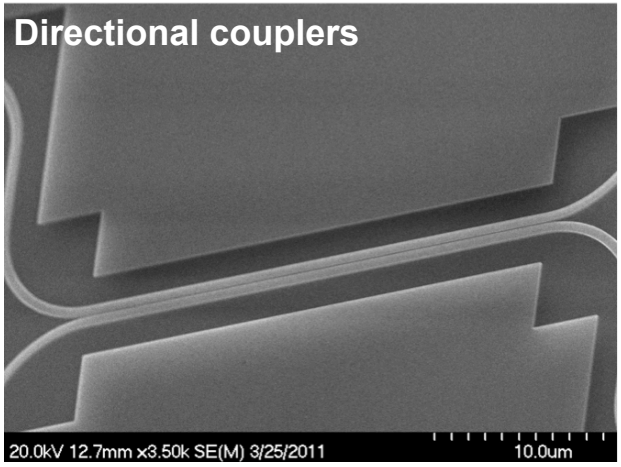
Photonic Integrated Circuit (PIC)

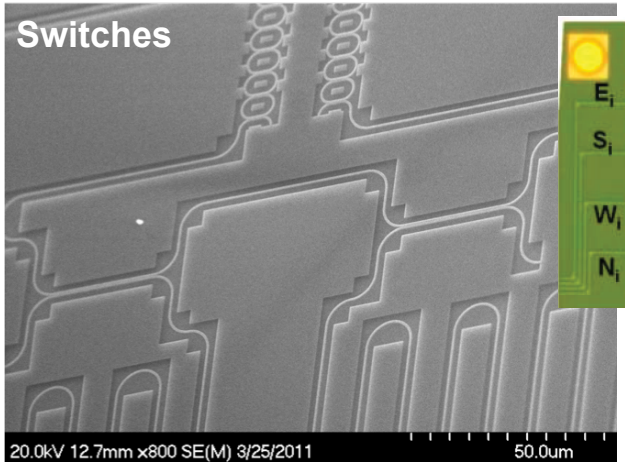
- Optical setup is translated to a PIC in Silicon on Insulator (SOI): contains most components for Alice & Bob in phase-stable device



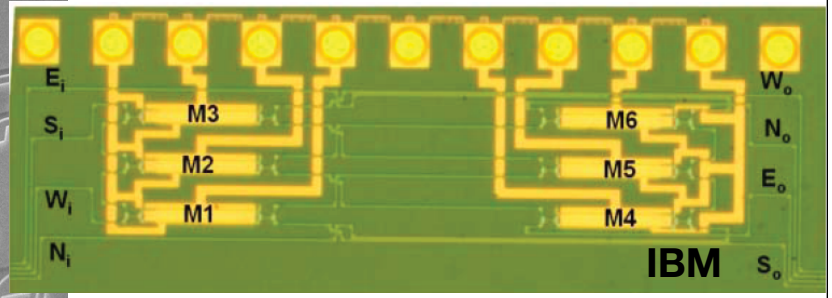








tunable networks

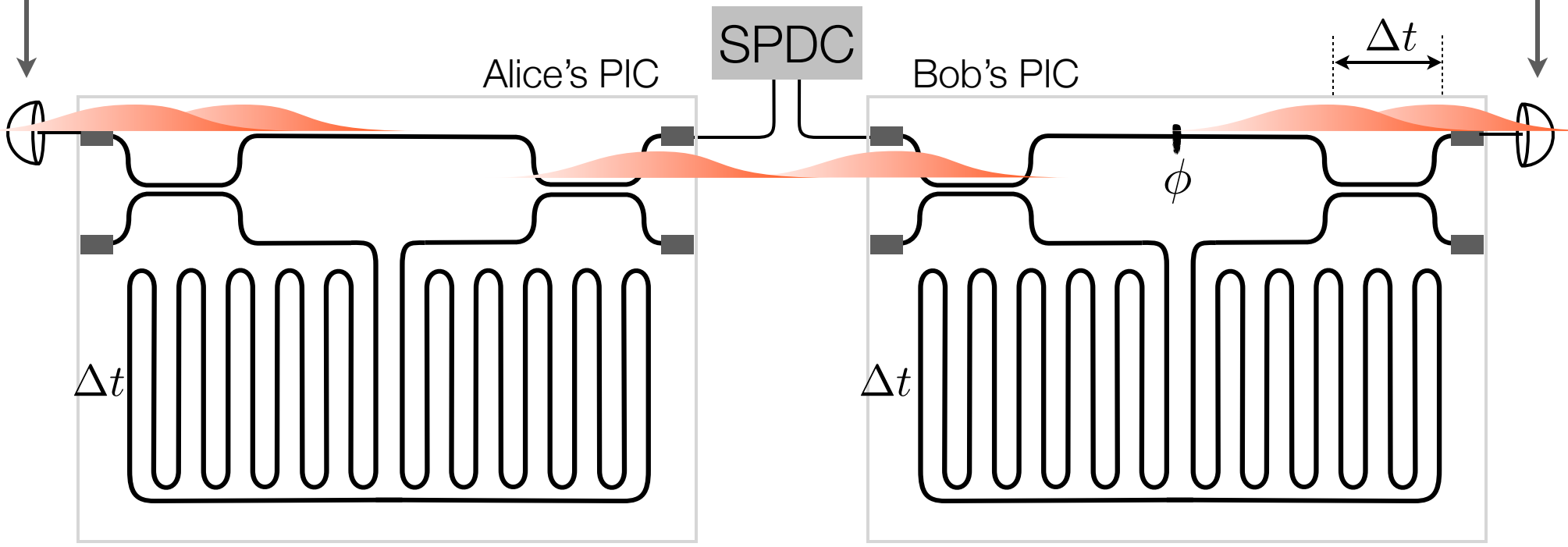


J. Mower (CU) &
Solomon Assefa (IBM)

Testing quantum correlations between PICs

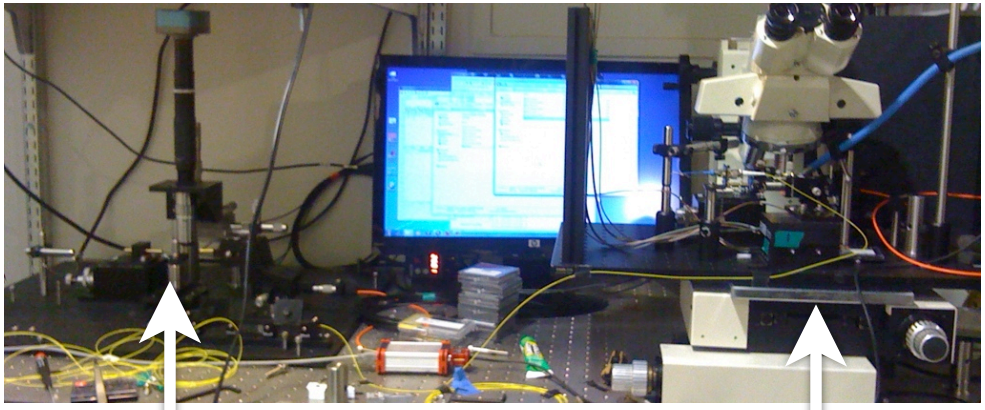
Franson interferometer

$$P_C \propto \frac{1}{2} + \frac{1}{2} V \cdot \cos[\phi_o + \phi]$$

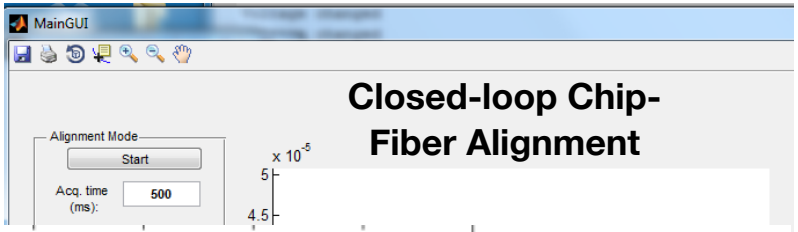


[1]J. D. Franson, Phys. Rev. A, (1991)
Use in QKD?: [2]I. Ali-Khan et al, Phys. Rev. Lett. **98** (2007)

PIC Setup

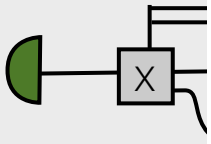


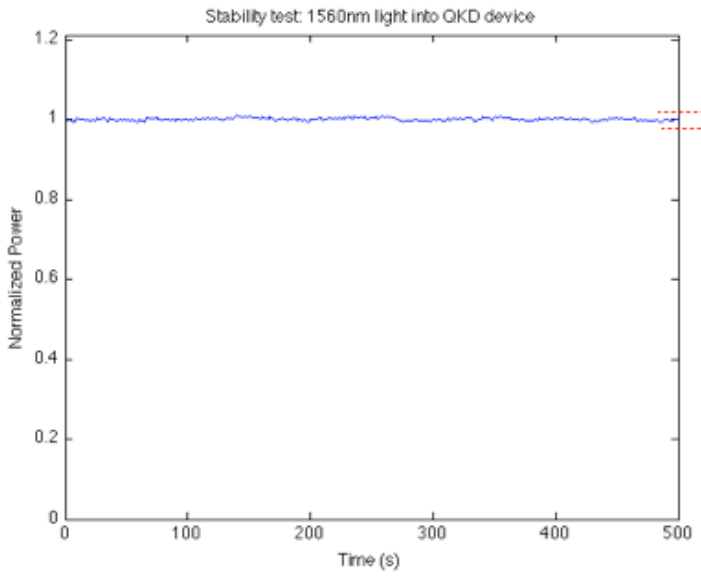
- Alice and Bob are computer controlled

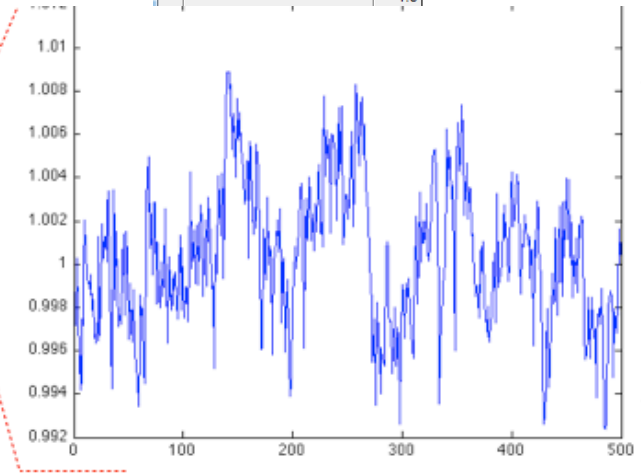


Closed-loop Chip-Fiber Alignment

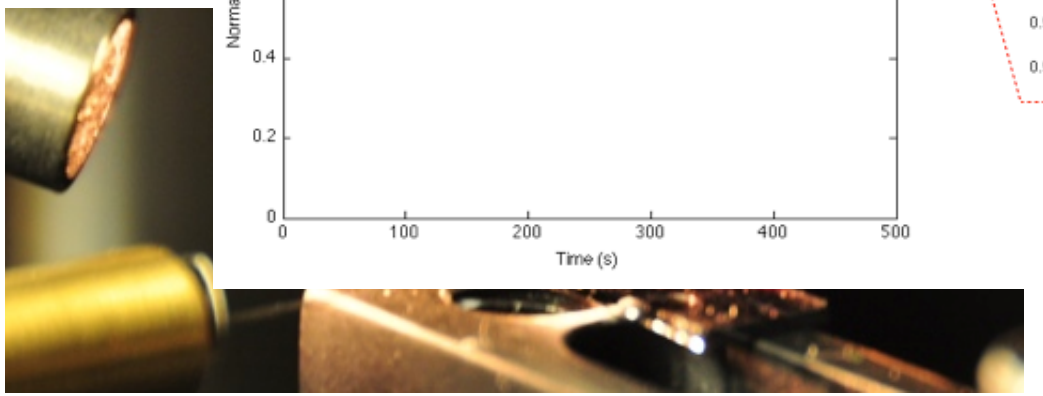
BOB





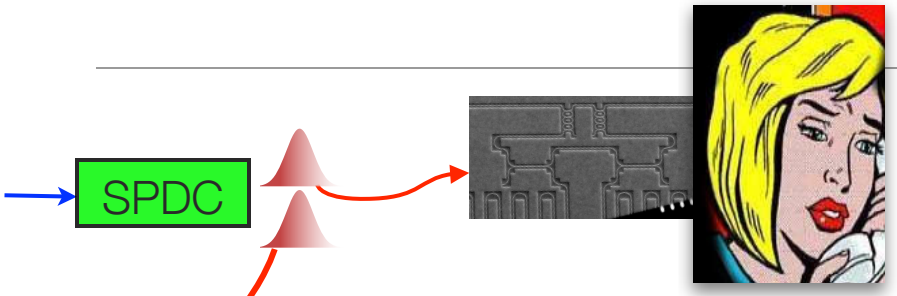


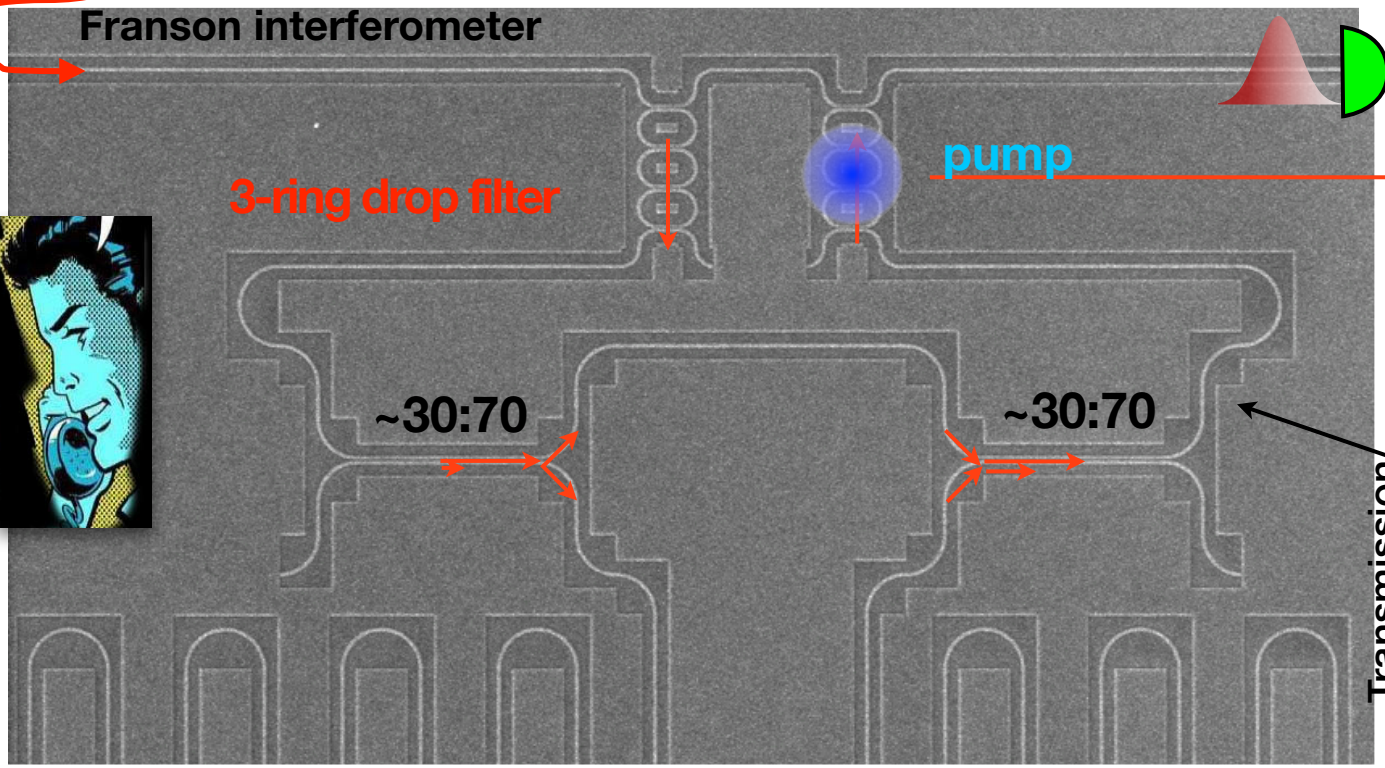
+/- <1%

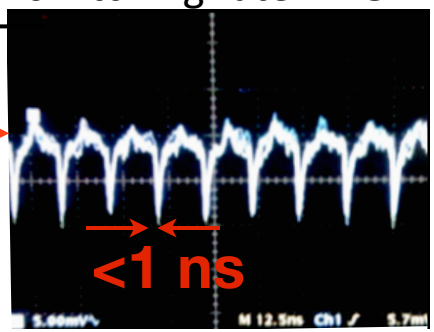


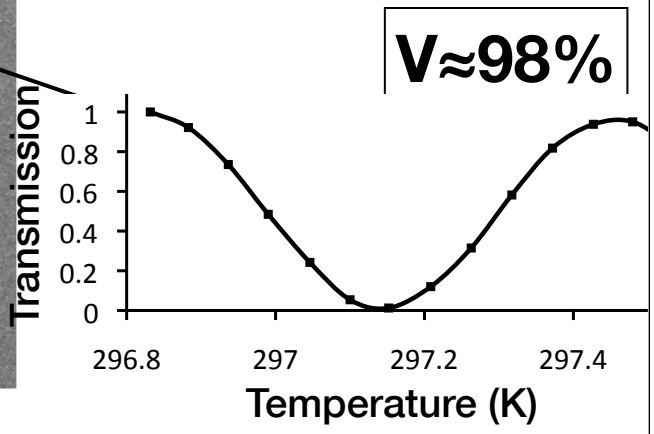
J. Mower, Chris Hoder, D. Englund

Chip-based quantum key distribution systems





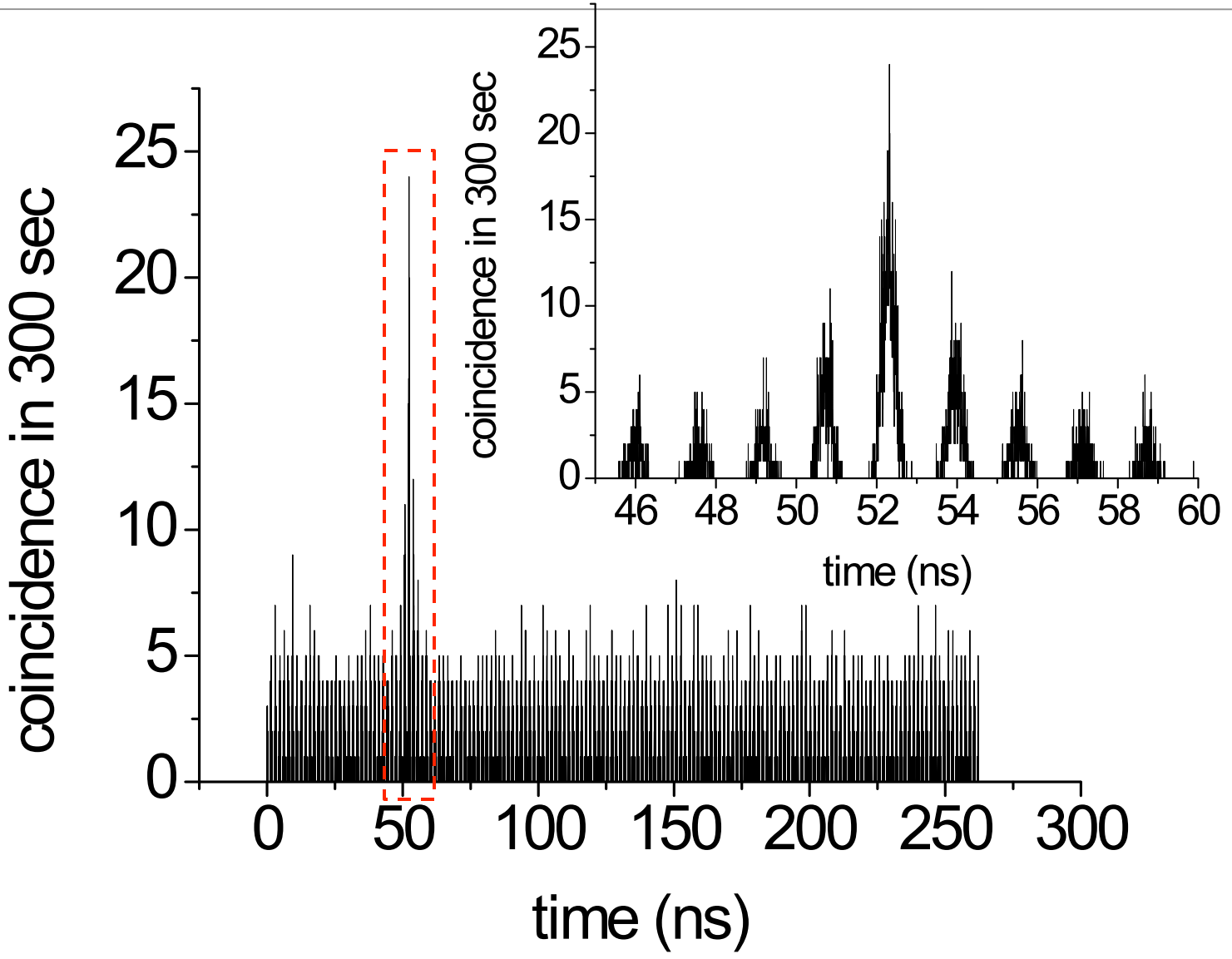




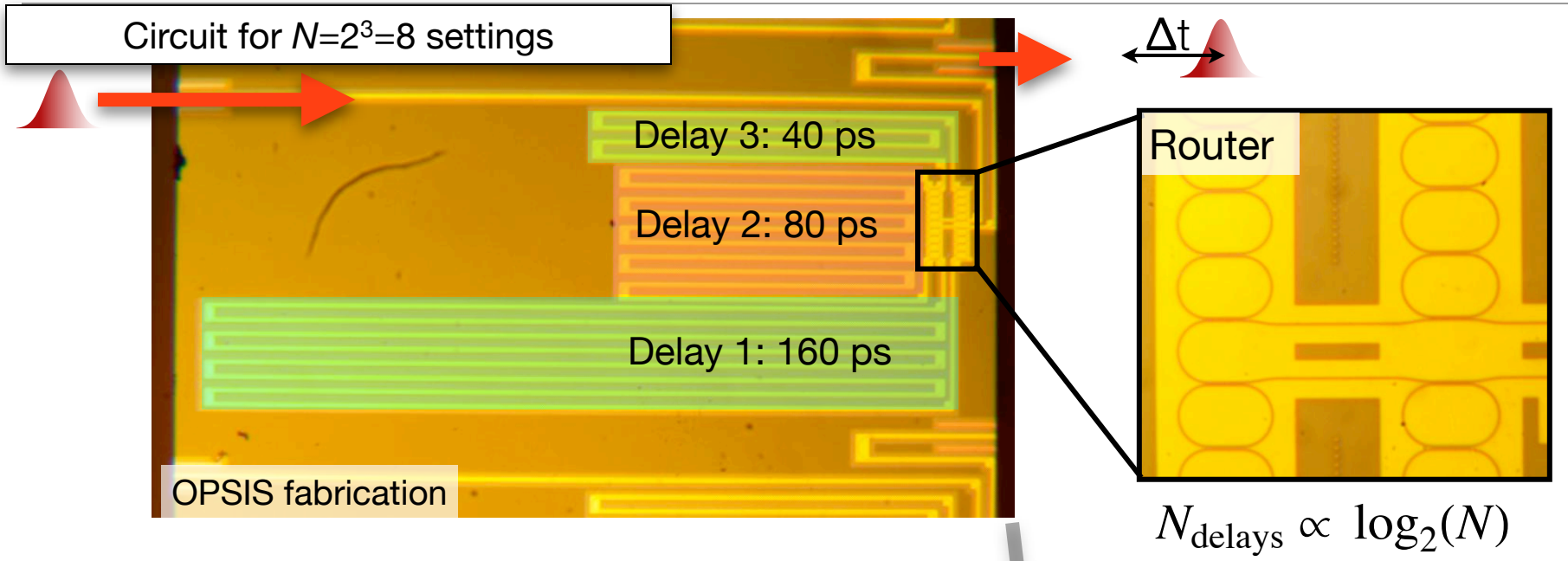
J. Mower, S. Assefa (IBM), D. Englund

•Franson for checking QKD security? Khan, Broadbent, Howell PRL 2007

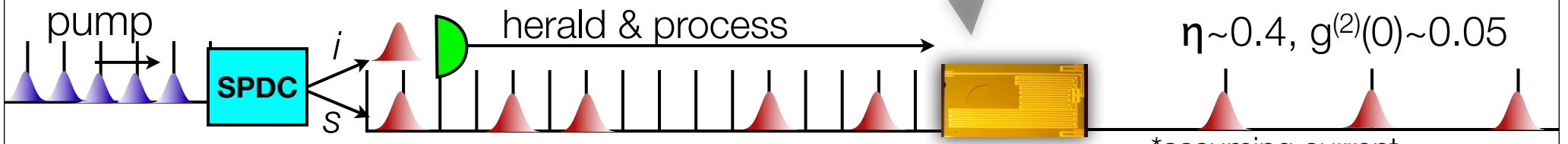
Coincidence across two silicon waveguides



Reconfigurable photon delay circuit for deterministic single photon generation



Actively multiplexed parametric photon (AMPP):



Estimate for $N_{delays}=5$*:

η~0.4, $g^{(2)}(0)$~0.05

*assuming current switches & detectors; η~0.8 with better devices

Generalized for generation of range of nonclassical states.

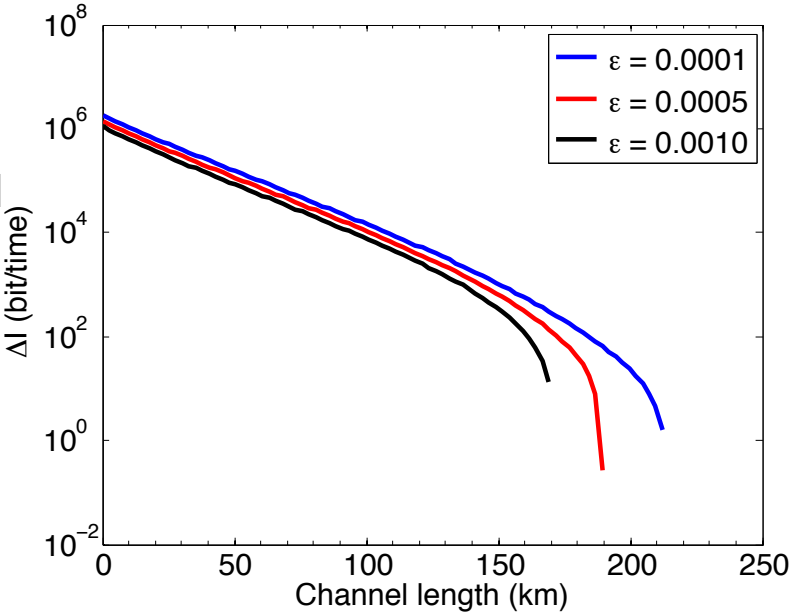
[1] J. Mower and D. Englund, PRA **84** (2011)

Free-space proposals: A. L. Migdall et al, PRA **66** (2002); -J. H. Shapiro and F. N.Wong, Opt. Lett. **32** (2007); E. Jerey, N. A. Peters, and P. G. Kwiat, New J. Phys. **6** (2004).

Conclusions and outlook

I. DO-QKD:

1. Temporal correlations + dispersive optics transformation allows high-dimensional QKD protocol secure to general coherent attacks
2. Suited for fiber optics
3. Scale key generation rate with WDM

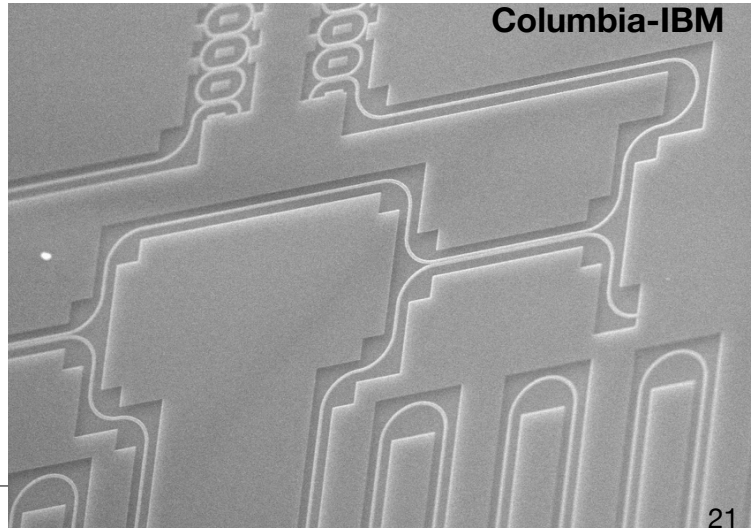


II. On-chip silicon photonics:

1. Nearly all optics can be integrated on chip
2. Active control & electronics integration
3. Deterministic source of indistinguishable single photons at room temperature

III. Future:

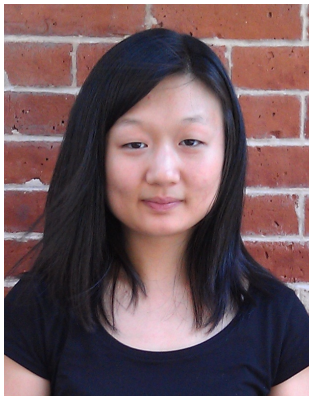
1. Complete security analysis of DO-QKD
2. Experimental implementation
3. Error correction & privacy amplification
4. Scale up bit per photon



Acknowledgements

- **PhD Students:**
- Jake Mower (G3)
- Pierre Desjardins (G1)
- Catherine Lee (G1)
- Xualong Hu (postdoc)
- **Collaborators:**
- Jeffrey Shapiro, MIT
- Franco Wong, MIT
- Solomon Assefa, IBM Watson Research Center






Funding

- DARPA Information in a Photon Program