Generating entanglement in solids, and detecting entanglement for QKD

Josh Nunn

Clarendon Laboratory, Oxford University, UK

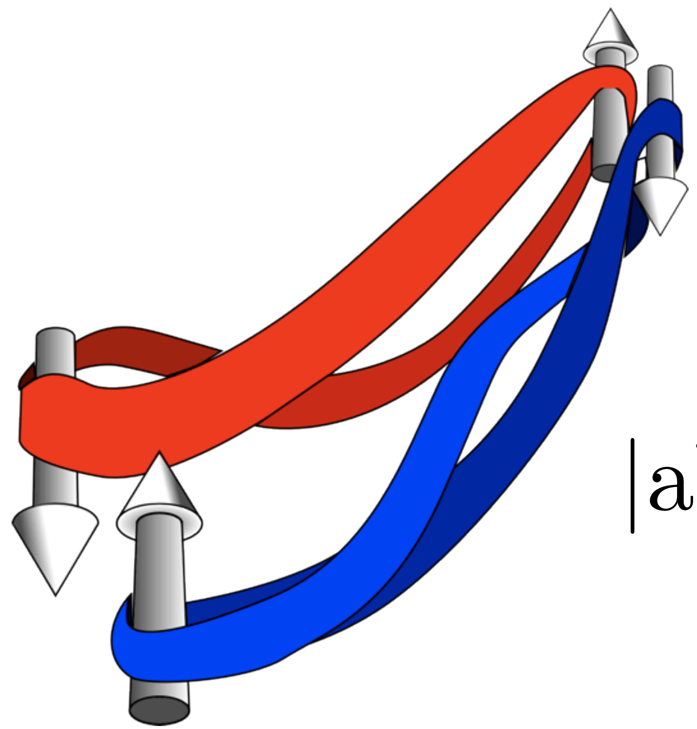
& NRC, Security & Disruptive Technologies, Ottawa, Canada

Two talks, tenuously linked…

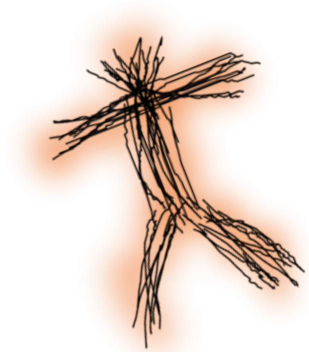
Part I: Entangling solids

Quantum correlations

- EPR
- Bohm
- Bell
- Kochen Specker
- PBR
- ……..

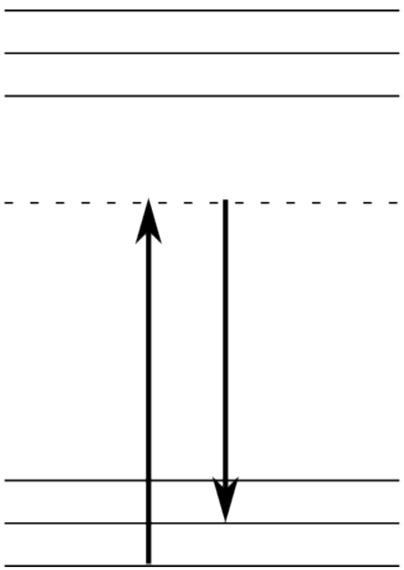


$$|ab\rangle + |ba\rangle$$



- What are the limits to quantum correlations?
- Can large objects be entangled?
- Can solid objects be entangled?
- Can room-temperature objects be entangled?
- How could we “see” entanglement in a classical object?

Raman scattering

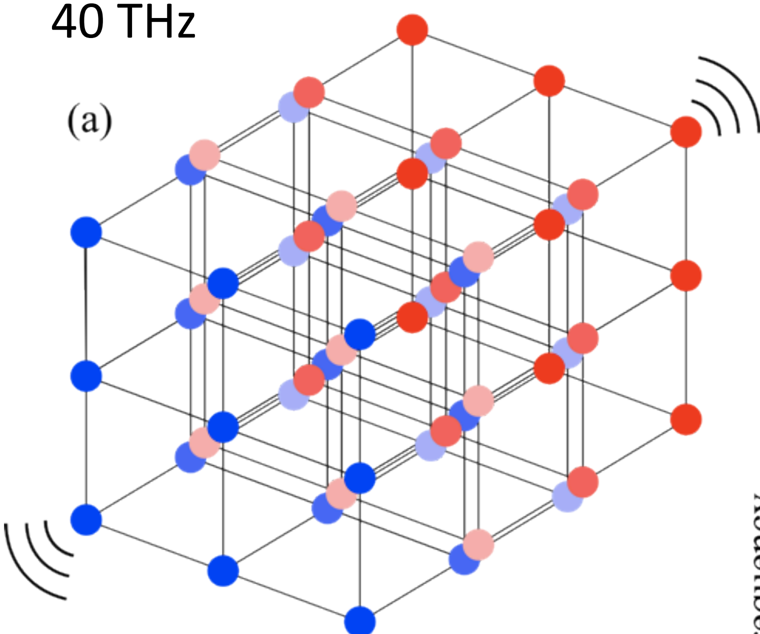


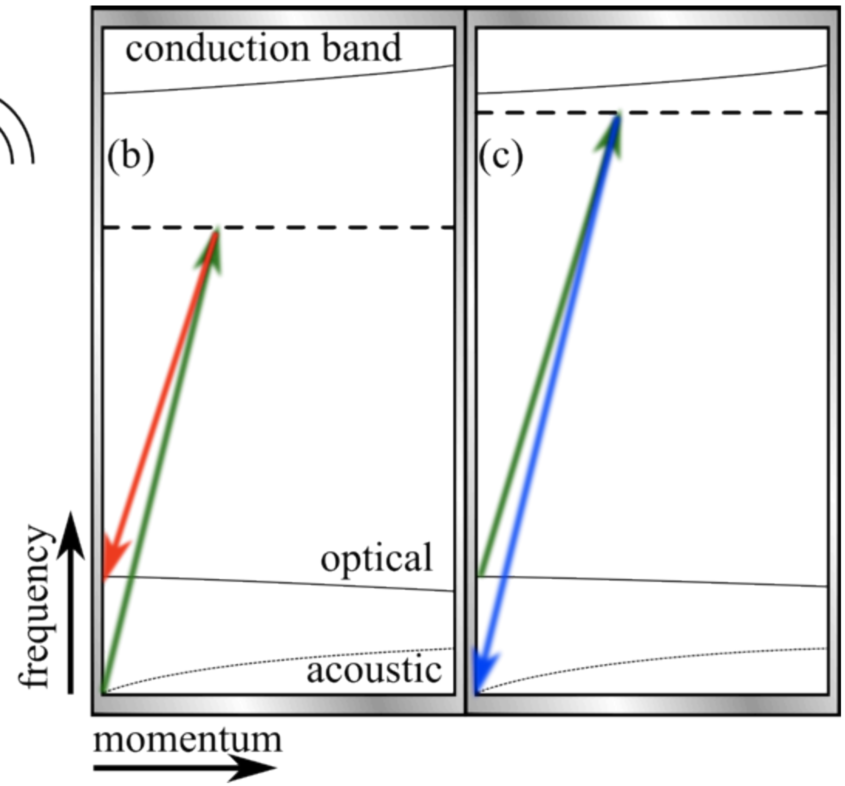
- inelastic scattering (energy change)
- off-resonant (virtual resonance)
- access non-optical transitions
- fast and coherent
- Gases, liquids, solids…

[Bloembergen, Raymer, Walmsley…]

Optical phonons in diamond

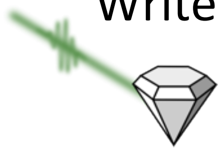
40 THz



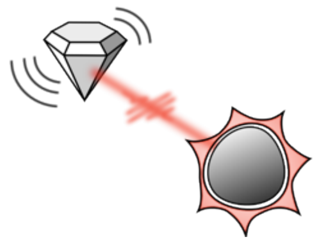


Diamond scattering

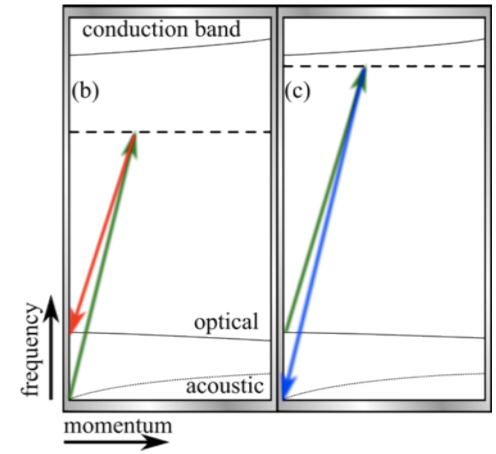
Write



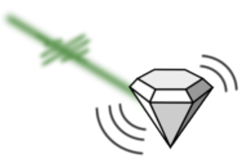
Phonon created



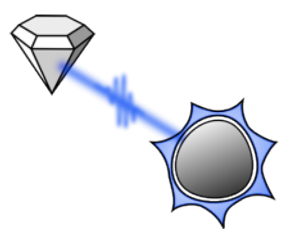
Stokes
(spontaneous)



Read

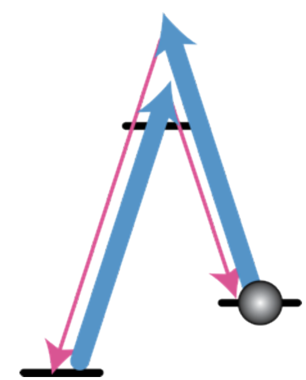


Phonon destroyed



anti-Stokes
(requires Stokes first)

FWM



Cauchy-Schwarz inequality

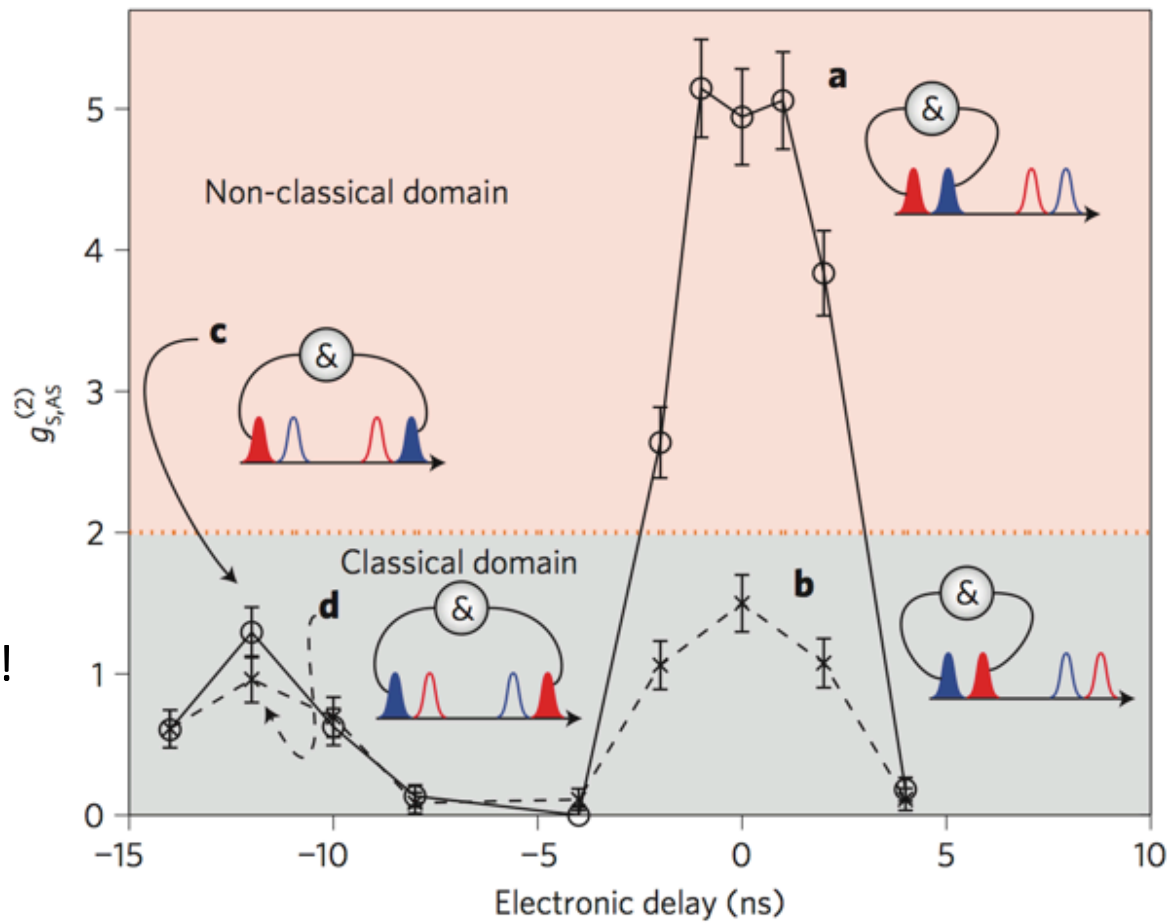
Classical scattering:

$$g^{(2)}_{\mathrm{S,AS}}(0) < 2$$

Violation

↓

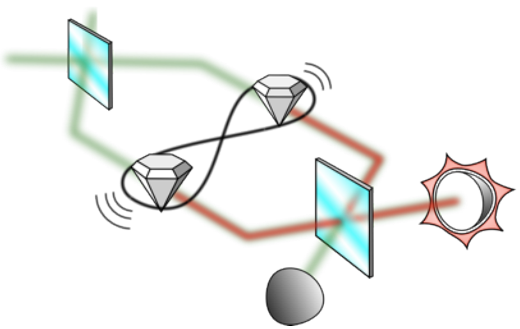
Quantum correlations!



Lee *et al.* Nature Photonics **6** 41 (2012)

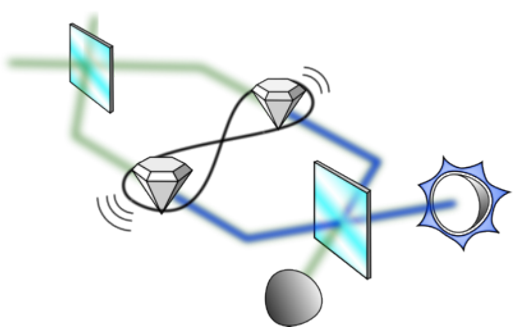
Try with two…

Write (delocalized phonon created)



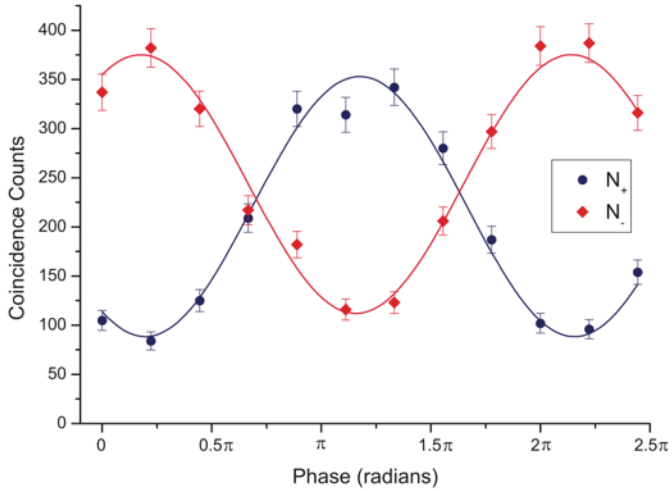
$$|01\rangle + |10\rangle$$

Read (verify **entanglement**)

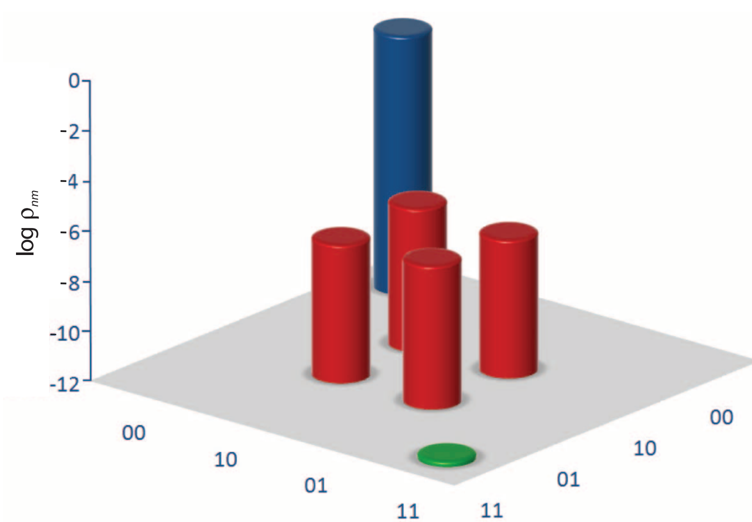


Results

Interference (i.e. phase matters)



Photons one at a time…



Concurrence C = (5.2 ± 2.6) × 10^{-6}

Entangled with 98 ± 1% confidence (took 3 weeks!)

Two entangled objects:

- Macroscopic
- Solid state
- Motional degree of freedom
- Room temperature / pressure

Visible on ultrafast timescales…

Are long timescales possible?
Are C of M superpositions possible?

Lee *et al.* Science **334** 1253 (2012)

Please also see Usmani *et al.* Nat. Phot. **6**(4) 234 (2012)

Perhaps the public know best…

One might wonder if this phenomenon of phonon activity constitutes a "quantum ecology" in an environmental field of relatively (referenced by detector) differential equations. On the practical scale, there is something of a model here (albeit in a vaguely lit shadow form) of neuron activity (with phantom pathway schema for dendritic branching?) in the synchronicity of mind/brain mapping (evoked/provoked?) potentials.

PBS News comments page. Many more like this…

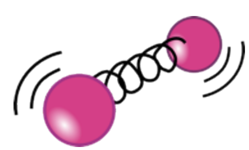
Plug for my sponsors…

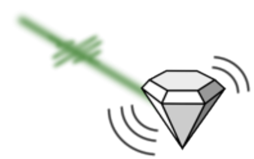
- **Ben Sussman's group at NRC, Ottawa (no jet lag!)**

- Ultrafast quantum random numbers via Raman scattering…

- THz bandwidth quantum memories

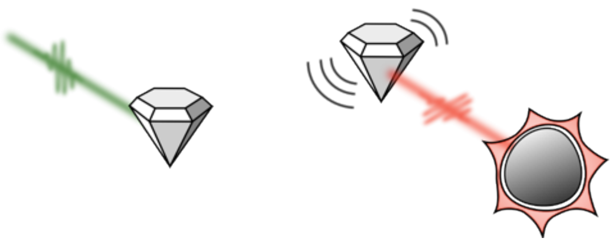
- In both solids (phonons) and molecules (vibrons / rotons)





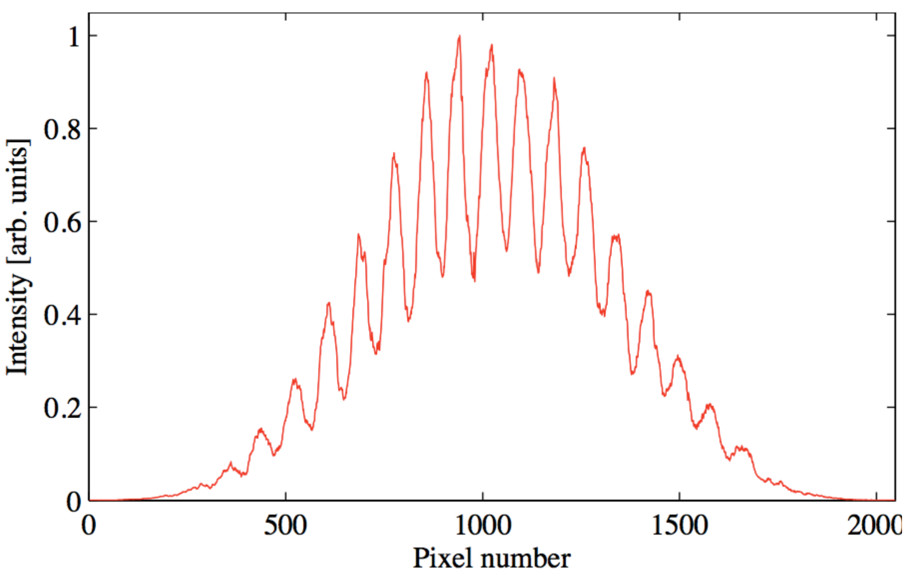
- Hiring grad students!

Example: diamond random numbers



Phase of spontaneous Stokes is a source of quantum random numbers

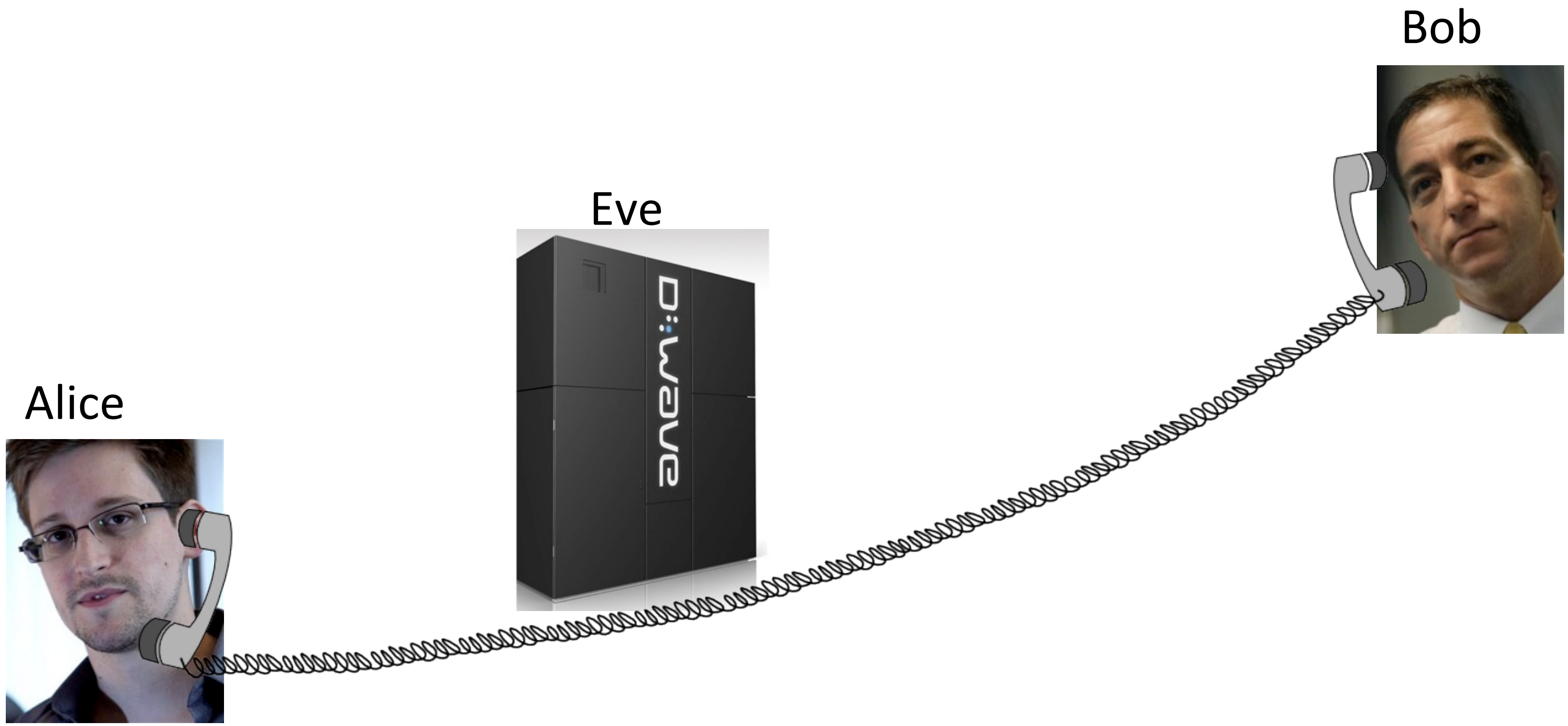
Re-set time = phonon lifetime (3.5 ps). So THz speeds possible…



Birthday spacings	0.140289 (KS)[‡]	Success
Overlapping 5-permutation	0.234407	Success
Binary rank test for 31×31 matrices	0.857819	Success
Binary rank test for 32×32 matrices	0.888548	Success
Binary rank test for 6×8 matrices	0.595644 (KS)	Success
Bitstream	0.11249	Success
OPSO	0.0547	Success
OQSO	0.0806	Success
DNA	0.0247	Success
Count the 1's test	0.217644	Success
Count the 1's test for specific bytes	0.171729	Success
Parking lot	0.437972 (KS)	Success
Minimum distance	0.312133 (KS)	Success
3D Spheres	0.012979 (KS)	Success
Squeeze	0.344869	Success
Overlapping sums	0.100233 (KS)	Success
Runs	0.101465 (KS)	Success
Craps	0.213158	Success

[Quantum Random Bit Generation using Stimulated Raman Scattering, Bustard *et al.* Op. Ex. **19**(25) 25173 (2012)]

Part II: QKD



Quantum Key Distribution

- Send quantum states
- Alice and Bob measure in complementary bases

Any measurement by Eve introduces errors

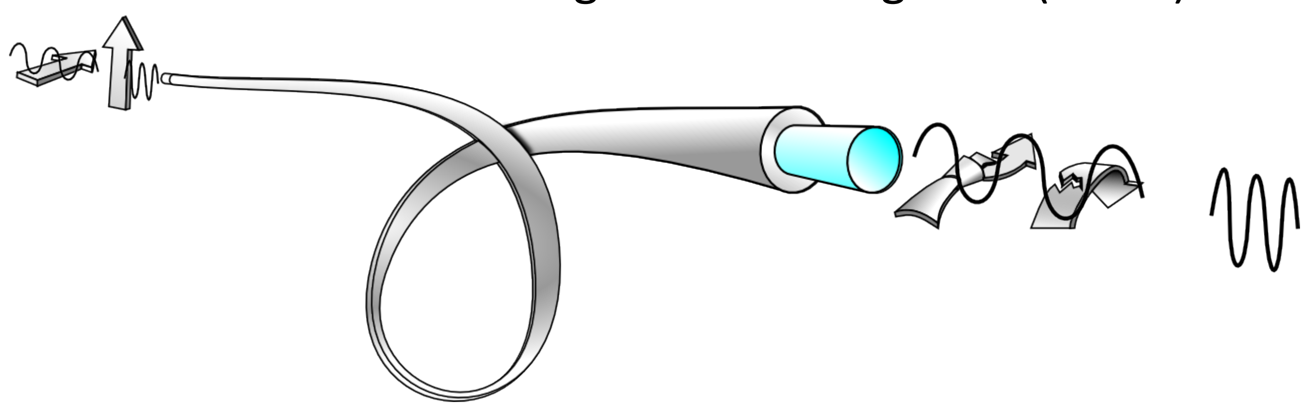
Guaranteed security!

Which encoding?

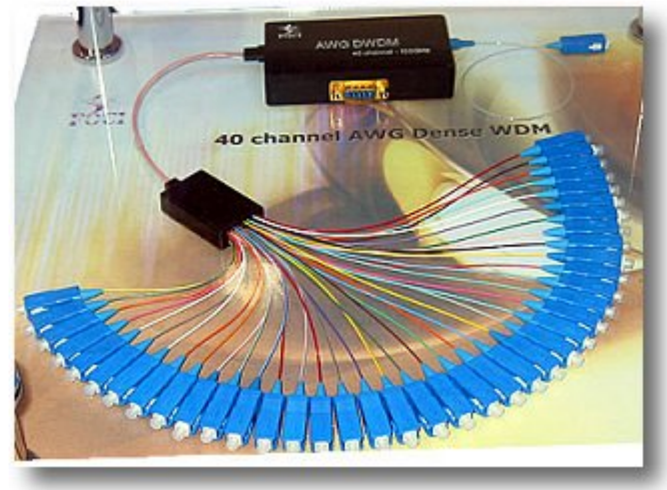
Original proposal: polarisation (BB84)

Time/frequency is more robust!

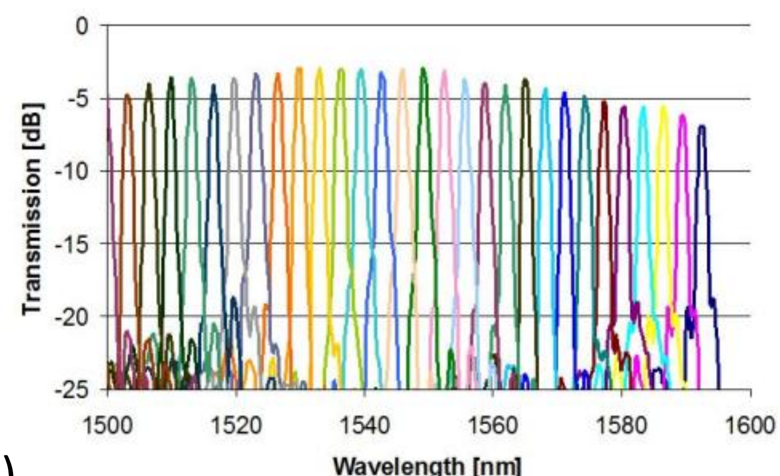
Drawback: birefringence in waveguides (fibres)



Time / frequency



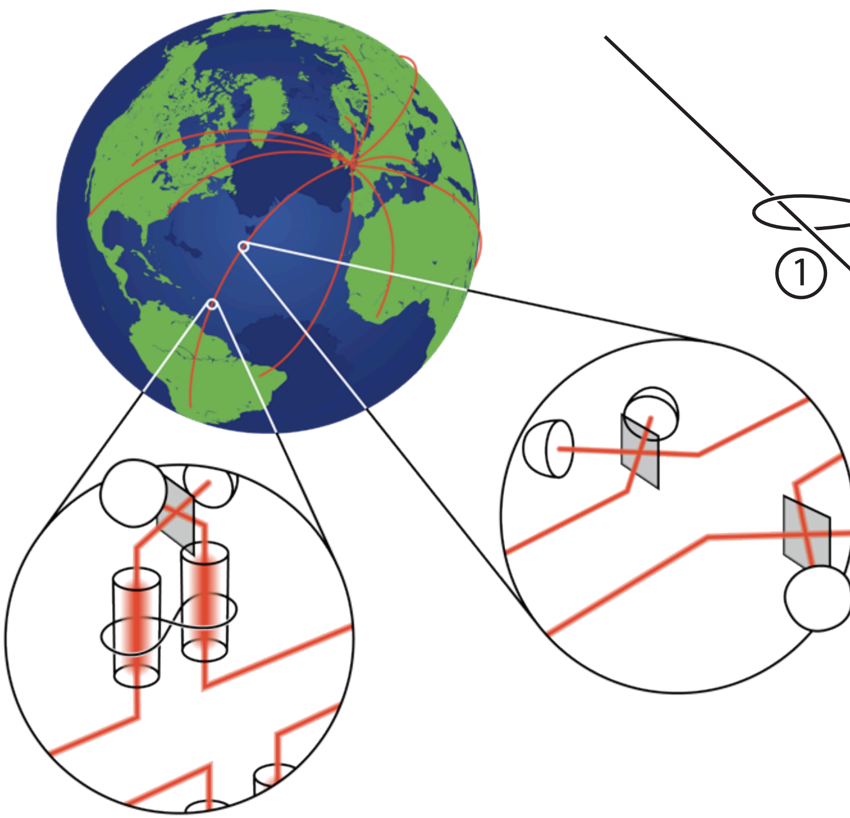
- Already used in classical telecoms…
- High capacity
- Minimal cross-talk in waveguides
- Increasingly recognised in QIP

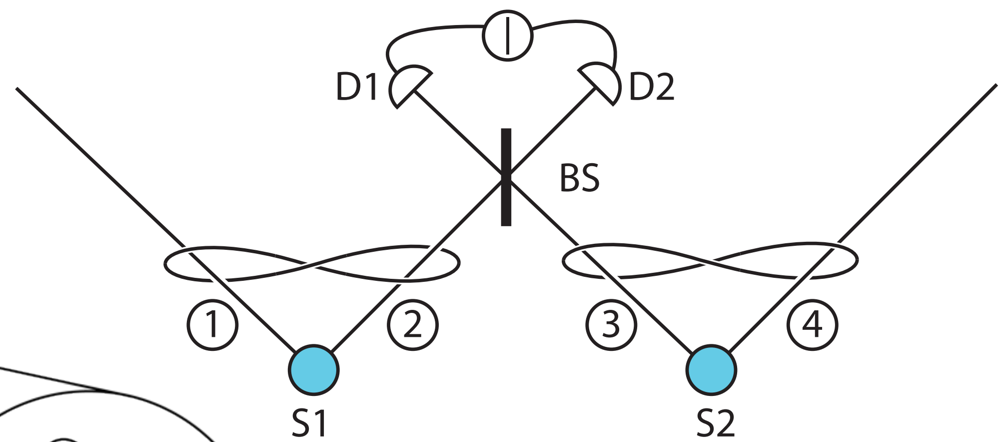


P.P. Rohde *et al.* arXiv:1211.1427 (2012)
Hayat *et al.* Op. Ex. **20**(28) 29174 (2012)

Repeaters

Conventional amplifiers cannot be used
Long distance can be achieved with *quantum repeaters*
Requires entanglement (works via *swapping*)

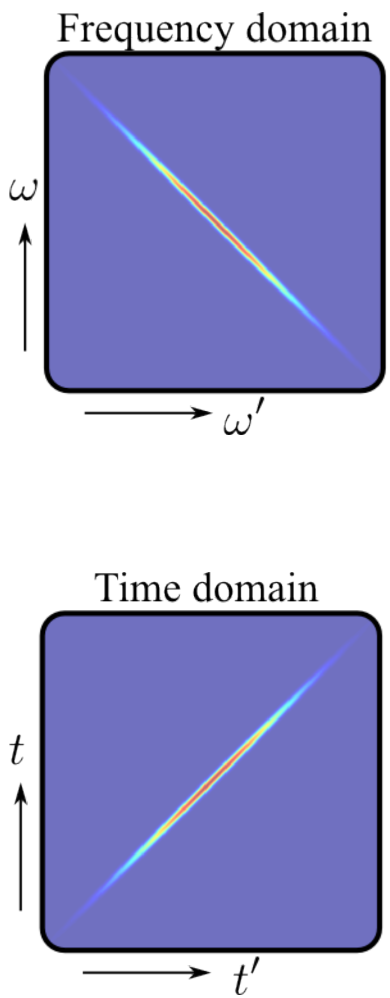


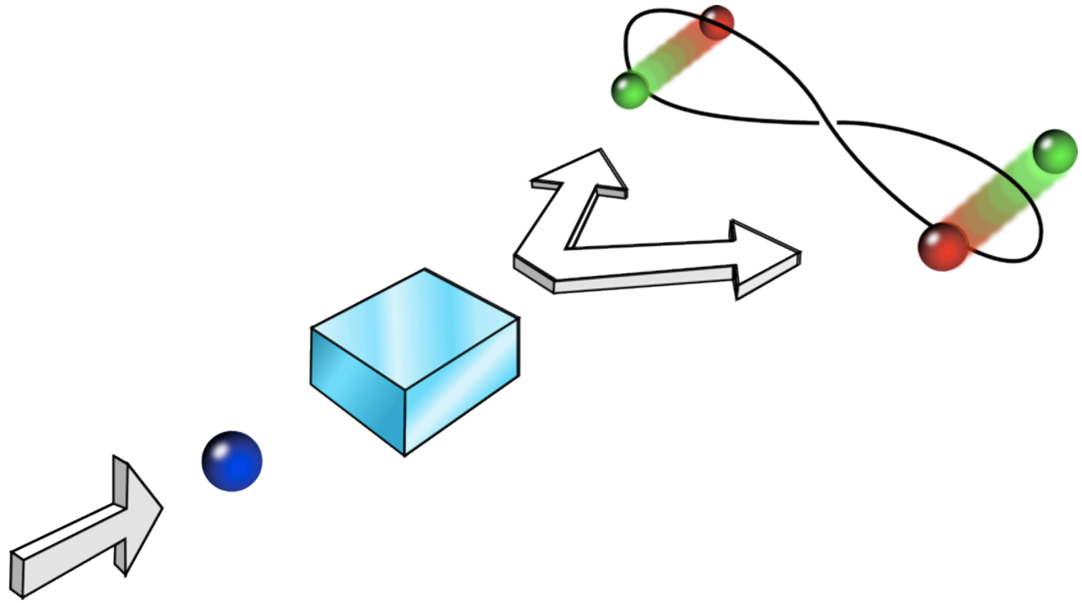


Duan *et al.* Nature **414** 6862 (2001)

Saglamyurek *et al.* IQEC (2011)

Downconversion for T/F entanglement



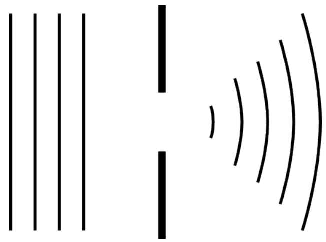


- Highly entangled in frequency and arrival-time
- Difficulty: measuring in both bases
- Efficient detectors are slow
  (although this is changing fast!)
- Can we measure arrival time with slow detectors?

[See Mower *et al*. PRA **87,** 062322 (2013) for the OPPOSITE IDEA!]

[See Zhang *et al*. PRL **100,** 110504 (2008) for QKD with spatial entanglement]

Detour: Fourier optics

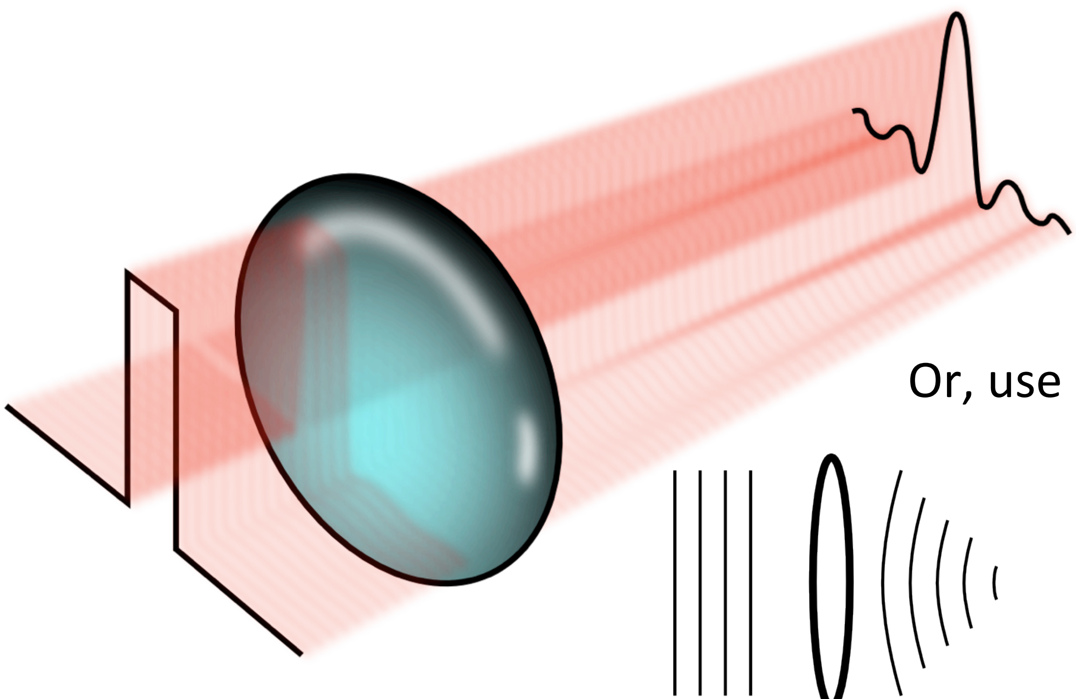


Diffraction in free space: Paraxial wave equation

$$(\nabla_\perp^2 + 2\mathrm{i}k\partial_z)E = 0 \qquad \Rightarrow \widetilde{E} \sim e^{-\mathrm{i}k_\perp^2 z/2k}\widetilde{E}_0$$

Quadratic phase in transverse momentum

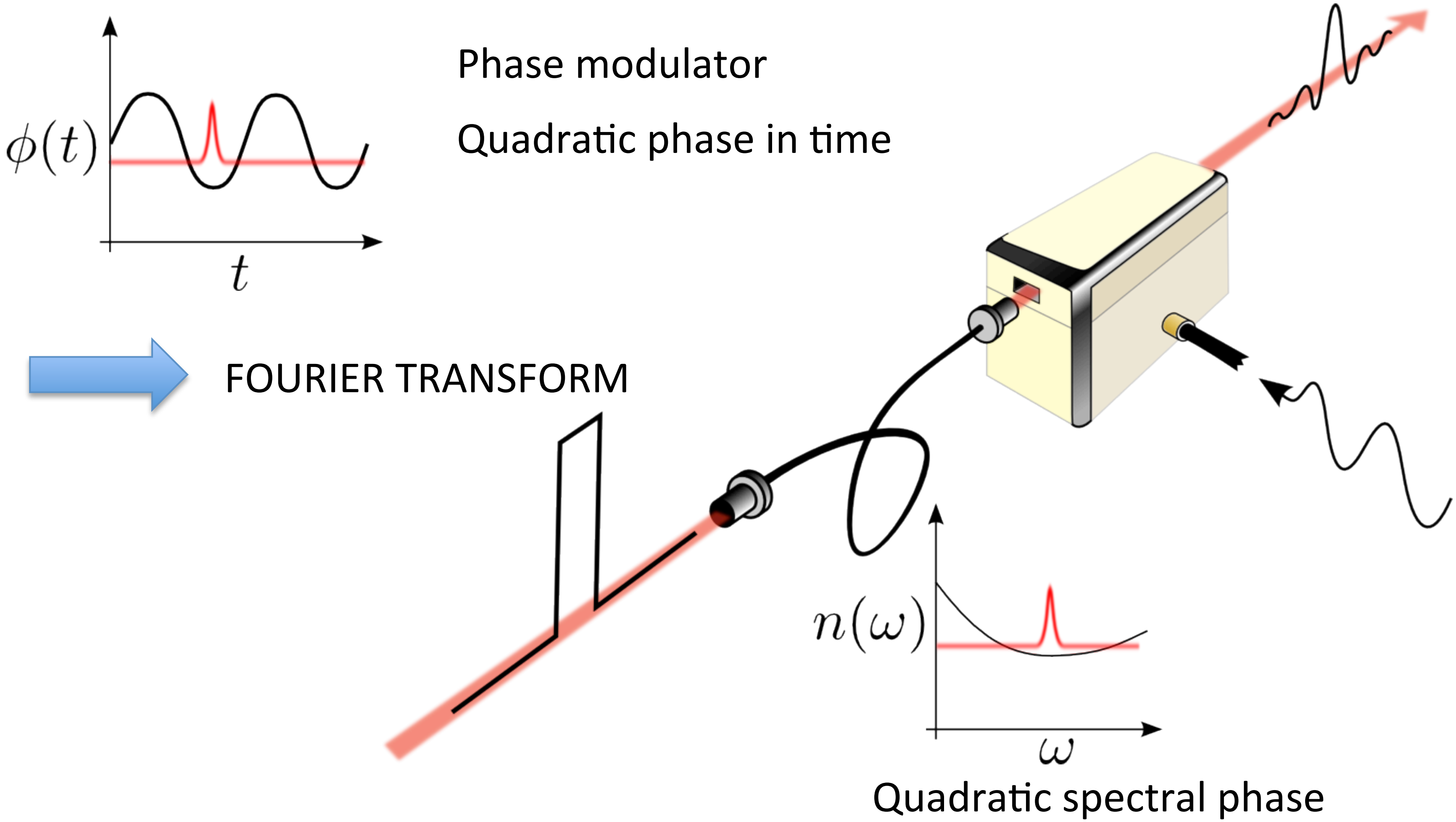
FOURIER TRANSFORM in the far field



Or, use lens to reach Fraunhofer limit (shorter distance)

Quadratic spatial phase

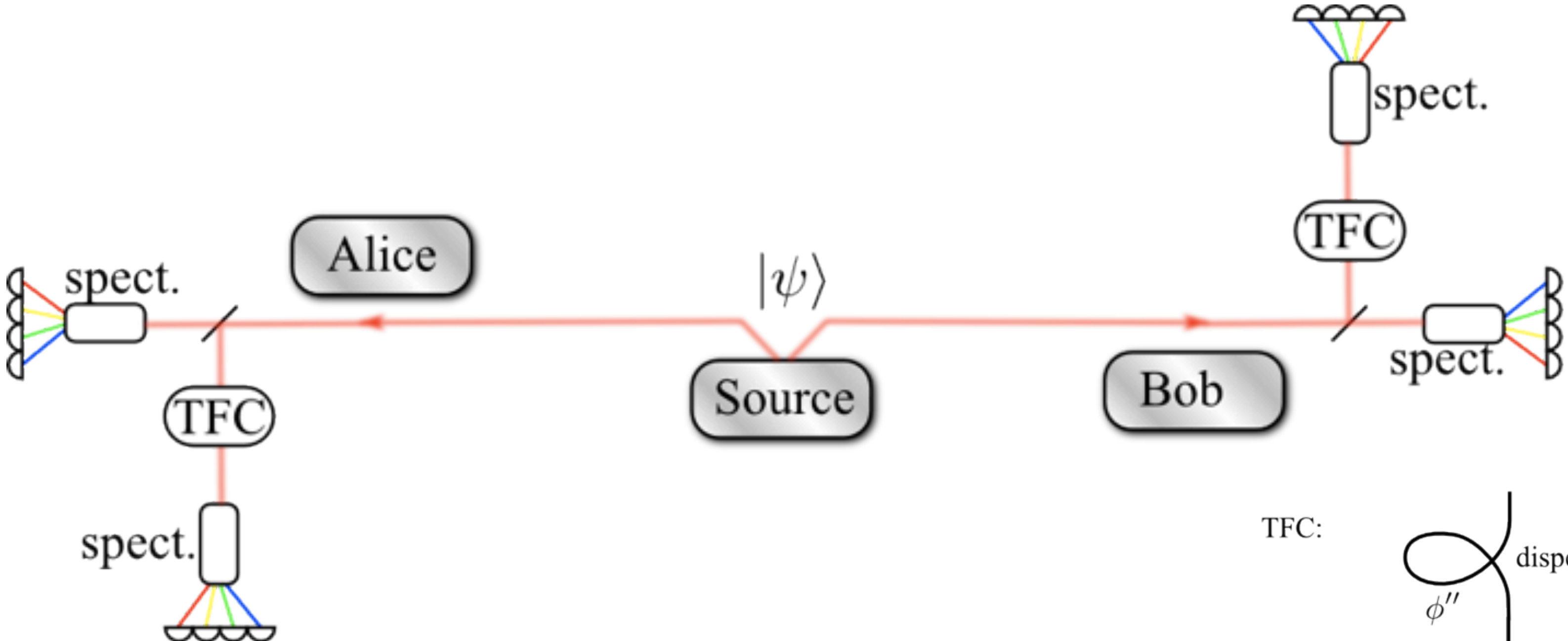
Time-to-frequency conversion

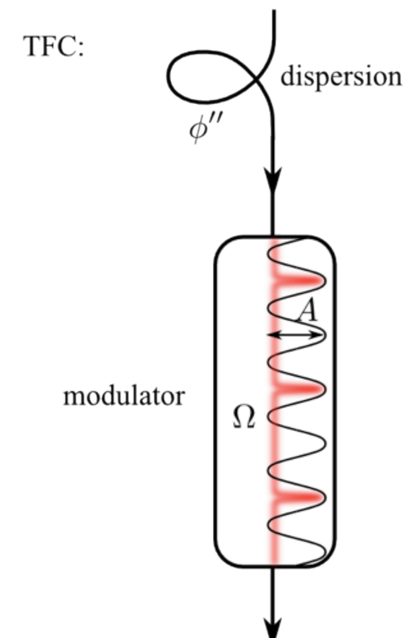


Or, use dispersive element to reach Fraunhofer limit
(smaller modulation depth)

[See e.g. Kolner, J. Quant. Elec. **30**(8) 1951 (1994)]

Our scheme for TFQKD





Modulation cannot be faster than pulse duration

$$A \sim M$$

Modulation depth

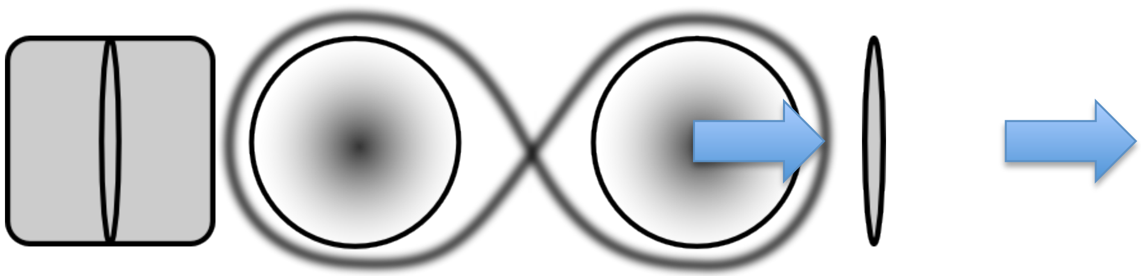
Number of measurement bins

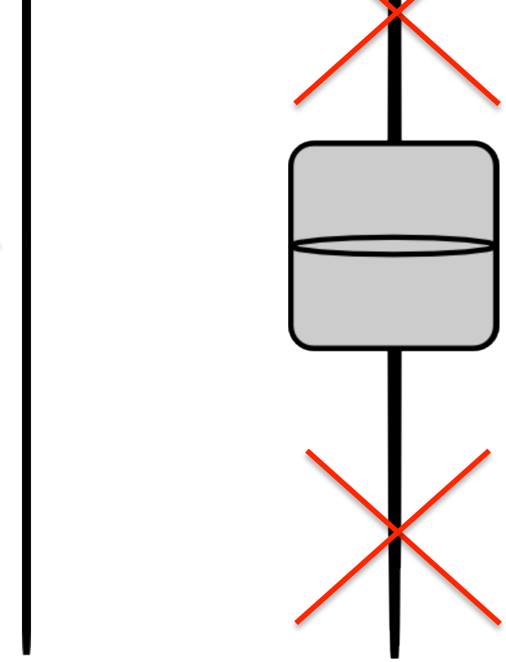
Conventional modulator: $A \sim 20\pi$ $I_M = \log_2 M = 4$ bits

Security analysis

Intuitively: it should work because T/F are Fourier conjugates
But T/F is *continuous*
Any measurement will have *finite* resolution and *finite* range…

Range issue: Alice and Bob must FILTER and TIME-GATE





Could use dielectric stacks / Pockels cells…

Ray and van Enk, arXiv:1302.5087v1 (2013)
Qi, arXiv:1101.5995v1 (2011)

Finite resolution

Hinges on bounding conditional entropy of Bob's outcomes, given Eve's intervention

Uncertainty principle: $H_{\mathrm{B}}(\rho_{\mathrm{cond}}) + \widetilde{H}_{\mathrm{B}}(\rho_{\mathrm{cond}}) \geq B$

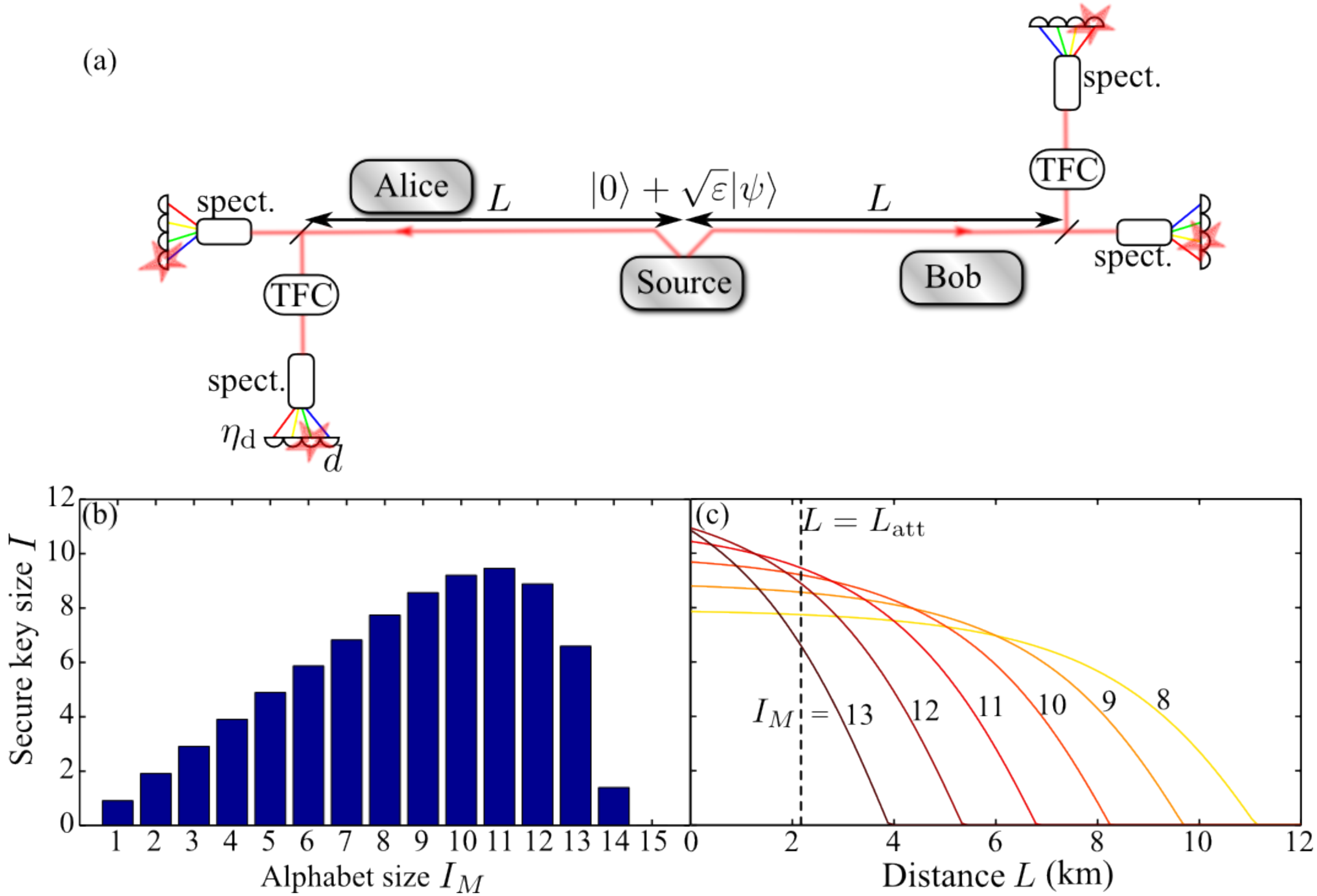
Where $B = -2\log_2 \max_{jk} ||\Pi_j^{1/2}\widetilde{\Pi}_k^{1/2}||_\infty$

Independent of ρ_{cond} — Time measurement — Frequency measurement

Security threshold is essentially the threshold for entanglement detection with coarse measurements [Schneeloch *et al.* arXiv:1303.7432v1 (2013)] (this is my attempt to link the two topics…)

Krishna, M. and Parthasarathy, KR, Ind. J. Stat. A, 842 (2002)
Thank you, Google…

Dark counts & losses



- Key size same as discrete QKD [Bourennane *et al*. J. Phys. A **35**(47) 10065 (2002)], except for small "binning deficit"
- Dark counts "sudden death". Large capacity but sensitive to noise…

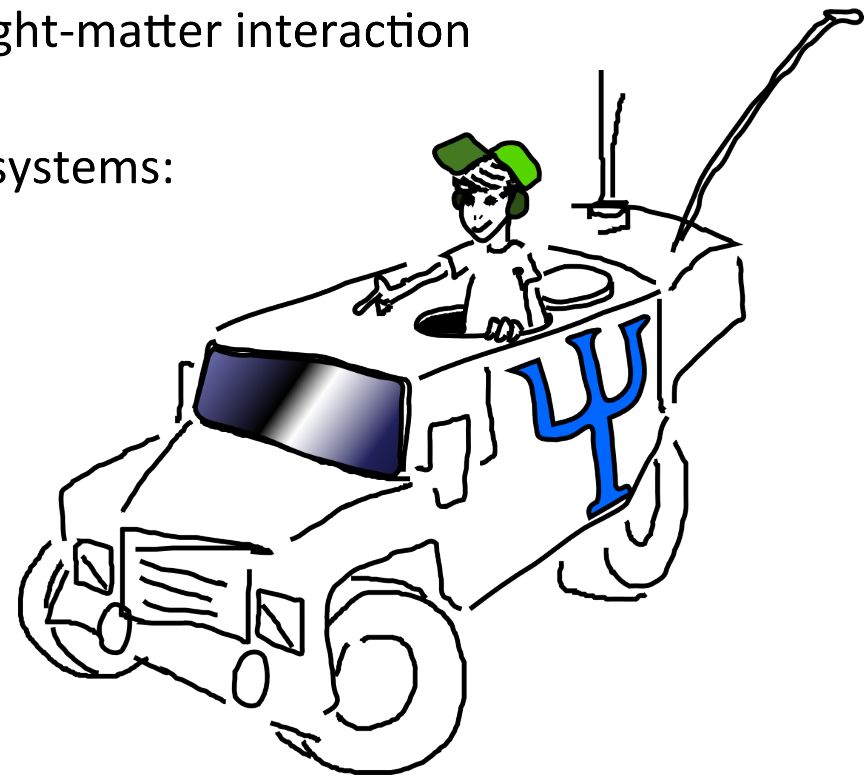
Summary

PART I

- Raman: powerful tool for coherent light-matter interaction
- Entangled 2 diamonds
- Technique applicable to many other systems: (Anything with a Raman line!)

PART II

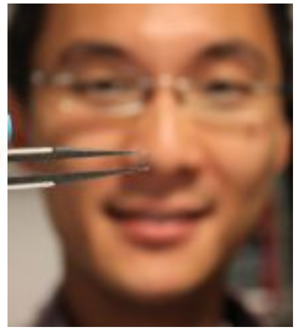
- TFQKD with TFC
- Can encode > 4 bits off-the-shelf
- Analyzed security including binning…



People

Ian Walmsley (Ox)

Michael Sprague



KC Lee

Xian-Min Jin (Ox / Nanjing)

Lijian Zhang (MPSD / Beijing)

Brian Smith (Ox)

Laura Wright

Christoph Söller

Ben Sussman (NRC)

Duncan England

Phil Bustard

Thanks for listening!

CLARENDON FUND

Oxford Physics

NRC·CNRC From Discovery to Innovation...

EPSRC

THE ROYAL SOCIETY

NSERC CRSNG

QESSENCE

FastQuast

SEVENTH FRAMEWORK PROGRAMME

AFOSR AIR FORCE OFFICE OF SCIENTIFIC RESEARCH

CQT Centre for Quantum Technologies