

Title: Towards experimental quantum position verification with true single photons by quantum dot cavity-QED

Speakers: Wolfgang Loeffler

Collection: QPV 2023: Advances in quantum position verification

Date: September 20, 2023 - 4:00 PM

URL: <https://pirsa.org/23090020>

# Towards experimental quantum position verification with true single photons by quantum dot cavity-QED

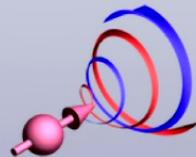
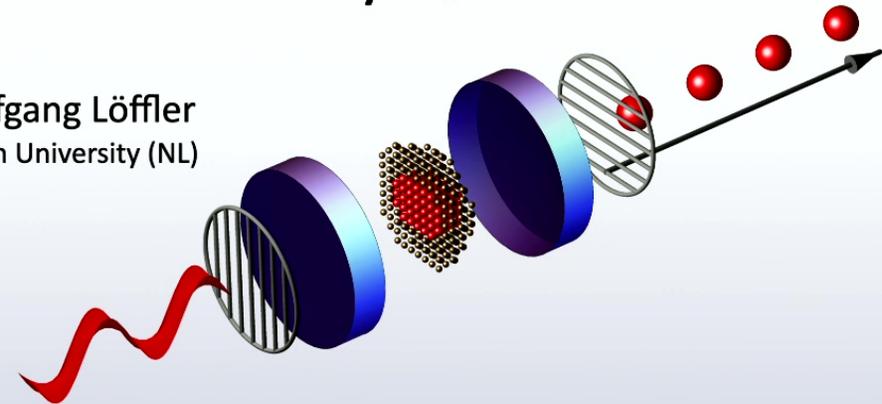
Kirsten Kanneworff  
Mio Poortvliet  
Petr Steindl  
Henk Snijders



Universiteit Leiden



Wolfgang Löffler  
Leiden University (NL)



quphotonics.org

# Towards experimental quantum position verification with true single photons by quantum dot cavity-QED

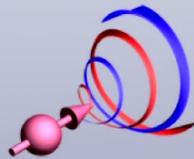
Kirsten Kanneworff  
Mio Poortvliet  
Petr Steindl  
Henk Snijders



Universiteit Leiden

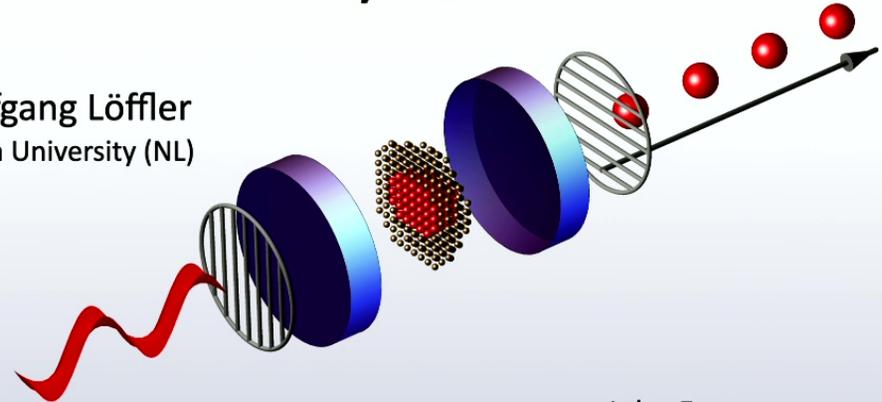


Rene Allerstorfer  
Philip Verduyn Lunel  
Llorenç Escolà Farràs  
Florian Spielman  
Harry Buhrman



quphotronics.org

Wolfgang Löffler  
Leiden University (NL)

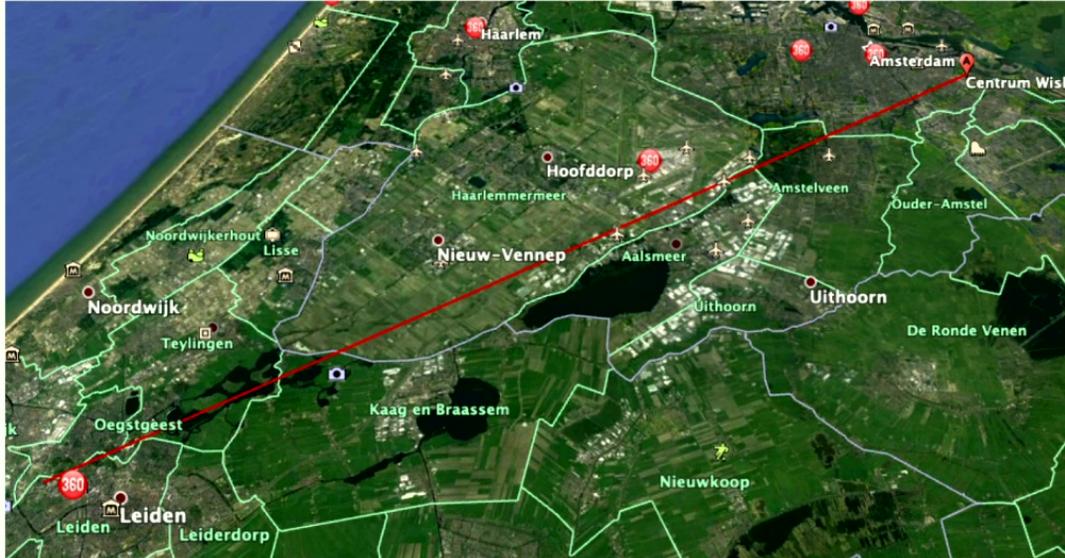


- An experimentalist view on quantum position verification
- Single photon sources
- Two-photon interference
- The QPV demo experiment

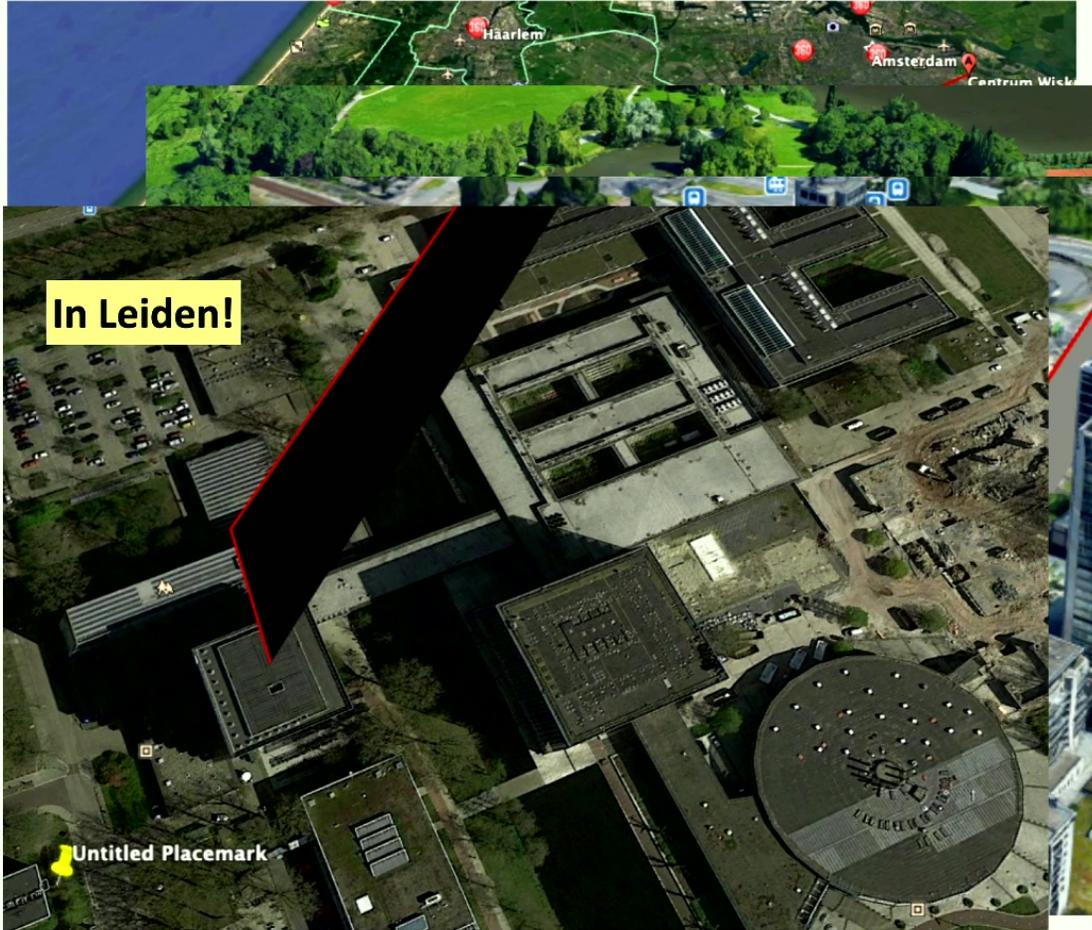
John Frey  
Justin Norman  
Art Gossard  
John Bowers  
Dirk Bouwmeester



# Free-space QKD / QPV in NL (flat)?



# Free-space QKD / QPV in NL (flat)?



QPV2023

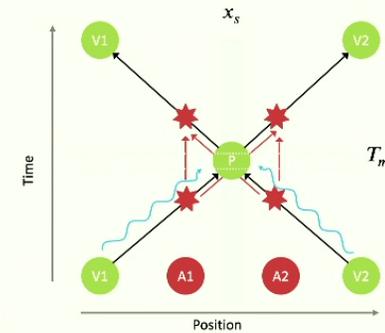
3

Wolfgang Löffler [qphotonics.org](http://qphotonics.org)

# Protocols for a QPV demo

We want to make a demo. About what does an experimentalist care?

Protocol	Message	Prover task	Loss tolerant	Slow quantum
BB84 (Kent, Munro, Spiller, 2011)	1 qubit + 1 cbit	Measure qubit in certain basis	NO	NO
Functional BB84 (Bluhm, Christandl, Speelman, 2021)	1 qubit + 2n cbits	Measure qubit in certain basis	NO	YES
Lim (Lim et al., 2016)	2 qubits	Bell measurement	YES	NO
SWAP (Allerstorfer, Buhrman, Speelman, Verduyn Lunel, 2021)	2 qubits	SWAP test	YES	NO
Functional SWAP	2 qubits + 2n cbits	SWAP test	YES	?
Routing (Bluhm, Christandl, Speelman, 2021)	1 qubit + 2n cbits	qubit routing	NO	NO
Routing with memory	1 qubit + 2n cbits	qubit routing	YES	YES
Reversed Lim (?)	? cbits + Bell pair	send particular Bell state	YES	?



- \* 2 single BB84 qubit photons (a lot)
- \* SWAP test (*really* equal photons)
- \* a lot of infrastructure

# Baseline: quantum states

	Basis	Vector notation	A pure state
Computational basis:	$\{ 0\rangle,  1\rangle\}$	$\left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\}$	$ \Psi\rangle = \alpha 0\rangle + \beta 1\rangle$
Hadamard basis:	$\{ +\rangle,  -\rangle\}$	$\left\{\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}\right\}$	

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

Another equivalent basis?

“Mutually unbiased bases”!  $|\langle e_j | f_k \rangle|^2 = \frac{1}{d}, \quad \forall j, k \in \{1, \dots, d\}$

With orthonormal bases  $e, f: \{|e_1\rangle, \dots, |e_d\rangle\}$

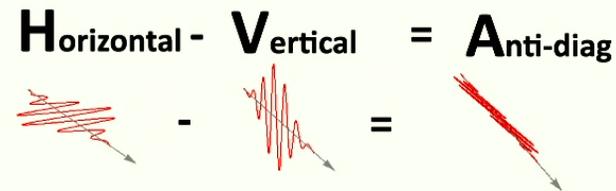
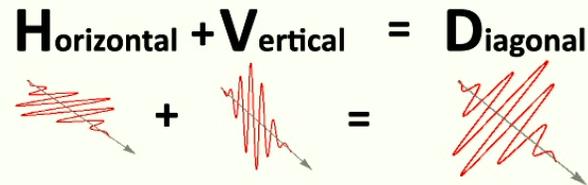
for  $d=2$ : 3rd is complex superposition:

$$|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$$

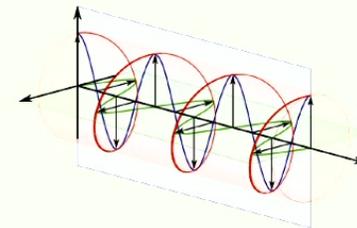
We have  $d+1$  MUBs for  $d$  prime & prime power  
#MUBs unknown already for  $d=6$  !

# Light: polarization qubit

	Basis	Vector notation	Direct physical correspondence:
Linear polarization of photon:	$\{ H\rangle,  V\rangle\}$	$\begin{pmatrix} E_x \\ E_y \end{pmatrix}$	E-field or Jones vector
$ D/A\rangle = \frac{1}{\sqrt{2}} ( H\rangle \pm  V\rangle)$	$\{ D\rangle,  A\rangle\}$	$\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$	

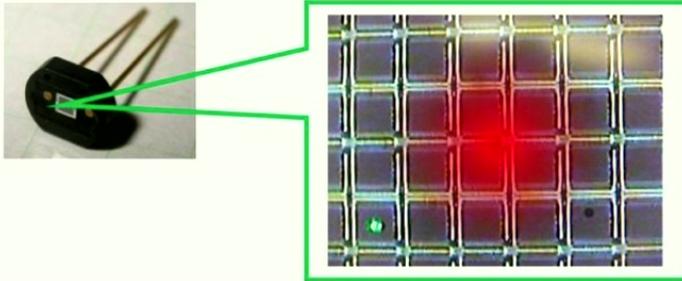


$|\pm i\rangle = \frac{1}{\sqrt{2}} (|0\rangle \pm i|1\rangle)$       **Circular polarization!**

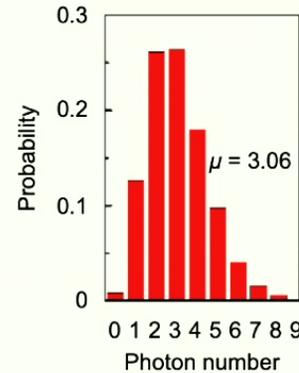


# Single photons <> coherent (laser) light

Laser pulses on photon detector array:



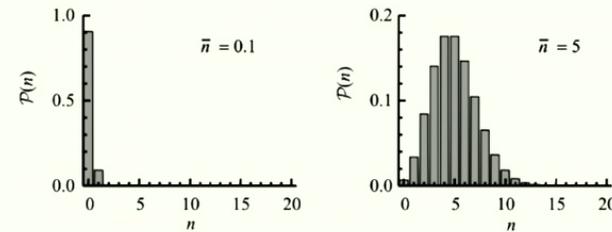
Silicon multi-pixel photon counter (APDs)



JEST 17, 204 (2019)

Probability to detect n photons

Probability to detect n photons in time T follows Poisson distribution



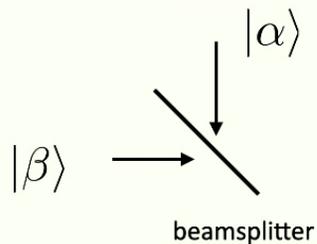
Coherent (laser) light is in coherent state!

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

Infinite quantum superposition of photon number states!

# Single photons from coherent states by linear optics?

## Interference of coherent states?

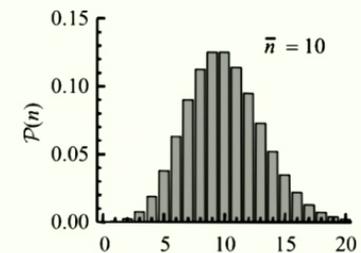
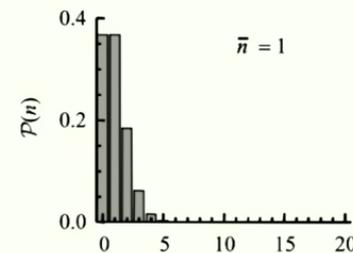
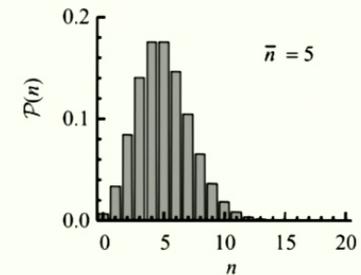
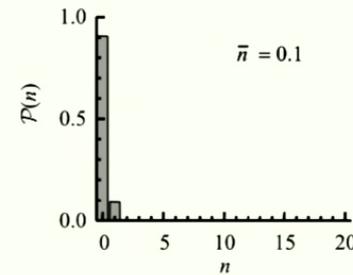


\* Coherent states are not orthogonal

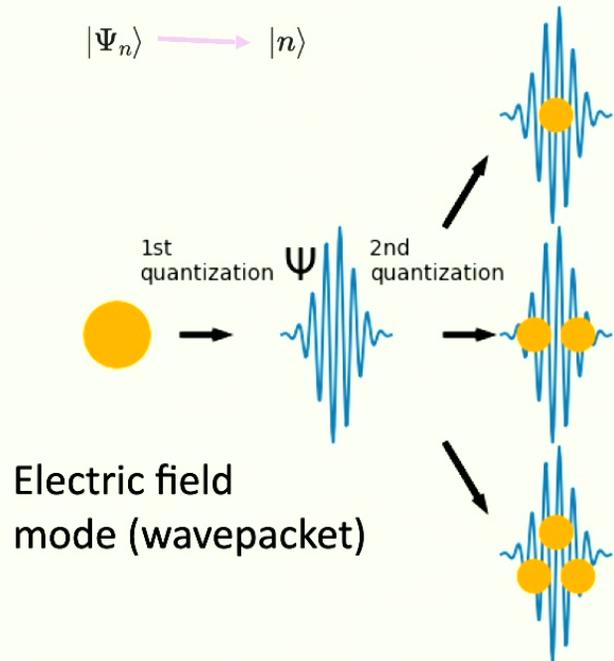
$$|\langle\alpha|\beta\rangle|^2 = \exp(-|\alpha - \beta|^2)$$

\* Sums of normal distributions are again “normal”

With linear optics it is not possible to make coherent states of light non-coherent!



# Photon number states (Fock space)



Ladder operator add or remove photons:

$$a^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle$$

$$a |n\rangle = \sqrt{n} |n-1\rangle$$

The number operator counts photons:

$$N = a^\dagger a$$

$$N |n\rangle = n |n\rangle$$

Warning: different states, different space!

Here we always "have" a qubit:  $|H\rangle, |0\rangle, |1\rangle$

And in Fock space possibly not:  $|n_{\text{state}}\rangle$

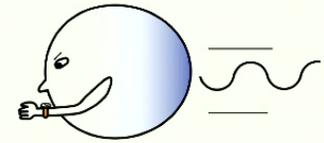
Fun fact: discrimination of "non-orthogonal" states:

$$|\langle 1_R | 1_H \rangle|^2 = 1/2$$

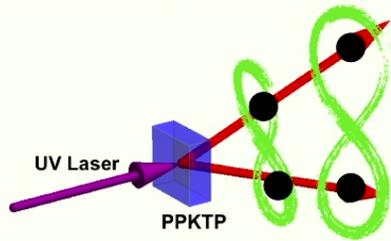
$$|\langle 2_R | 2_H \rangle|^2 = \left| \langle 0 | \frac{1}{\sqrt{2}} \hat{a}_R^2 \cdot \frac{1}{\sqrt{2}} (\hat{a}_H^\dagger)^2 | 0 \rangle \right|^2 = \dots = 1/4$$

# How to make a single photon?

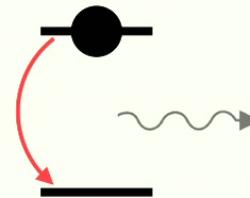
Visible:  $E \approx 1 \text{ eV}$  is large,  $\gg k_B \cdot T$ , so should be easy!?



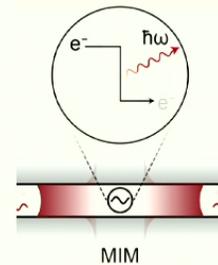
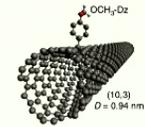
Spontaneous downconversion  
("photon decay") & heralding



Atomic decay

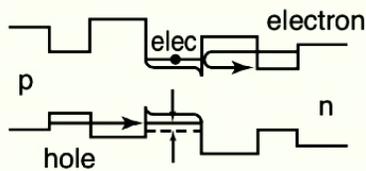


© G.S. Springer, 2010

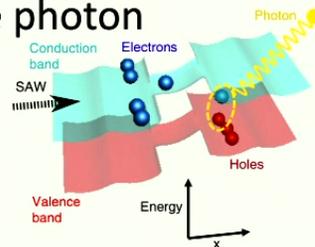


Inelastic electron tunneling

Single-electron  $\rightarrow$  single photon



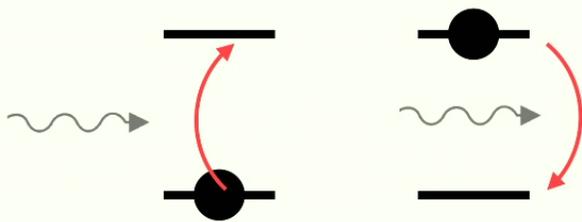
Nature 397, 500 (1999)



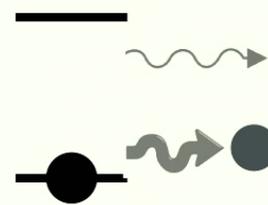
Nat. Commun. 11, 917 (2020)

# How can we make a single photon from a laser?

Excite single two-level system  
(laser light: random # photons)



Single-photon  
emission



Remove excitation  
laser



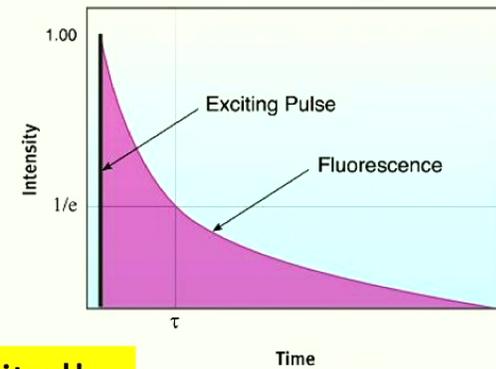
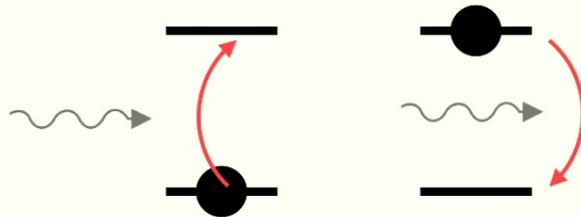
True single photon!

How to remove the excitation laser?

- \* Wavelength filtering: non-resonant excitation
- \* Temporal filtering
- \* Direction: Side-excitation
- \* Polarization filtering: easy using crossed polarizers!

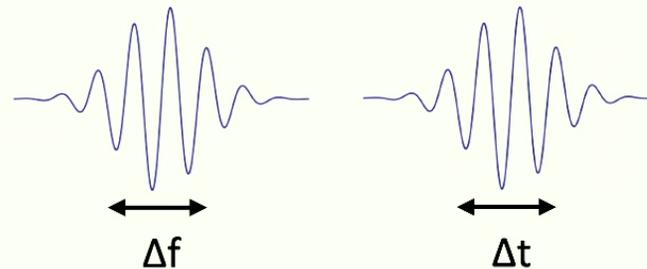
# Single photon wavepackets

Back to excitation of two-level system / atom / quantum dot:



Excitation laser pulse can be very short but decay is lifetime-limited!

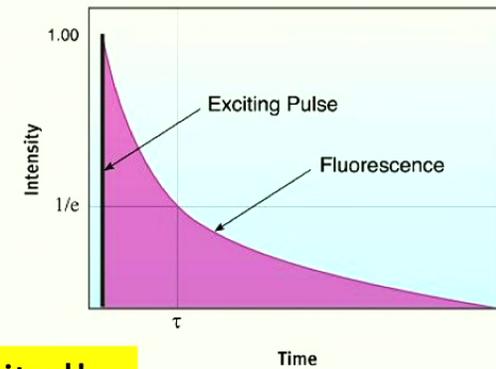
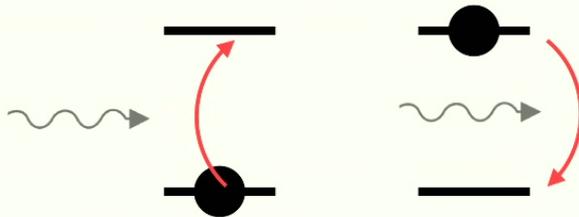
- \* Want high rate (GHz):  $\Delta t < 1$  ns  
btw: nW range!
- \* Also: noise on  $\mu$ s scale



$$\Delta t \cdot \Delta f = 0.44 \text{ (Gaussian envelope)}$$

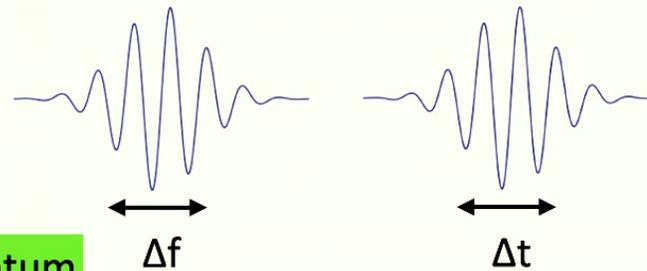
# Single photon wavepackets

Back to excitation of two-level system / atom / quantum dot:



Excitation laser pulse can be very short but decay is lifetime-limited!

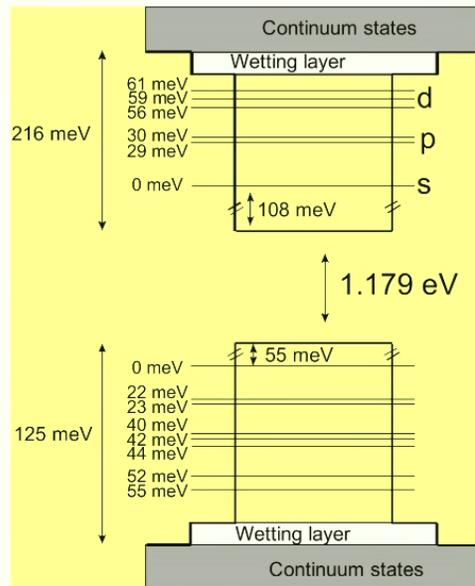
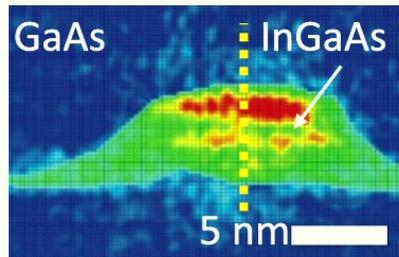
- \* Want high rate (GHz):  $\Delta t < 1$  ns  
btw: nW range!
- \* Also: noise on  $\mu$ s scale



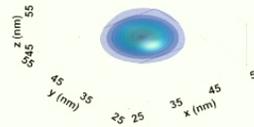
Ideal system: semiconductor quantum dot in optical microcavity

$$\Delta t \cdot \Delta f = 0.44 \text{ (Gaussian envelope)}$$

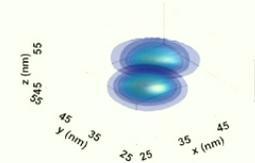
# Semiconductor quantum dots (self-assembled)



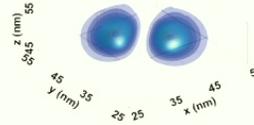
s-like



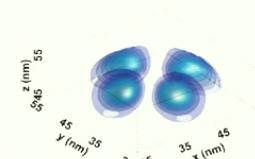
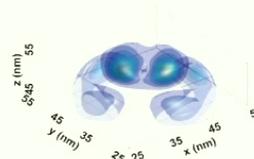
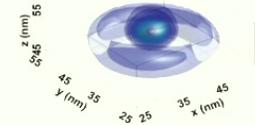
p-like



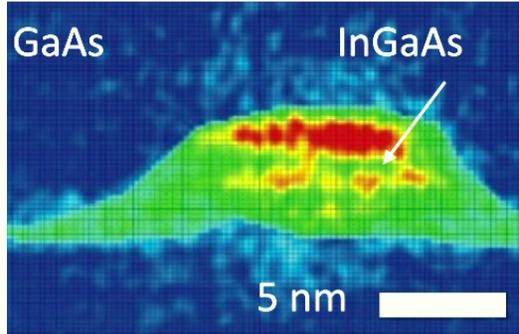
p-like



p-like



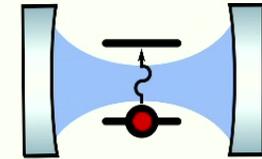
# Quantum dots: efficient interaction with light



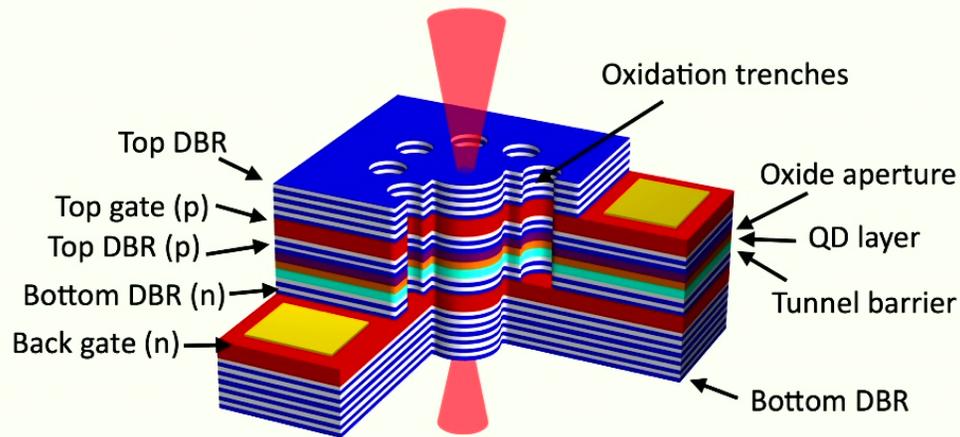
Efficient interaction

$$\underbrace{\frac{3\lambda^2}{2\pi}}_{\sigma_{\text{abs}}} \times \underbrace{\frac{\mathcal{F}}{\pi}}_{\text{bounces}} \gg \underbrace{\frac{\pi}{4} w_0^2}_{\text{beam area}}$$

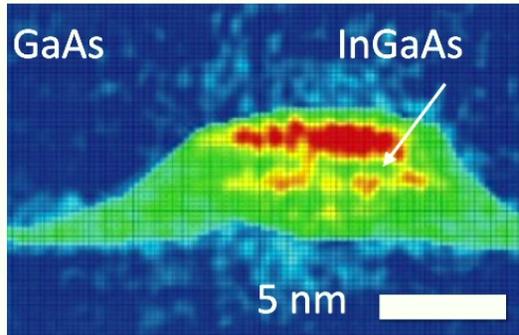
Reiserer & Rempe, Rev. Mod. Phys. 87, 1379 (2015)



Cooperativity  $C = \frac{g^2}{2\kappa\gamma} \gg 1$



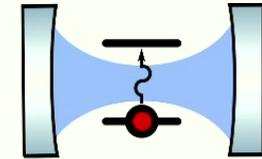
# Quantum dots: efficient interaction with light



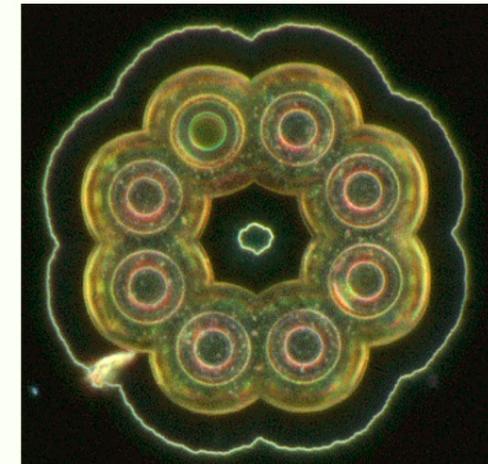
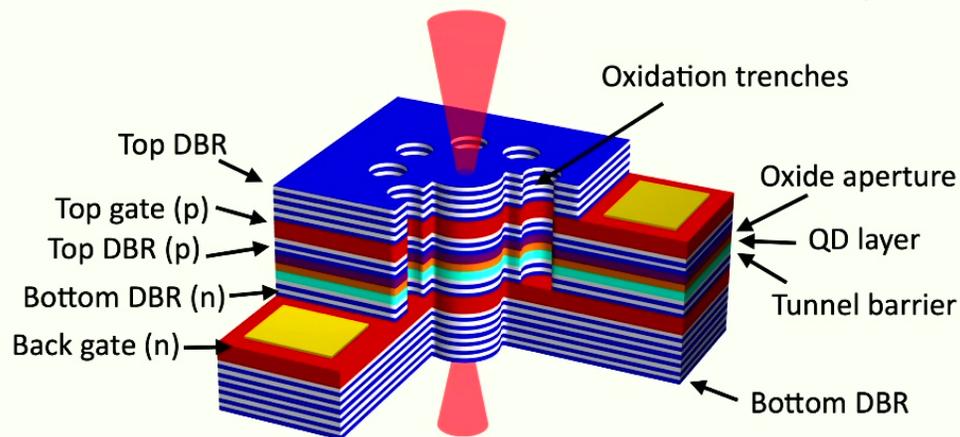
Efficient interaction

$$\underbrace{\frac{3\lambda^2}{2\pi}}_{\sigma_{\text{abs}}} \times \underbrace{\frac{\mathcal{F}}{\pi}}_{\text{bounces}} \gg \underbrace{\frac{\pi}{4} w_0^2}_{\text{beam area}}$$

Reiserer & Rempe, Rev. Mod. Phys. 87, 1379 (2015)

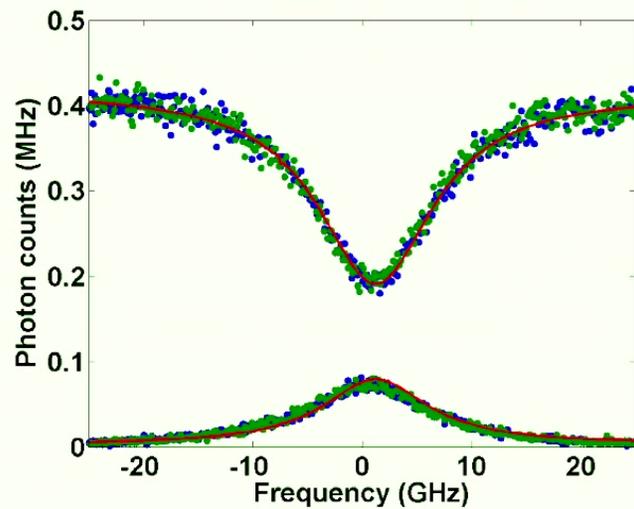


Cooperativity  $C = \frac{g^2}{2\kappa\gamma} \gg 1$



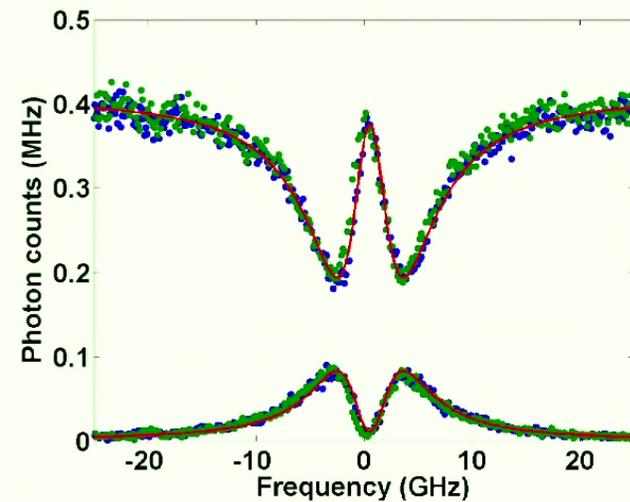
# Efficient interaction with light: cavities

Quantum dot in optical micro-cavity:



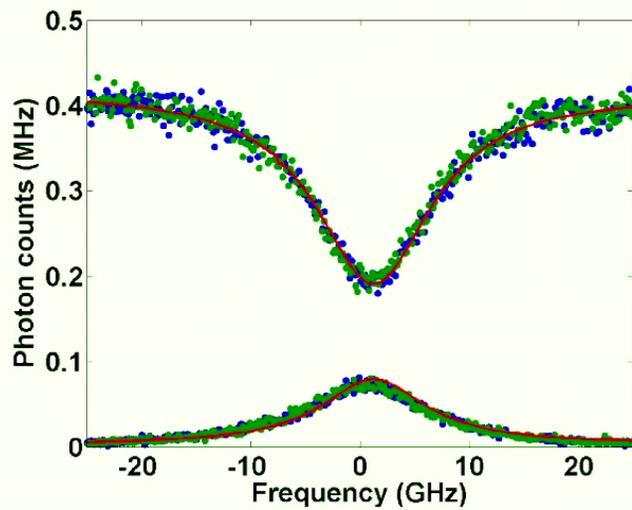
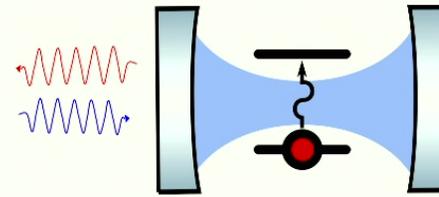
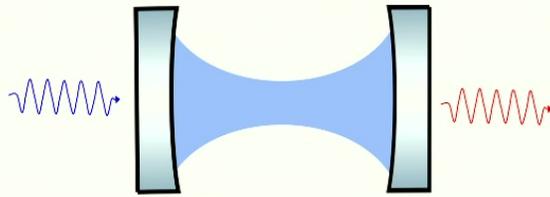
← Reflection

← Transmission



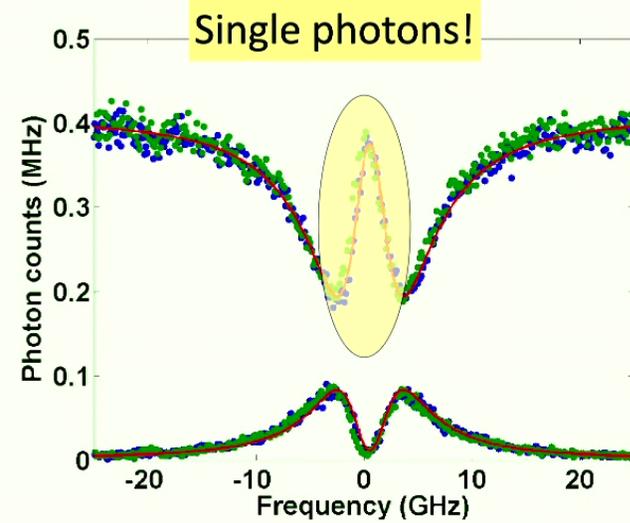
# Efficient interaction with light: cavities

Quantum dot in optical micro-cavity:

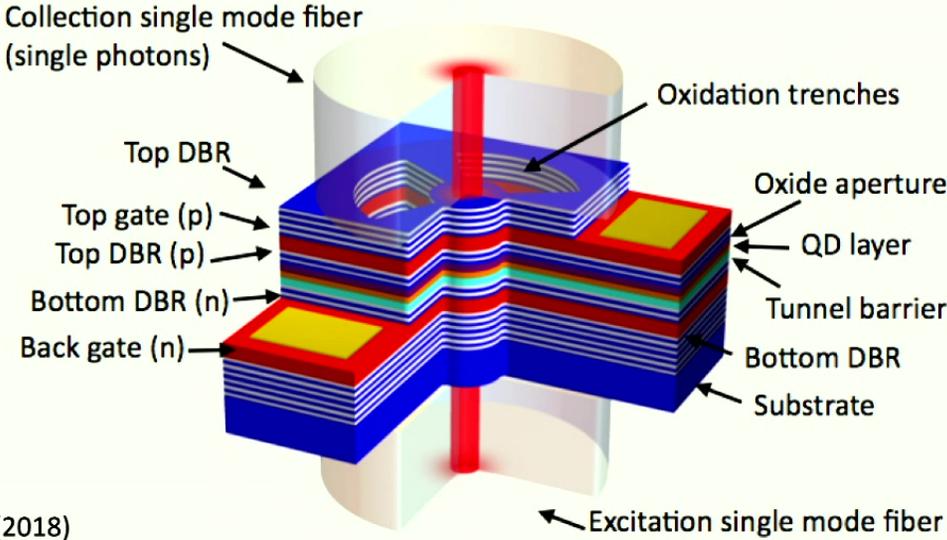
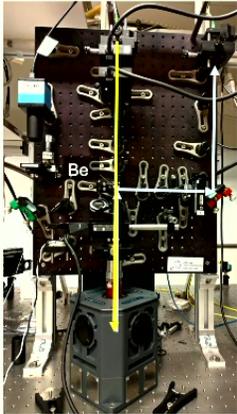
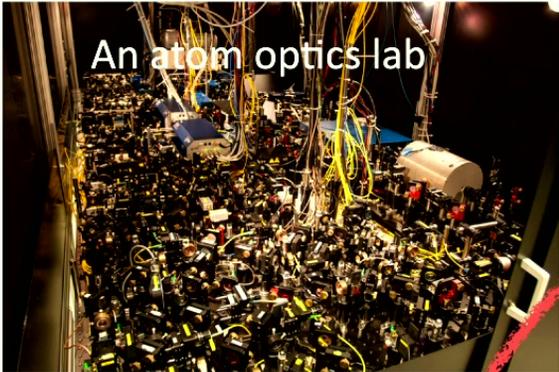


← Reflection

← Transmission



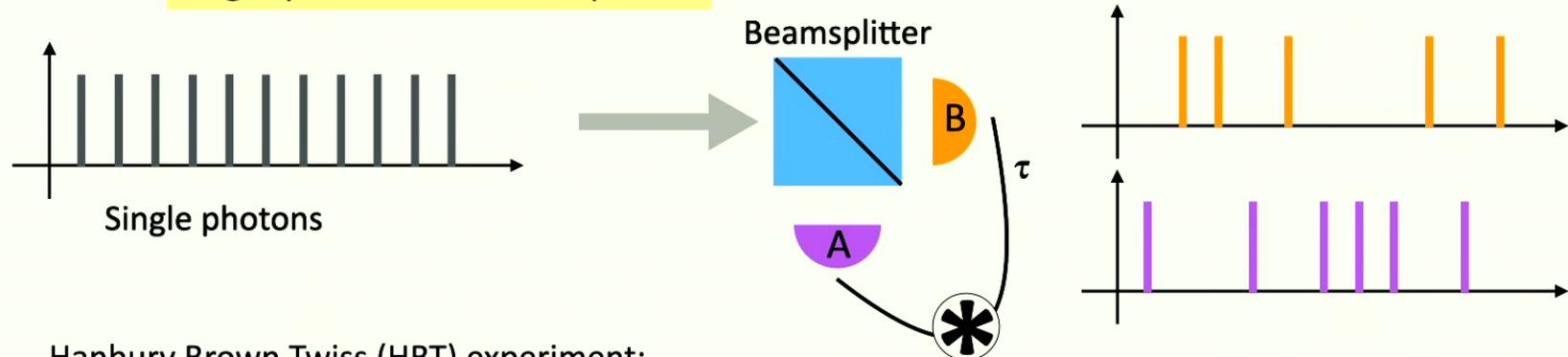
# Fiber integration possible!



Snijders et al., Phys. Rev. Applied 9, 031002 (2018)

# Quality of single photons: “purity”

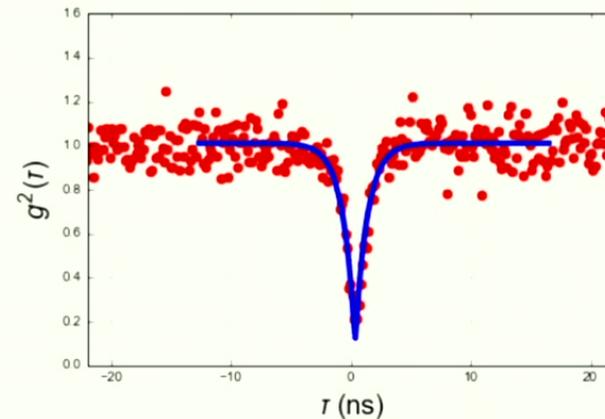
## Single photons & beamsplitter:



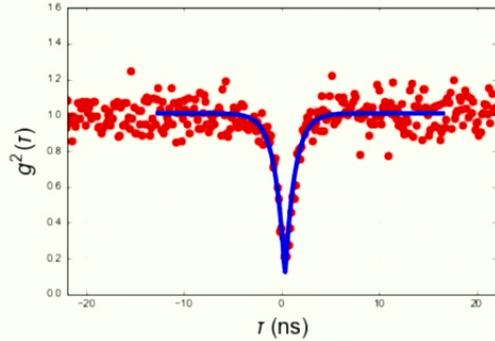
Hanbury Brown Twiss (HBT) experiment:

2nd-order correlation function:  
(photon/intensity = field<sup>2</sup>)

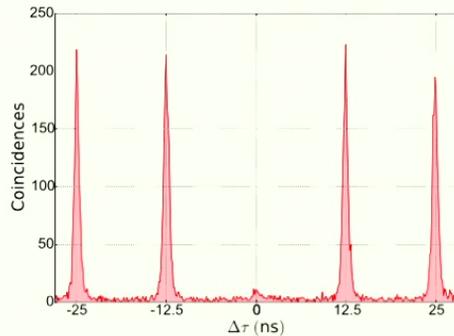
$$g^{(2)}(\tau) = \frac{\langle n_A(t)n_B(t + \tau) \rangle}{\langle n_A(t) \rangle \langle n_B(t + \tau) \rangle}$$



# Quality of single photons: “purity”



**With pulsed laser:**  
 Detector resolution irrelevant!  
 97% purity =  $1 - P(n > 1)$  [ $P(0) = 0$ ]



$g^2(0)$

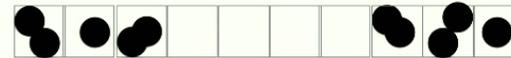
=1

Coherent light: random statistics!



Bunched light:

>1



Antibunched light:

0

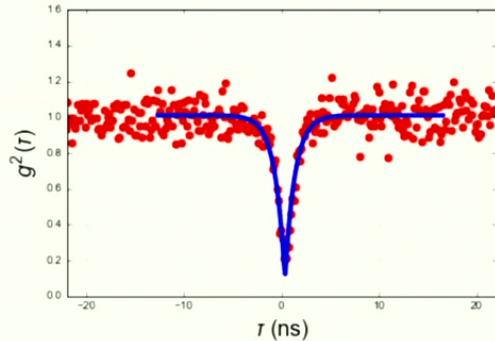


Antibunched light (loss):

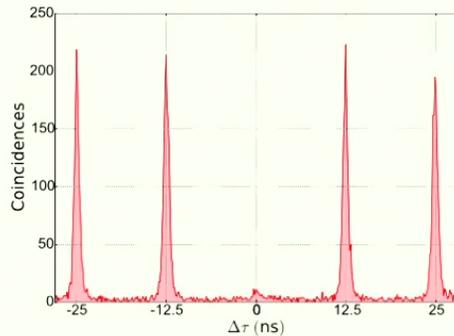
0



# Quality of single photons: “purity”



**With pulsed laser:**  
 Detector resolution irrelevant!  
 97% purity =  $1 - P(n > 1)$  [ $P(0) = 0$ ]



$g^2(0)$

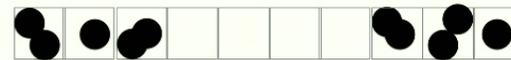
=1

Coherent light: random statistics!



>1

Bunched light:



0

Antibunched light:



0

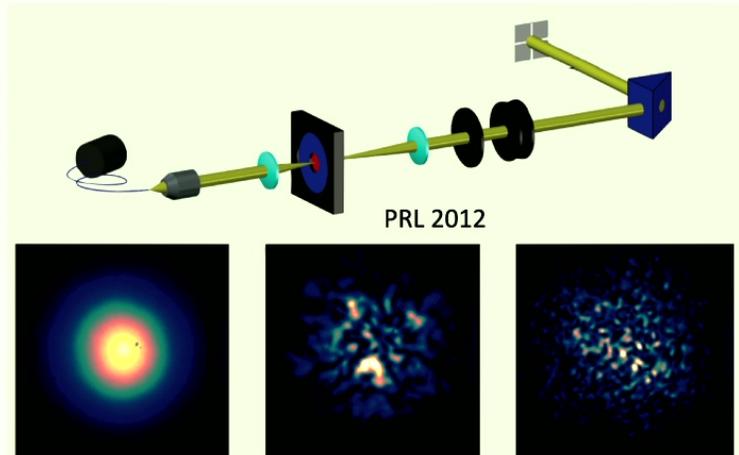
Antibunched light (loss):



**Single photon brightness:**  
 probability of photon in each time bin

# Free-space optical links

Atmospheric turbulence: diffraction, multi-mode, up to few kH



Turbulence in atmosphere:  
10 km thick. 30km max.



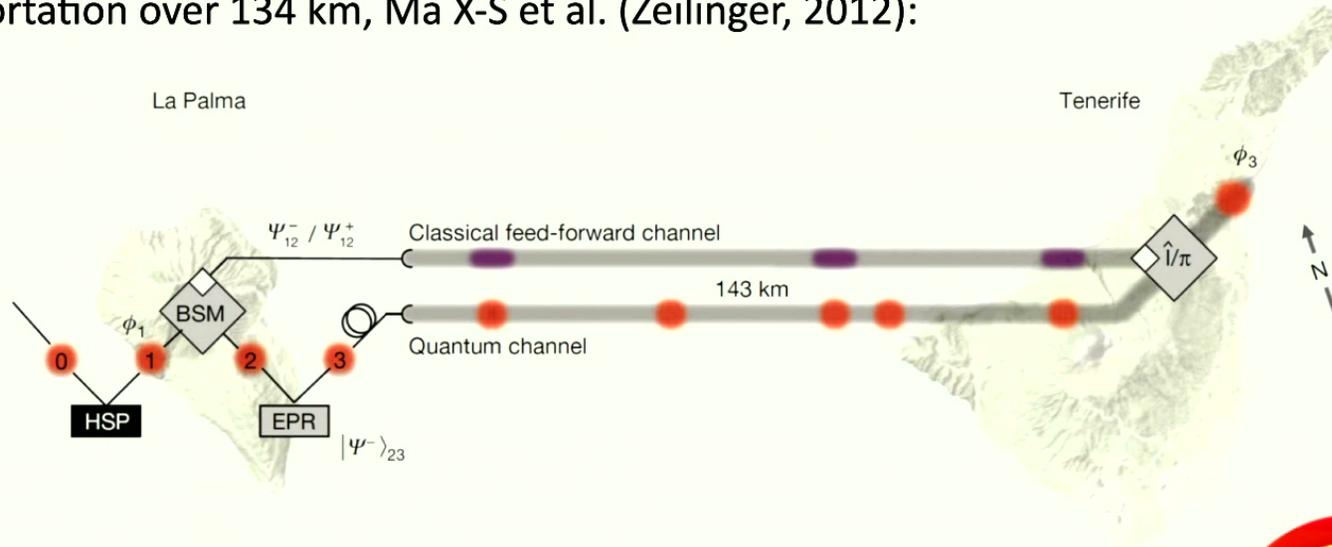
Satellite-based entanglement distribution over  
1200 kilometers

● Juan Yin<sup>1,2</sup>, Yuan Cao<sup>1,2</sup>, Yu-Huai Li<sup>1,2</sup>, Sheng-Kai Liao<sup>1,2</sup>, ● Liang Zhang<sup>2,3</sup>, Ji-Gang Ren<sup>1,2</sup>, Wen-Qi Cai<sup>1,2</sup>, ...

JW Pan 2017

# Free-space optical links

Teleportation over 134 km, Ma X-S et al. (Zeilinger, 2012):



much less turbulences at 2.4 km altitude...

Let's start with fibers



# Fiber transport: photon loss

$\alpha$  : attenuation coefficient

Lambert Beer absorption:

$$P_i/P_o = \exp(-\alpha L)$$

Fiber optics: dB (base-10):

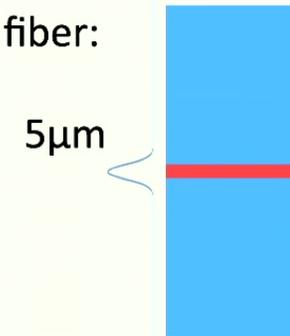
$$P_i/P_o = 10^{-\alpha L/10}$$

transmission after:	5 km	50 km	100 km	300 km
900 nm: 3 dB/km	0.03	$10^{-15}$	$10^{-30}$	$10^{-90}$
1550 nm: 0.2 dB/km	0.8	0.1	0.01	$10^{-6}$
0.16 dB/km	0.83	0.15	0.03	$2 \cdot 10^{-5}$

Single-mode optical fiber:

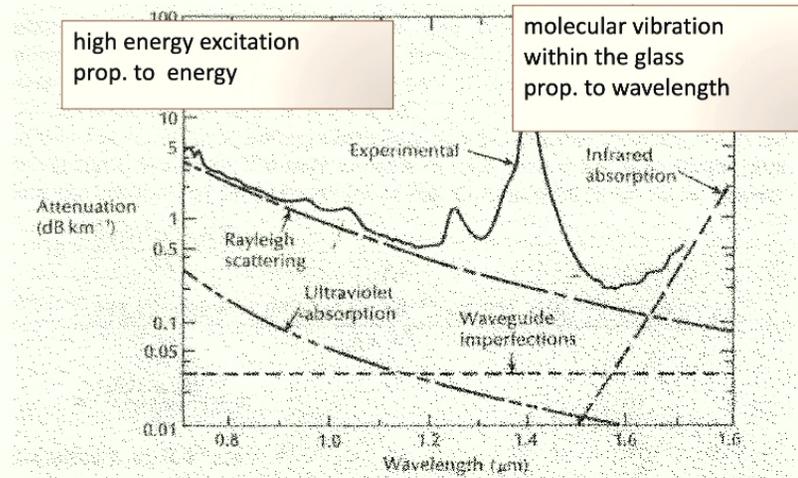
\* amorphous SiO<sub>2</sub>

\* thick cladding

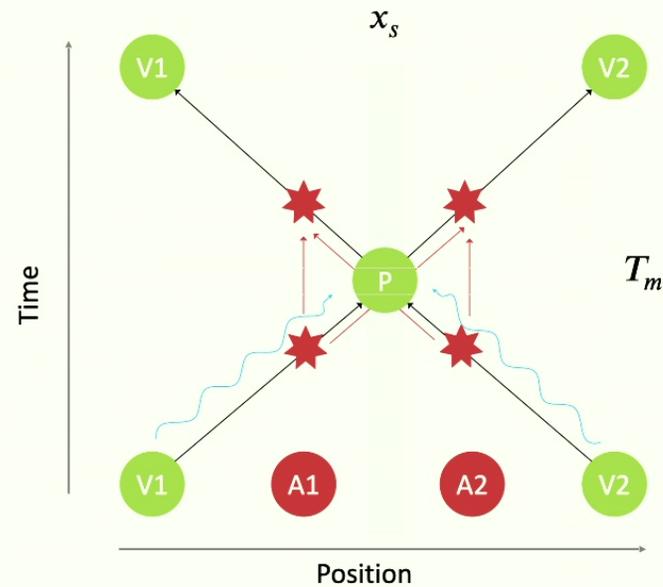


3 dB loss = 50%

125 μm



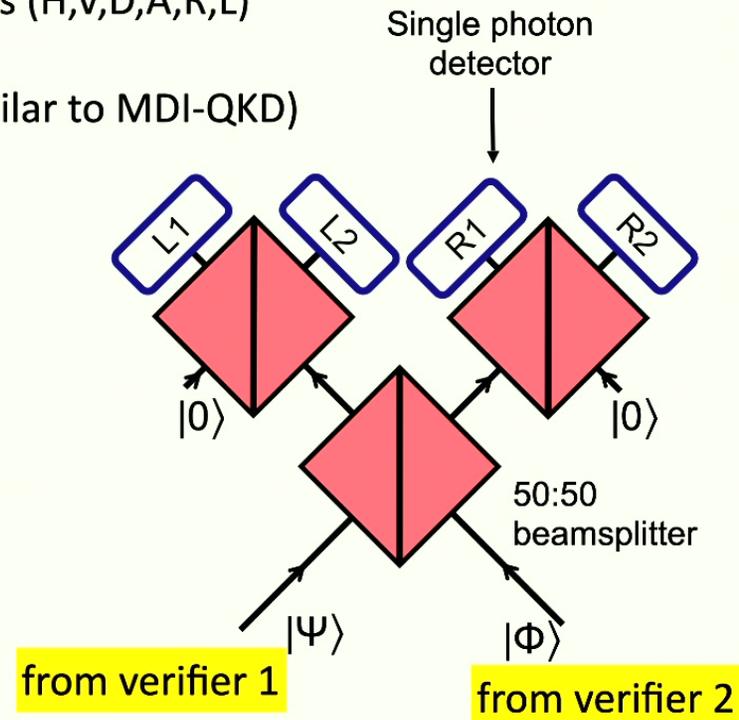
# QPV & loss



Must prevent “loss loophole”:  
Attackers intercept & measure in random basis, claim loss if this was wrong basis  
=> Two-photon interference: no basis chosen!

# QPV: swap protocol

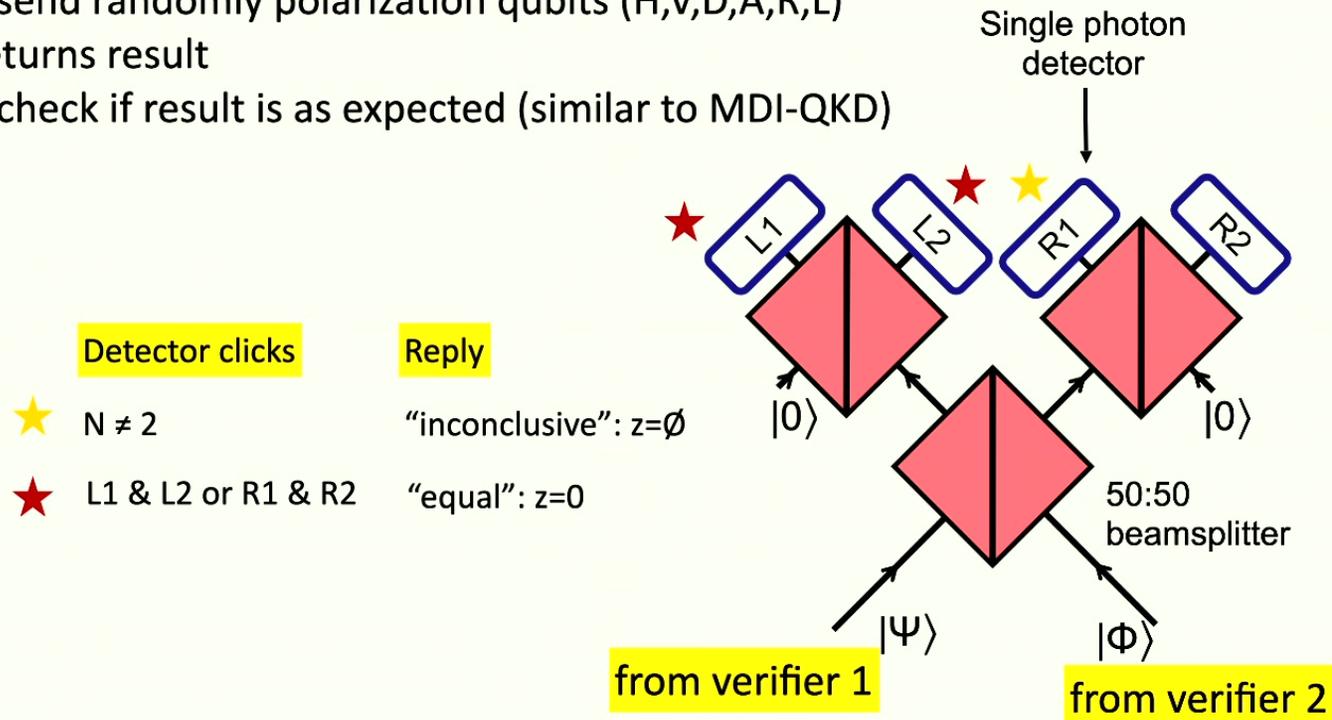
1. Verifiers send randomly polarization qubits (H,V,D,A,R,L)
2. Prover returns result
3. Verifiers check if result is as expected (similar to MDI-QKD)



Allerstorfer, Buhrman, Speelman, Verduyn Lunel,  
New Protocols and Ideas for Practical Quantum Position Verification, ArXiv:2106.12911

# QPV: swap protocol

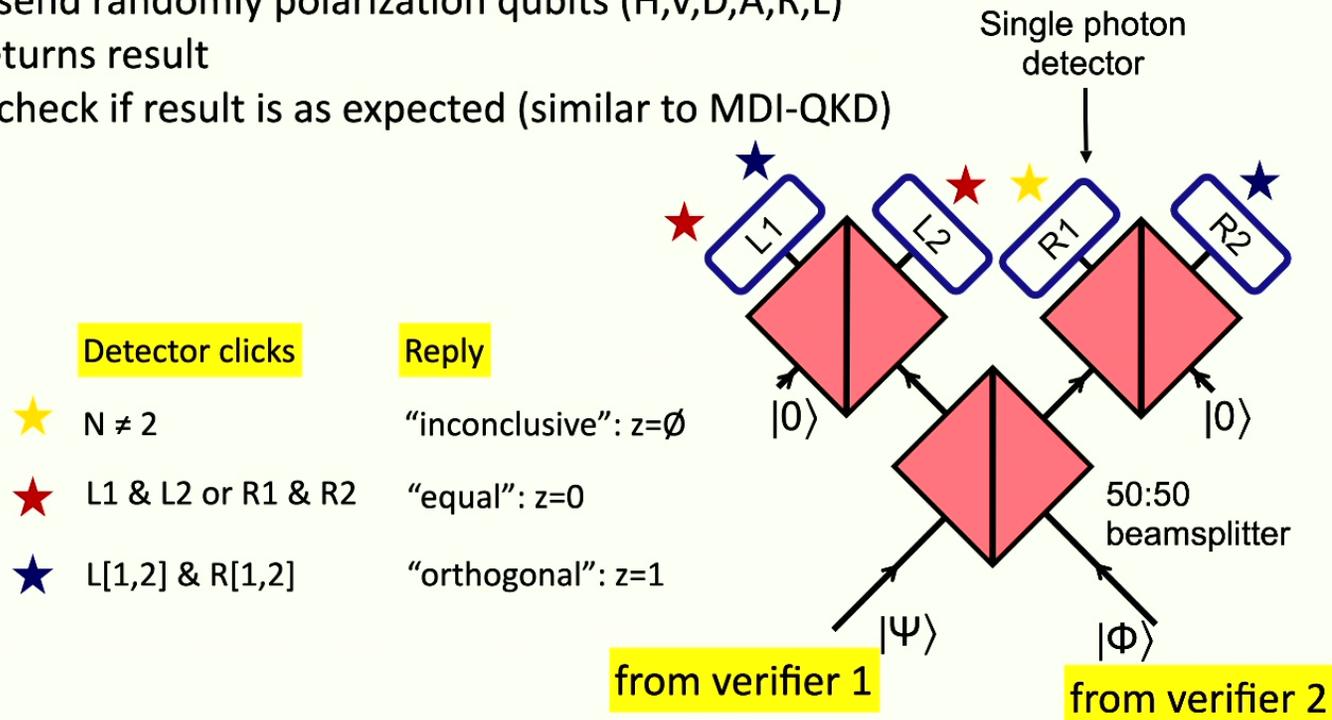
1. Verifiers send randomly polarization qubits (H,V,D,A,R,L)
2. Prover returns result
3. Verifiers check if result is as expected (similar to MDI-QKD)



Allerstorfer, Buhrman, Speelman, Verduyn Lunel,  
 New Protocols and Ideas for Practical Quantum Position Verification, ArXiv:2106.12911

# QPV: swap protocol

1. Verifiers send randomly polarization qubits (H,V,D,A,R,L)
2. Prover returns result
3. Verifiers check if result is as expected (similar to MDI-QKD)



Allerstorfer, Buhrman, Speelman, Verduyn Lunel,  
 New Protocols and Ideas for Practical Quantum Position Verification, ArXiv:2106.12911

# SWAP test for photon equality: Hong-Ou Mandel interference

Symmetric convention:

$$r = i/\sqrt{2} \quad t = 1/\sqrt{2}$$

$$\hat{a}_1^\dagger \rightarrow \frac{\hat{a}_3^\dagger + i\hat{a}_4^\dagger}{\sqrt{2}} \quad \hat{a}_2^\dagger \rightarrow \frac{\hat{a}_4^\dagger + i\hat{a}_3^\dagger}{\sqrt{2}}$$

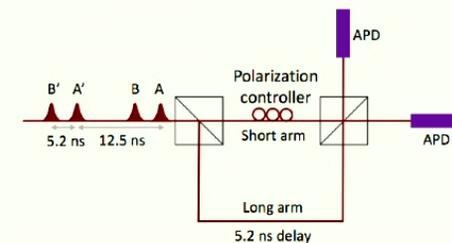
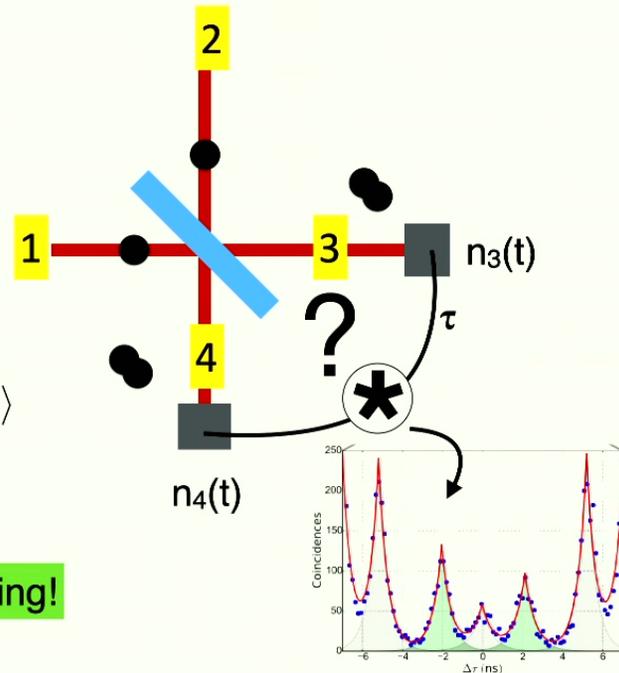
Input:  $|1, 1\rangle_{1,2} = \hat{a}_1^\dagger \hat{a}_2^\dagger |0, 0\rangle_{1,2}$

BS  $\rightarrow \frac{1}{2} (a_3^\dagger + ia_4^\dagger) (a_4^\dagger + ia_3^\dagger) |0_3 0_4\rangle$

$$= \frac{1}{2} (ia_3^\dagger a_3^\dagger - a_4^\dagger a_3^\dagger + a_3^\dagger a_4^\dagger + ia_4^\dagger a_4^\dagger) |0_3 0_4\rangle$$

$$= \frac{i}{\sqrt{2}} (|2_3 0_4\rangle + |0_3 2_4\rangle) \quad \text{Photon bunching!}$$

What if photons are not equal?  
 $\Rightarrow$  no quantum interference,  
 photons are again "beads"!



# Single photon source figures of merit

## Single photon brightness $B$

- > photon counting
- \* collection efficiency
- \* emitter properties

## Single-photon purity $1-g^{(2)}(0)$

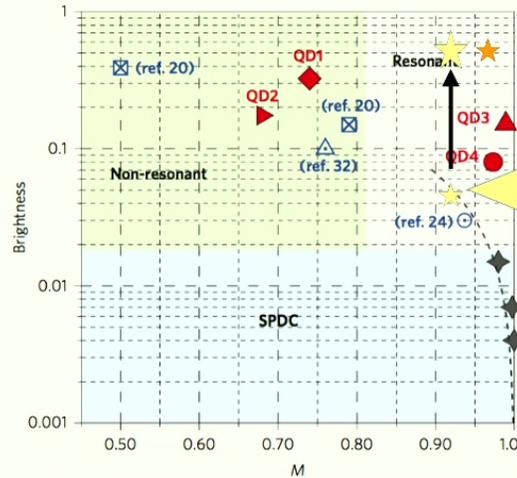
- > HBT measurement
- \* emitter properties
- \* re-excitation
- \* excitation laser filtering

## Indistinguishability $M$

- > Hong-Ou-Mandel interference
- \* spectral stability of emitter
- \* lifetime-limited wavepacket

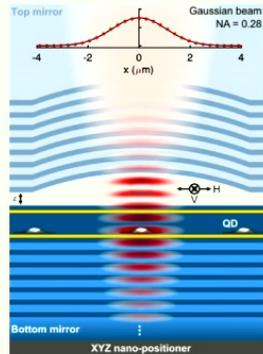
## Maximum photon rate

- \* emitter lifetime
- \* "quietness" of material



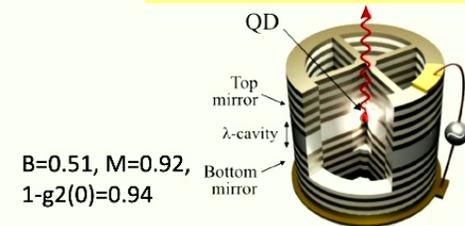
Our single photon source:  
 97% purity  
 90% indistinguishability  
 5% brightness (in-fiber, limited by material absorption  $\rightarrow$  ~35%)  
 ~100 ps wavepacket length (lifetime limited)

Tomm, ..., Warburton, Nat. Nano. 2021 ★



$B=0.65$ ,  $M=0.97$   
 $1-g^{(2)}(0)=0.98$

Thomas, ..., Senellart, PRL 2021



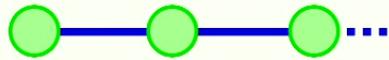
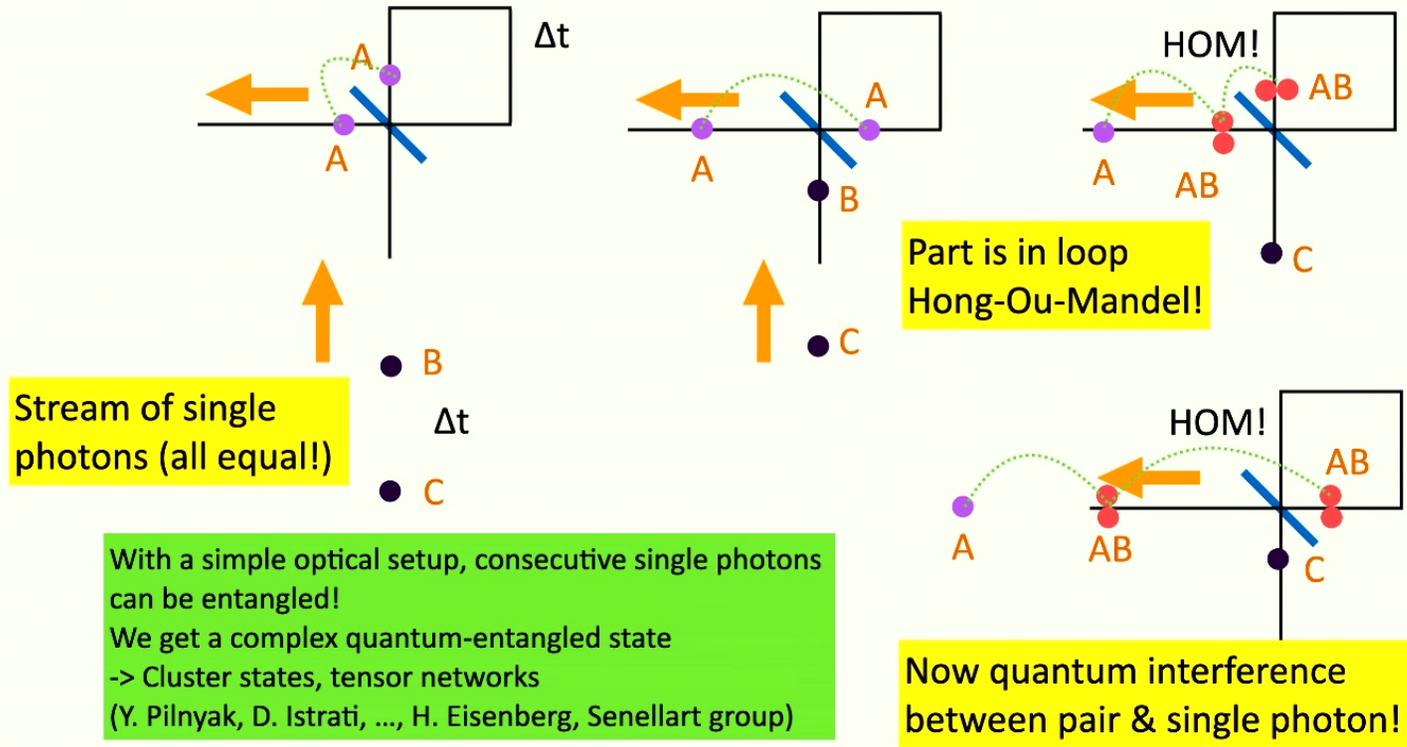
$B=0.51$ ,  $M=0.92$ ,  
 $1-g^{(2)}(0)=0.94$

Luckily, both are with us in



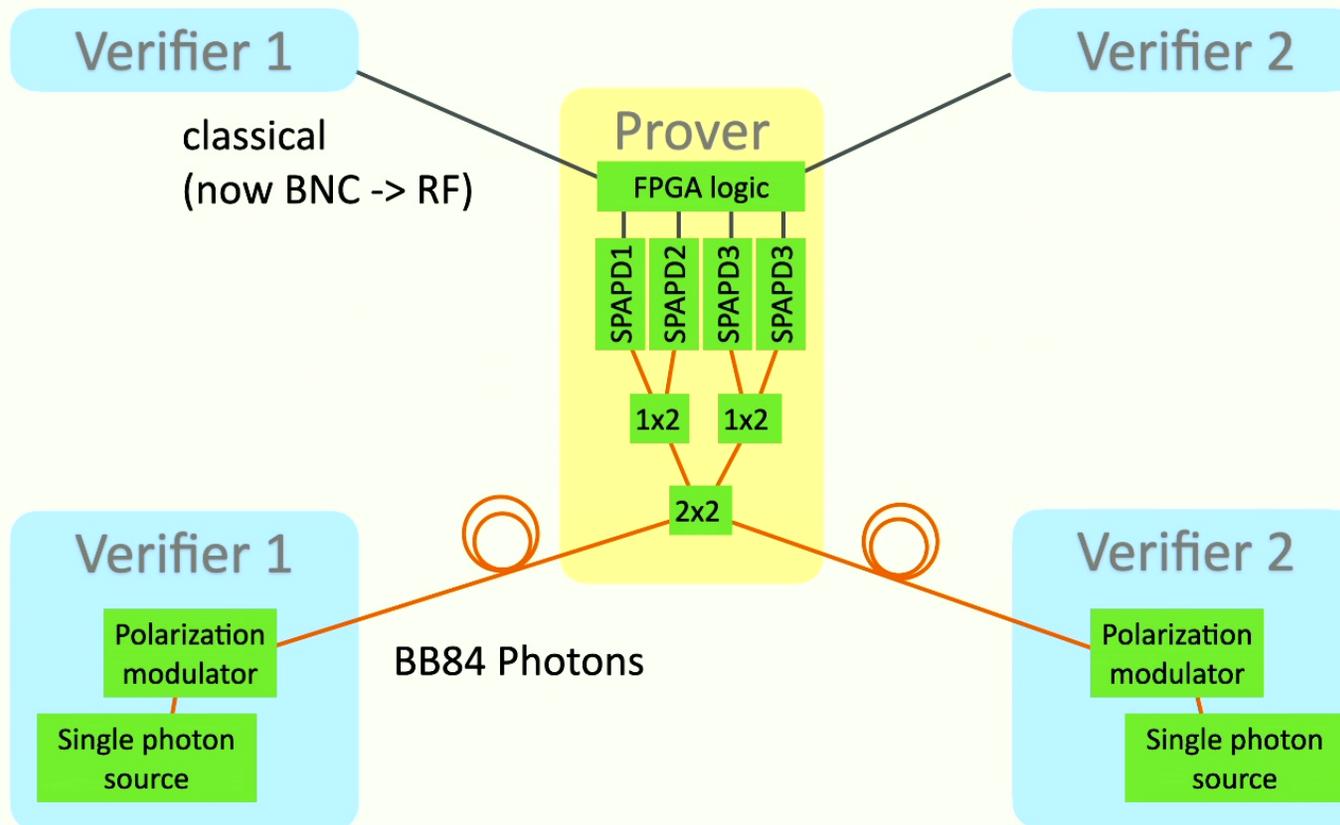
# Intermezzo: Delay loop quantum optics

Delay loop -> quantum memory & HOM interference: photon entanglement



Steindl et al., PRL 126, 143601 (2021)

# Our QPV demo experiment



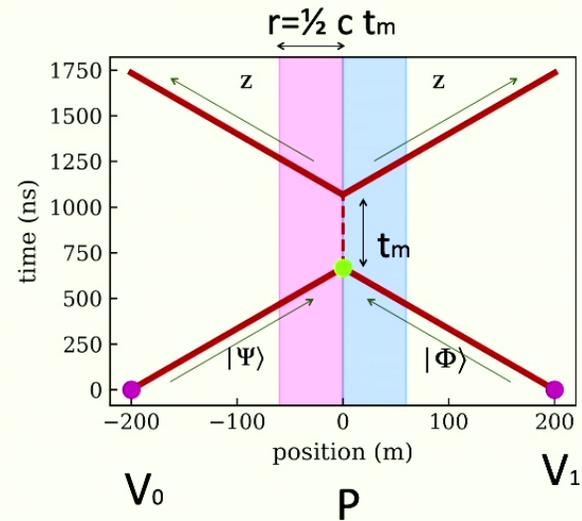
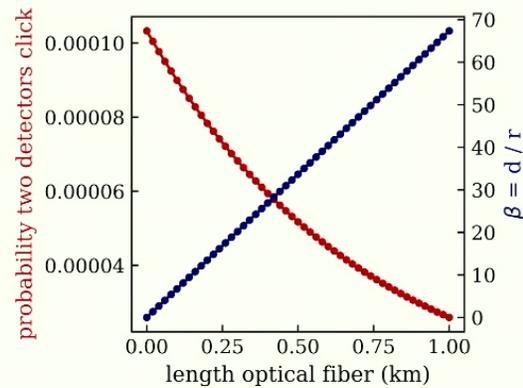
# Slow measurement & slow photons

Nonzero measurement time  $t_m$  leads to “unsafe radius”  $r$  around prover

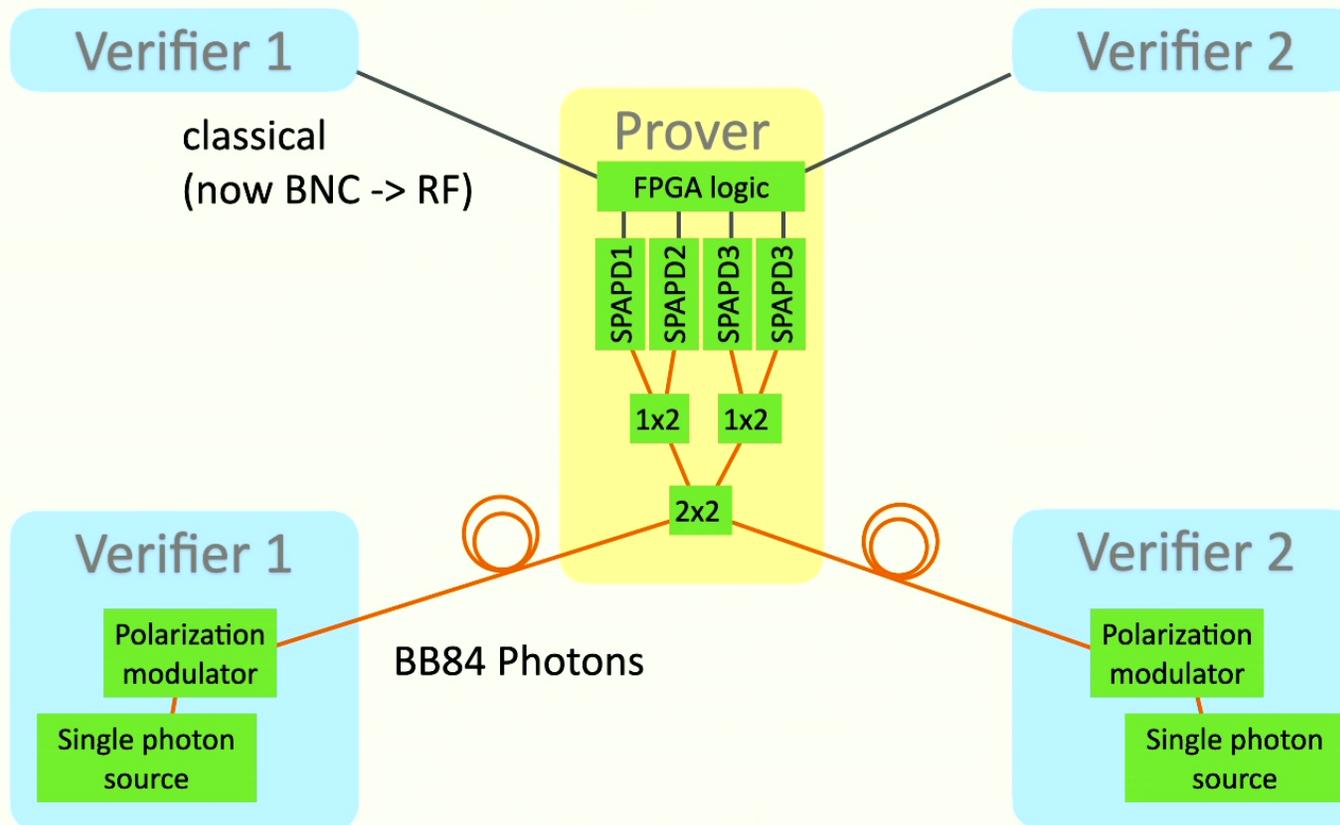


can be solved:  
fence  
== “safe space”!

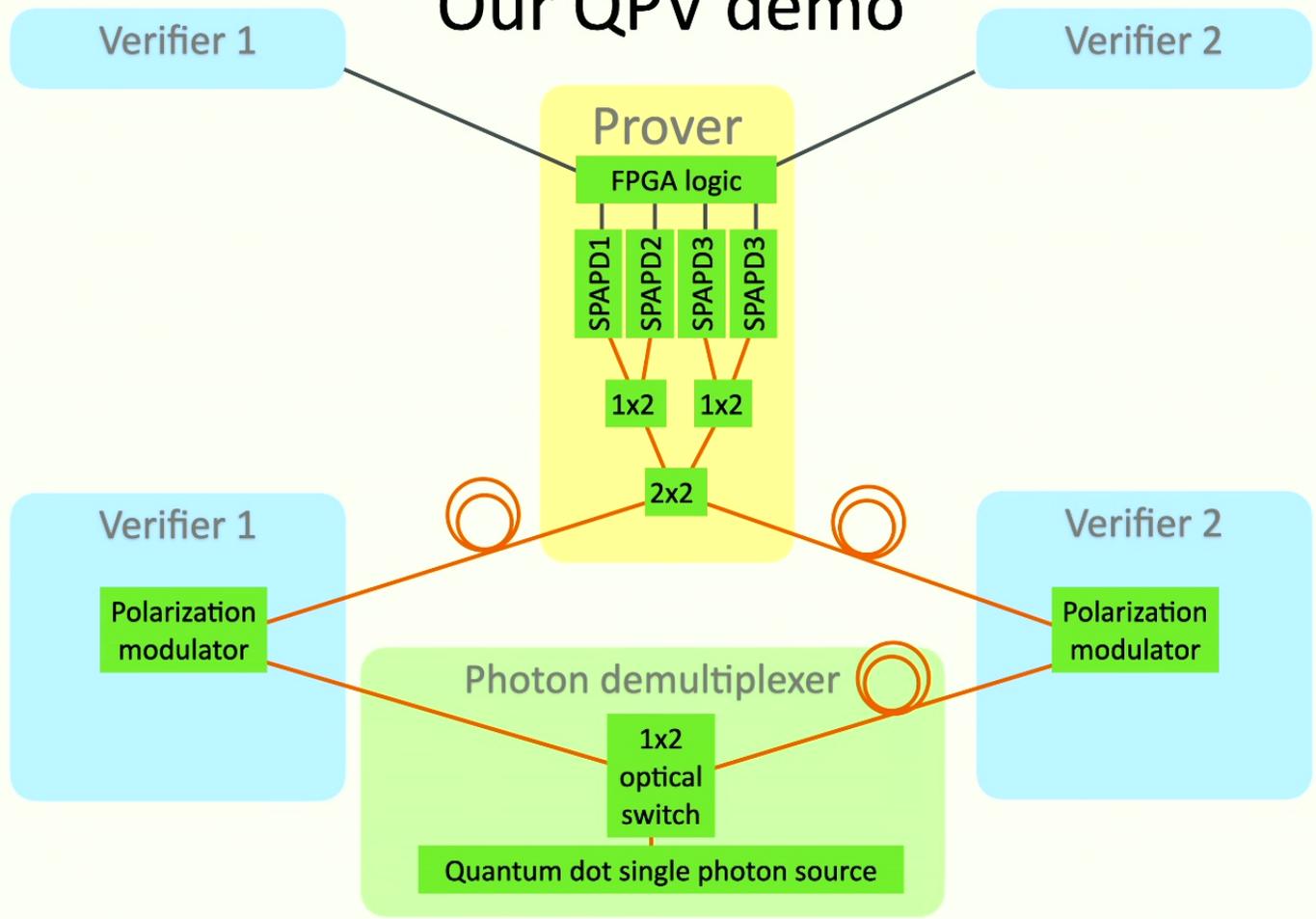
“safe space” should be small compared to channel distance  $r \ll d \rightarrow \beta = d/r$  small



# Our QPV demo experiment

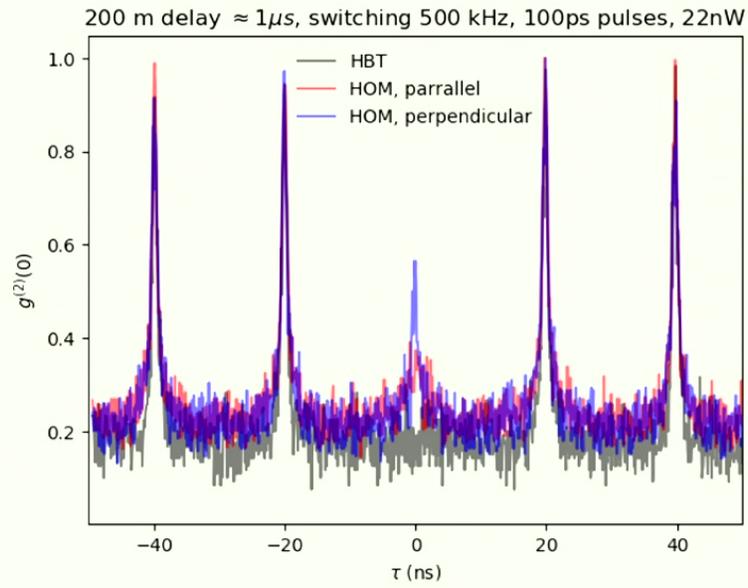


# Our QPV demo

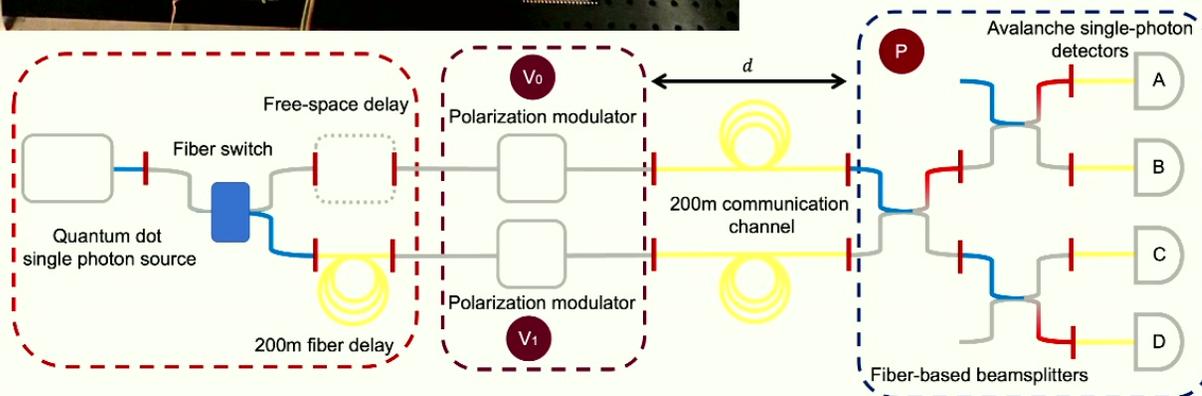
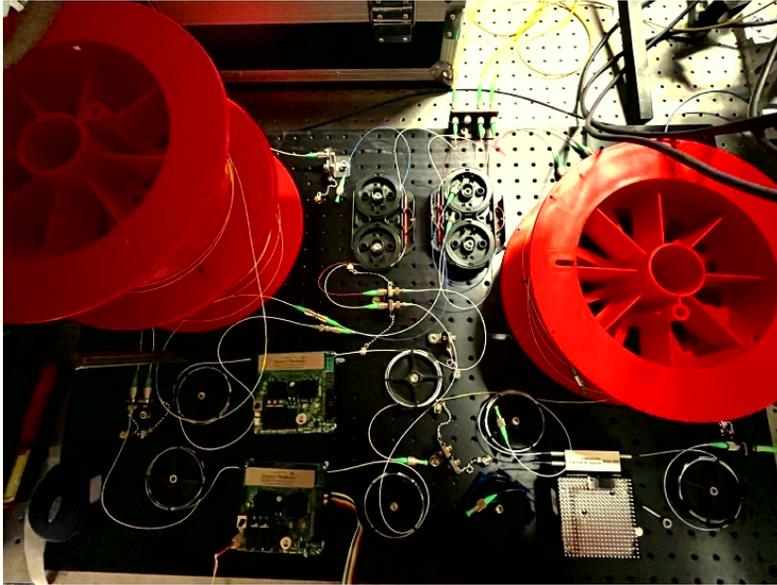


# Photon indistinguishability $1\mu\text{s}$

$1\mu\text{s}$  = photons produced around 1000 lifetimes apart!

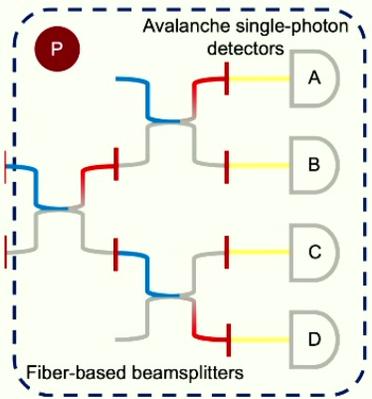
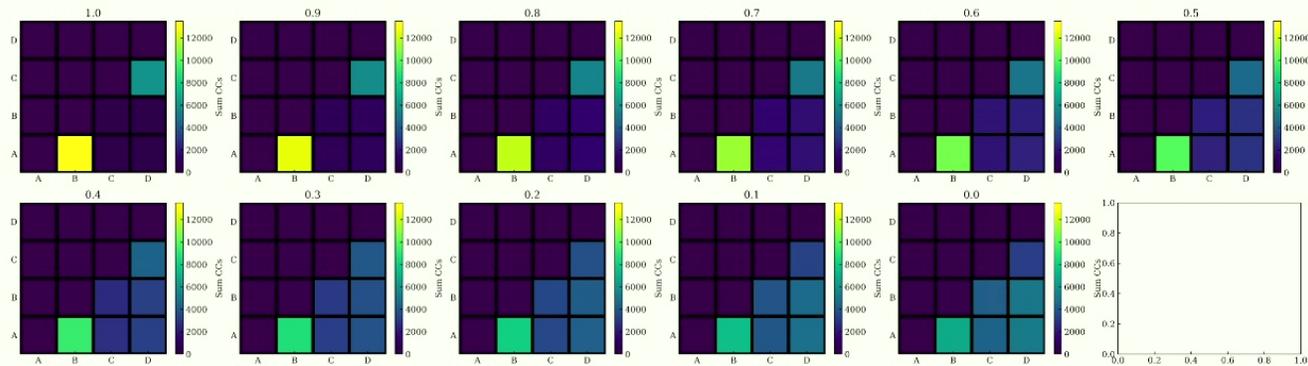


# Our QPV demo

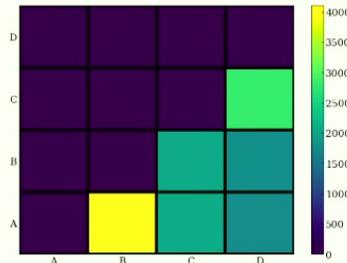


# Last week's results

Calculation for different photon indistinguishabilities with all experimental imperfections (fiber splitter imbalances etc.):



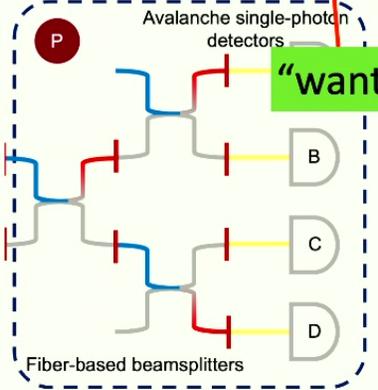
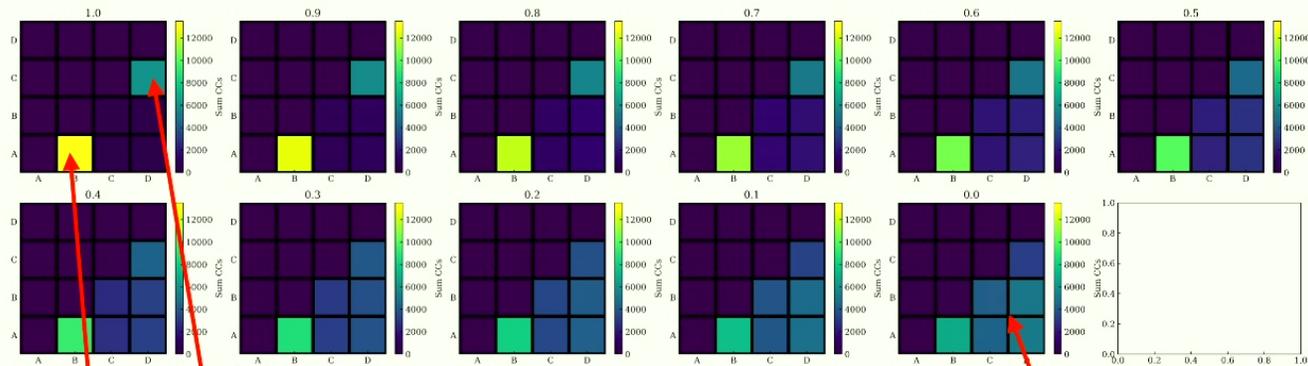
Experiment



coincidences between different detectors

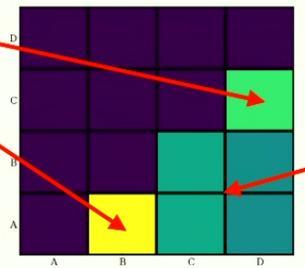
# Last week's results

Calculation for different photon indistinguishabilities with all experimental imperfections (fiber splitter imbalances etc.):



**"wanted" coincidences**

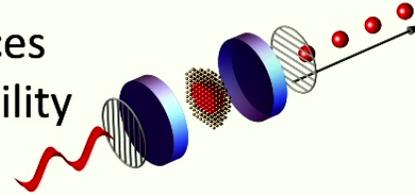
**Experiment**



**"unwanted" coincidences**

coincidences between different detectors

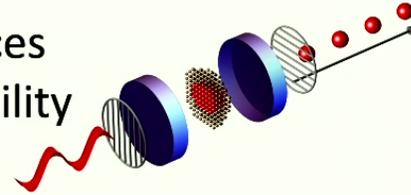
Quantum dot cavity-QED single photon sources  
Excellent brightness, purity & indistinguishability



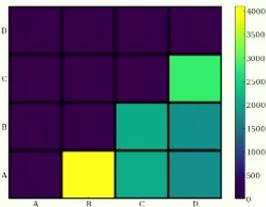
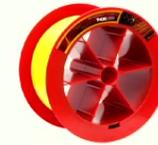
Experimentalists care about  
Loss (a lot) and fiber transport (speed  $< c$ )



Quantum dot cavity-QED single photon sources  
Excellent brightness, purity & indistinguishability



Experimentalists care about  
Loss (a lot) and fiber transport (speed  $< c$ )

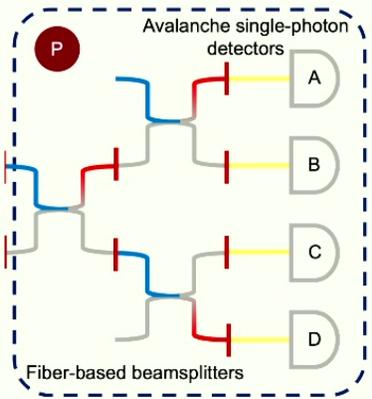
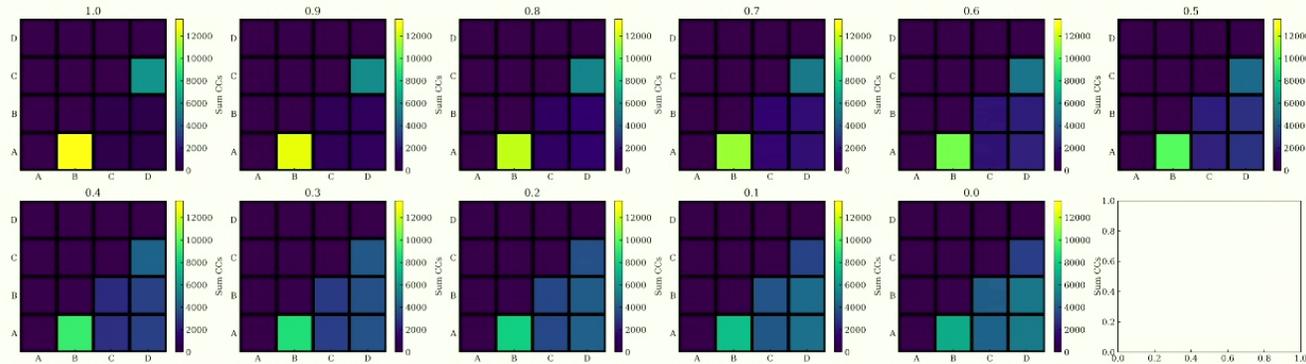


First data towards QPV!  
Many loopholes to be closed

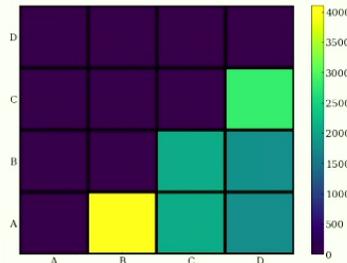
**Thank you!**

# Last week's results

Calculation for different photon indistinguishabilities with all experimental imperfections (fiber splitter imbalances etc.):



Experiment



coincidences between different detectors

# QPV loopholes

Locality loophole: space-like separation of verifiers and prover

Insecure quantum communication loophole (multiple photons/state)

Slow quantum  $\leftrightarrow$  safe space

Entanglement attacks  $\leftrightarrow$  complexity

Dislocation / replication loophole

Curved spacetime loophole

