Aktas
Djeylan

Quantum System engineering

Quantum Communication

QCI workshop, Tutorial
30/06/2022

Introduction

Cryptography

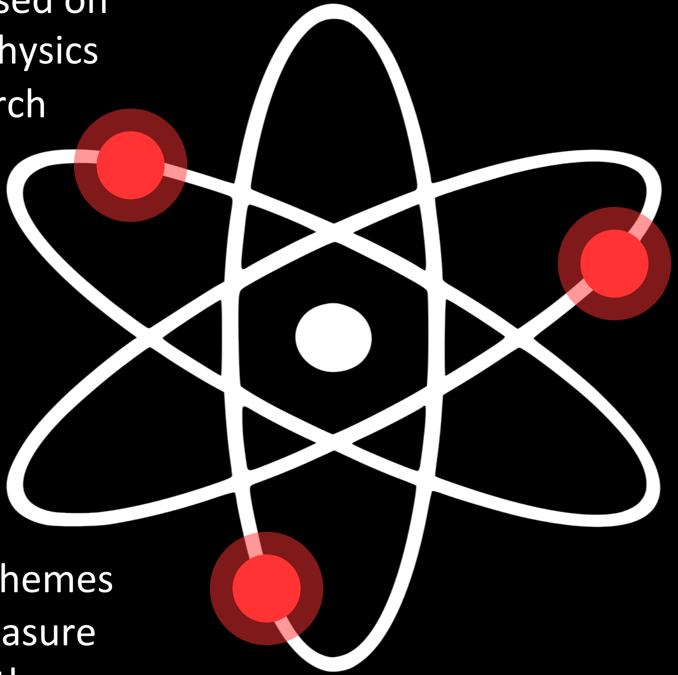
Quantum Key Distribution

Commercial QKD

- Introduction
- Cryptography
- Quantum Key Distribution
- Commercial QKD

Quantum Secured Communications

In classical communication security is based on computational assumptions. Quantum physics open the door to a new avenue of research with information-theoretic security (QKD, OT, Bit Commitment).



Quantum Computation

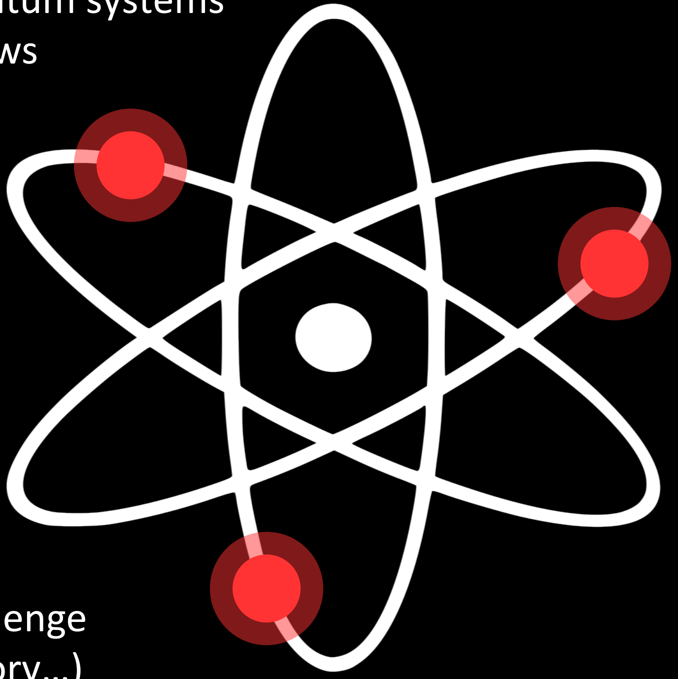
With Shor algorithm threatening the security of classical encryption, The quest for a quantum computer has been heavily pursued and is making steadily progress toward demonstrating quantum supremacy.

Quantum metrology & Sensing

At the heart of quantum metrology & sensing lies the N00N state. Quantum schemes have demonstrated the possibility to measure physical quantities with better accuracy than classical system ever could (Gas sensing, dispersion,…).

The Q-bit

The incompatible measurements in quantum systems and the superposition principle that allows encoding qbits on different carriers (electrons, ions, atoms, photons), constitute a very powerful resource.



Entanglement

The non-separability of a special class of state permit to produce non-local correlations that don't exist in the classical world.

Coherence

Coherence are at the centre of many if not all quantum protocols and preserving this coherence is often a challenge (choice of carrier, use of quantum memory…)

Quantum communication rely on this 4 pillars:

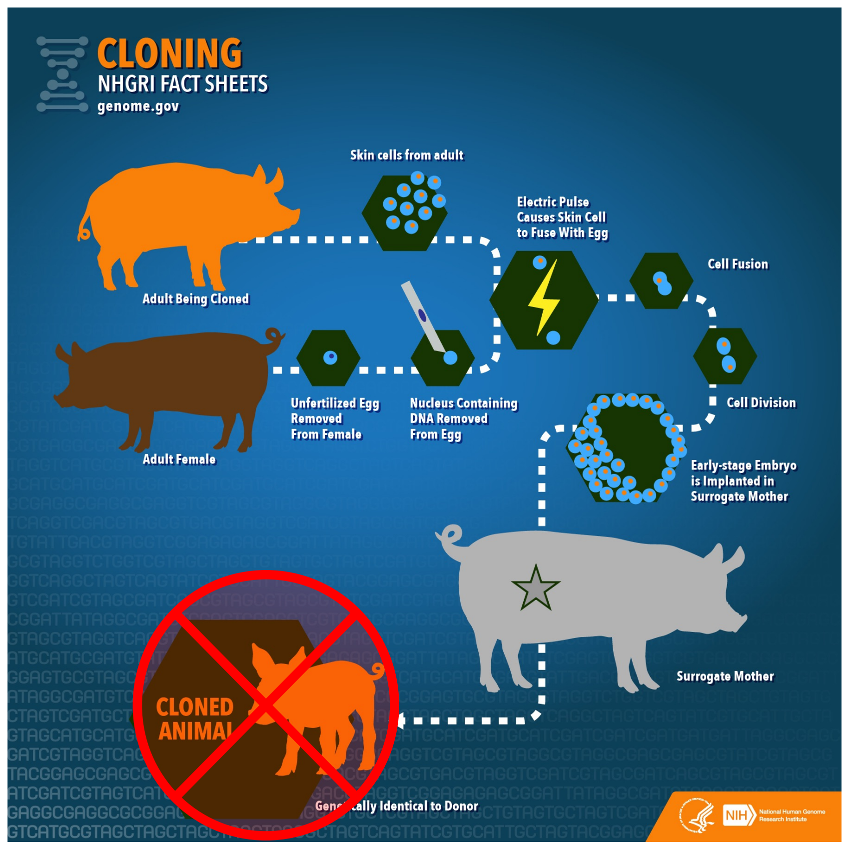
The non-cloning theorem

Entanglement

Single photon sources

Quantum relays

A brief history of the NCT

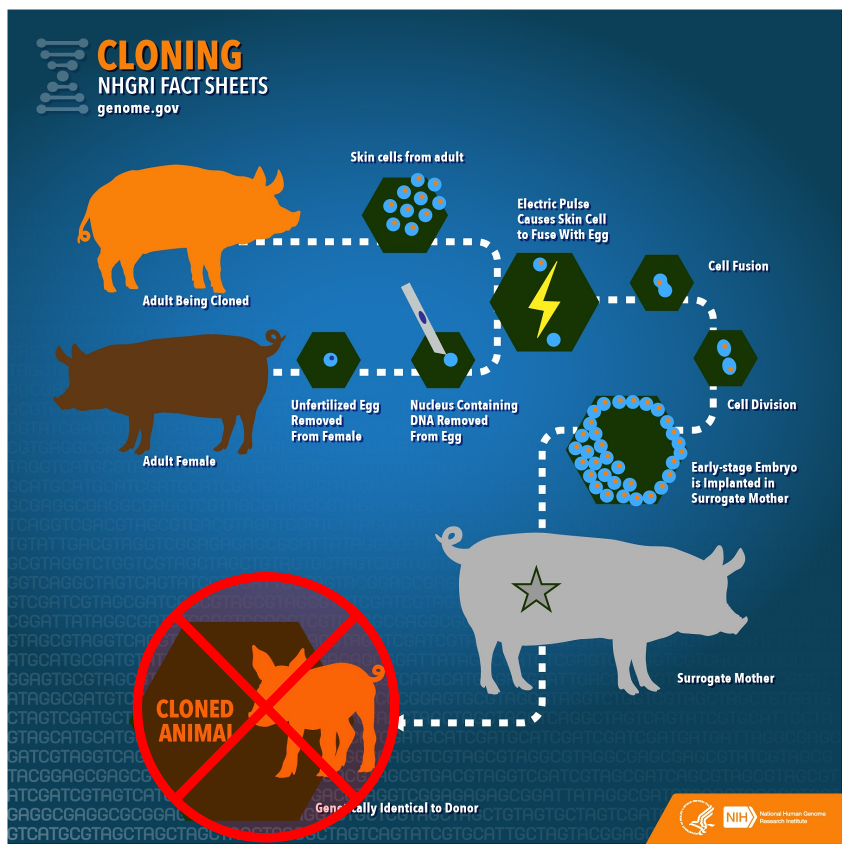


- Starting point: proposal to use entanglement to communicate via the perfect copy of an unknown q-state.
- 1982: NCT demonstrated by Wooter & Zurek.
- 1996: Generalization of NCT by Buzek & Hillery.

Bibliography

- V. Scarani *et al,* Rev. Mod. Phys. **77**, 1225 (2005)
- W. K. Wooters ans W. H. Zurek, Nature **299**, 802 (1982)
- V. Buzek and M. Hillery, Rev. A **54**, 1884 (1996)
- “Experimental Quantum Cloning”, A. Lamas-Linares *et al.* Science **296**, 712 (2002)
- “Quantum Cloning with an Optical Fiber Amplifier”, S. Fasel *et al.*, PRL **89**, 107901 (2002)

A No-go theorem



Problem:

One cannot measure the state $|\psi\rangle$ of a single system. The measurement of an observable A is one of its eigenstate, unrelated to the input state.

To reconstruct $|\psi\rangle$ one must measure the average of several observables implying a statistic over many identical systems.

One can imagine a solution that let the unknown state interact with N prepared blank reference state in order to obtain N+1 copies of the initial state:

$$|\psi\rangle \otimes |R\rangle \otimes |R\rangle ... \otimes |R\rangle \overset{?}{\rightarrow} |\psi\rangle \otimes |\psi\rangle ... |\psi\rangle$$

No quantum operation exists that can duplicate perfectly an unknown quantum state.

A perfect Quantum Cloning Machine

state to be cloned $|\psi\rangle$ → **Quantum Cloning Machine** (U) → $|\psi\rangle$ Initial state preserved

empty state $|\psi_0\rangle$ → **Quantum Cloning Machine** (U) → $|\psi\rangle$ perfect clone?

Where operator U performs unitary transformation

How to quantify the quality of the Q-cloning machine?

We simply need to calculate the overlap of the input/output state (fidelity):

$$F = \langle\psi|\rho|\psi\rangle$$

NCT easy proof

1) The goal is to achieve the following operation:

$$|\psi\rangle \otimes |\psi_0\rangle \xrightarrow{\mathbf{U}} |\psi\rangle \otimes |\psi\rangle$$

State to be cloned — Empty state — Perfect clone

⚠ $|\psi\rangle$ is unknown but defined in the computation basis $\{|0\rangle, |1\rangle\}$

2) Let's assume **U** is the "perfect cloning operator":

⚠ **U** unitary and universal

$$U|0\rangle \otimes |\psi_0\rangle \rightarrow |0\rangle \otimes |0\rangle$$
$$U|1\rangle \otimes |\psi_0\rangle \rightarrow |1\rangle \otimes |1\rangle$$

NCT easy proof

3) Now what about a Q-bit state?

$$|\psi\rangle = \alpha|0\rangle + e^{i\phi}\beta|1\rangle$$

Linearity simply gives:

$$U|\psi\rangle|\psi_0\rangle = \alpha|0\rangle|0\rangle + e^{i\phi}\beta|1\rangle 1\rangle$$

$$\neq$$

Instead of the expected:

$$U|\psi\rangle|\psi_0\rangle \rightarrow |\psi\rangle|\psi\rangle = \alpha^2|0\rangle|0\rangle + e^{i2\phi}\beta^2|1\rangle|1\rangle + e^{i\phi}\alpha\beta(|0\rangle|1\rangle + |1\rangle|0\rangle)$$

➡ Hence, such an operator **U cannot exist.**
An unknown quantum state cannot be cloned, but the basis states can be!

NCT easy proof

Conclusions:

- No violation of Heisenberg's relations
- Possibility to distribute secret keys for cryptography

However, can we do something?

- Can we extract some information?
- At the price of non perfect cloning?

Homework:

Can you calculate the fidelity of 2 different strategies for unperfect cloning? (Measure H/V resend H/V or send H/V randomly)

Entanglement in short

The tensor product of 2 qbits can be written:

$$\psi_{ab}\rangle = |\psi_a\rangle \otimes \psi_b\rangle = \alpha_a\alpha_b|0_a\rangle|0_b\rangle + \alpha_a\beta_b|0_a\rangle|1_b\rangle + \beta_a\alpha_b|1_a\rangle|0_b\rangle + \beta_a\beta_b|1_a\rangle|1_b\rangle$$

There are some 2 qbits state that cannot be written as such called entangled states:

2 qbits Bell state basis

$$\begin{cases} |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \\ |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \end{cases}$$

Entanglement Photon Pair Source (EPPS)

First experimental realization:

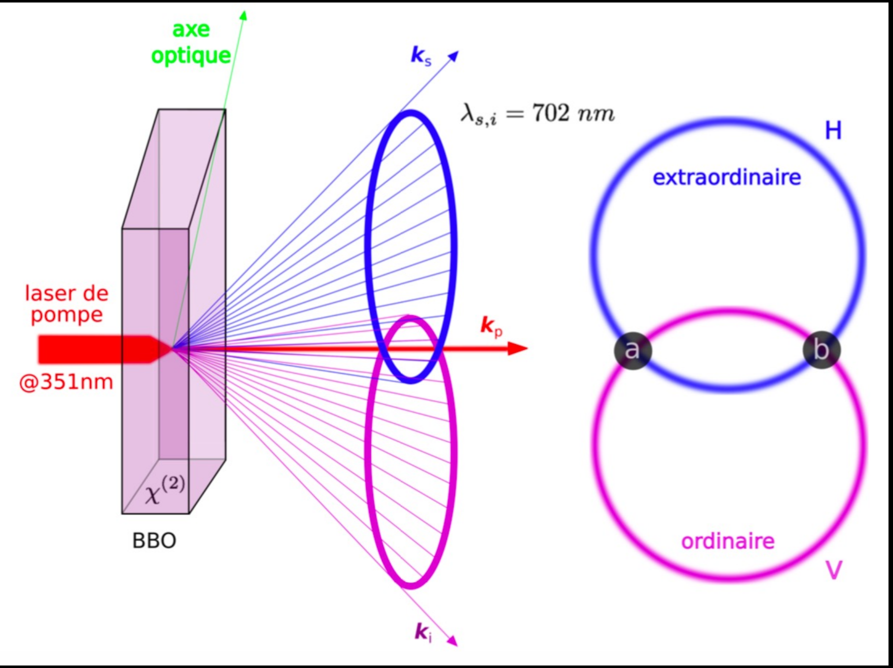
VOLUME 49, NUMBER 2 PHYSICAL REVIEW LETTERS 12 JULY 1982

Experimental Realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*: A New Violation of Bell's Inequalities

Alain Aspect, Philippe Grangier, and Gérard Roger
Institut d'Optique Théorique et Appliquée, Laboratoire associé au Centre National de la Recherche Scientifique, Université Paris-Sud, F-91406 Orsay, France
(Received 30 December 1981)

The linear-polarization correlation of pairs of photons emitted in a radiative cascade of calcium has been measured. The new experimental scheme, using two-channel polarizers (i.e., optical analogs of Stern-Gerlach filters), is a straightforward transposition of Einstein-Podolsky-Rosen-Bohm *gedankenexperiment*. The present results, in excellent agreement with the quantum mechanical predictions, lead to the greatest violation of generalized Bell's inequalities ever achieved.

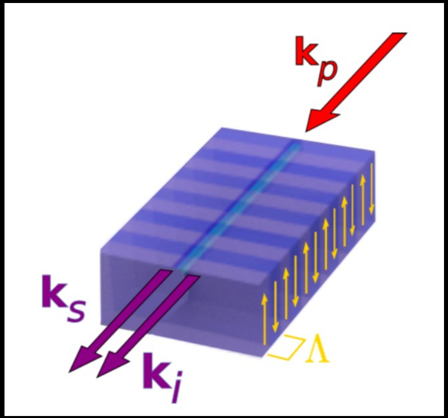
Entanglement Photon Pair Source (EPPS)



Kwiatt *et al.* (1995)

Many other experiments followed:

- Increasing brightness.
- Getting more compact.



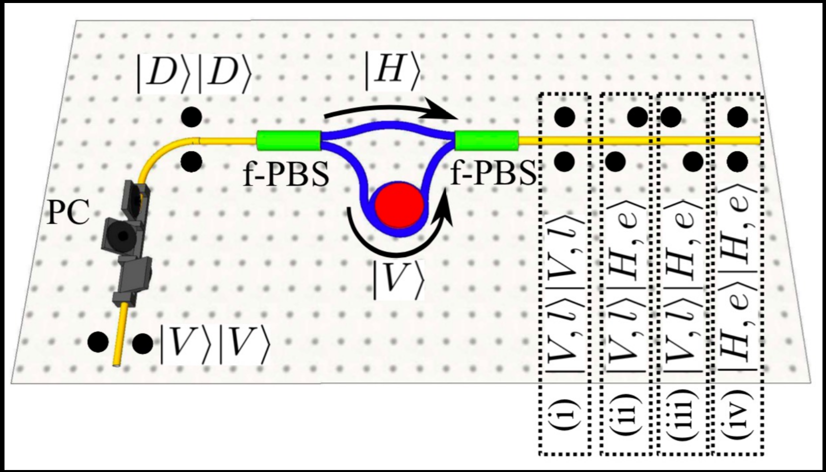
PPLN waveguide

Entanglement Photon Pair Source (EPPS)

SPDC sources with PPLN waveguides:

Type d'interaction	type-0	type-I	type-II
Polarisation	$\|V\rangle_p \rightarrow \|V\rangle_s\|V\rangle_i$	$\|V\rangle_p \rightarrow \|H\rangle_s\|H\rangle_i$	$\|H\rangle_p \rightarrow \|H\rangle_s\|V\rangle_i$
$\chi^{(2)}$ coeff. du LiNbO3	$d_{33} \approx 30\,\mathrm{pm/V}$	$d_{31} \approx -5\,\mathrm{pm/V}$	$d_{24} \approx 10\,\mathrm{pm/V}$
η_{SPDC} dans	$10^{-6} - 10^{-5}$	10^{-7}	10^{-9}
$\Delta\lambda$ à 1550 nm	20-100 nm	20-100 nm	0.8-3 nm
$\Delta\nu$ à 1550 nm	2.5-12.5 THz	2.5-12.5 THz	0.1-0.375 THz

Transcriber from ET to Pol:



Entanglement Photon Pair Source (EPPS)

SPDC sources based on type II performances :

Référence	Matériau	η_{SPDC}	V_{net}	Coïncidences
Lee et collab. [2006]	DSF	$3,2 \cdot 10^{-32}$	98,3%	$80\,s^{-1}$
Piro et collab. [2009]	PPKTP	$2,8 \cdot 10^{-10}$	98±1%	$5\,s^{-1}$
Medic et collab. [2010]	DSF	NA	99±1%	$5\,s^{-1}$
Martin et collab. [2010a]	PPLN/W	$1,1 \cdot 10^{-9}$	99±2%	$800\,s^{-1}$
Kaiser et collab. [2012b]	PPLN/W	$3,5 \cdot 10^{-10}$	99,5±0,8%	$1100\,s^{-1}$
Steinlechner et collab. [2013]	PPKTP	$5,4 \cdot 10^{-10}$	99,3±0,3%	$11800\,s^{-1}$
Jeong et collab. [2016]	PPKTP	$4,4 \cdot 10^{-11}$	96,8±0,8%	$90900\,s^{-1}$
Ce travail	PPLN/W	$6,0 \cdot 10^{-9}$	99±1%	$1200\,s^{-1}$

Type II is a very narrow process so the pair rates are usually limited

EPPS performances :

Group	Generator	Obser-vable	Bandwidth (MHz)	λ (nm)	B^*	V_{net}
[211] Cambridge (2006)	KTP OPO	polar.	22	795	0.7	77%
[58] Geneva (2008)	PPLN/W	time-bin	1200	1560	446	NA$^\times$
[212] Hefei (2008)	PPKTP OPO	polar.	9.6	780	6	97%
[52] Barcelona (2009)	PPKTP	polar.	22	854	3	98%
[213] Geneva (2009)	PPLN/W OPO	time-bin	117	1560	17	94%
[246] Hong Kong	Rb atoms	polar.	6	780	0.5	90%
This thesis, 540 MHz	PPLN/W	polar.	540	1560	306	99%
This thesis, 25 MHz	PPLN/W	polar.	25	1560	380	99%

Brightness is defined as the number of photon pairs /s /mW /MHz

Entanglement Photon Pair Source (EPPS)

EPPS based on $\chi^{(3)}$ performances:

Table S1. Typical bi/multi-photon quantum sources on various χ(3) platforms

Materials1[1]	Si	Si	Si	Si	Si	Hydex	Hydex	Si_3N_4
Structures	Nanowire[2]	Nanowire (This work)	Nanowire (This work)	Ring[3]	PhC[4]	Ring[5]	Ring[5]	Ring[6]
Number of photons	2	2	4	2	2	2	4	2
Nonlinear coefficient ($W^{-1}m^{-1}$)	300	285	285	—	5900	0.22[7]	0.22[7]	—
Average pump power (mW)	1	0.12	0.6	3.3	0.6	0.6	1.5	6
Collected photon bandwidth (GHz)	18	50	50	13	12.5	0.8	0.8	0.09
Brightness (pairs s^{-1})	40kHz	270 kHz	340kHz	14MHz	—	302kHz	135kHz	35MHz
coincidence–to-accidental ratio	42	230	—	45	~5	—	—	—
Raw visibilities of quantum interference	—	93.0±3.2%	96.5±1.5%	89.3±2.6%	74.1±4.8%	82.4%	89%	~90%
Fidelity	0.91±0.02	0.95±0.01 (raw)	0.78±0.02	—	—	0.96 (net)	0.64	—

Single Photon Source (SPS)

➢ Basic operation principle

Repetition rate & probability of collection

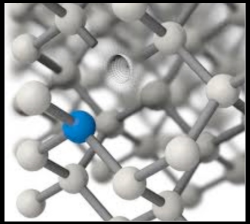
Prime features

- P_1: probaP$_0$: probability of no photon at all
- bility of exactly 1 photon
- P_2: probability of having 2 photons
- …

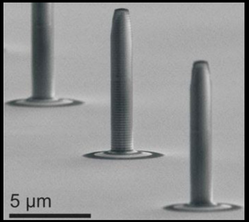
➢ Different types of "true" SPS

- Single molecules
- Single semiconductor device
- Single NV center in Diamond
- Isolated ion/atom

NV center



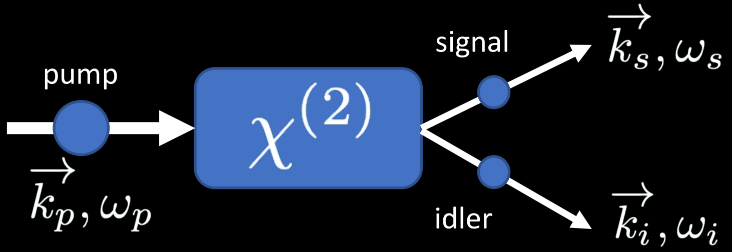
Q-dot

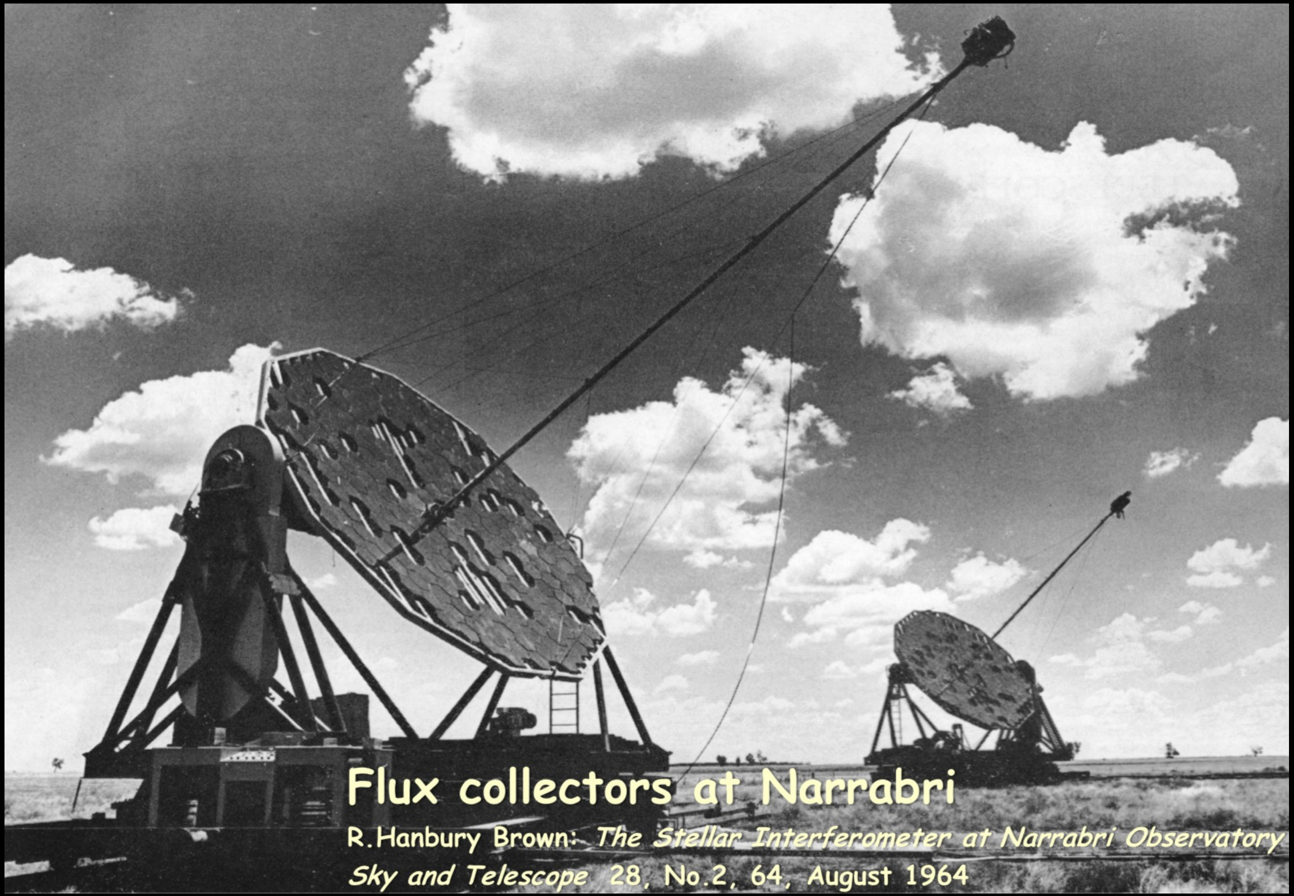


➢ Heralded SPS

Based on photon pair creation in nonlinear crystal

Spontaneous parametric down-conversion




Flux collectors at Narrabri
R.Hanbury Brown: The Stellar Interferometer at Narrabri Observatory
Sky and Telescope 28, No.2, 64, August 1964

HBT a bright idea for astrophysics

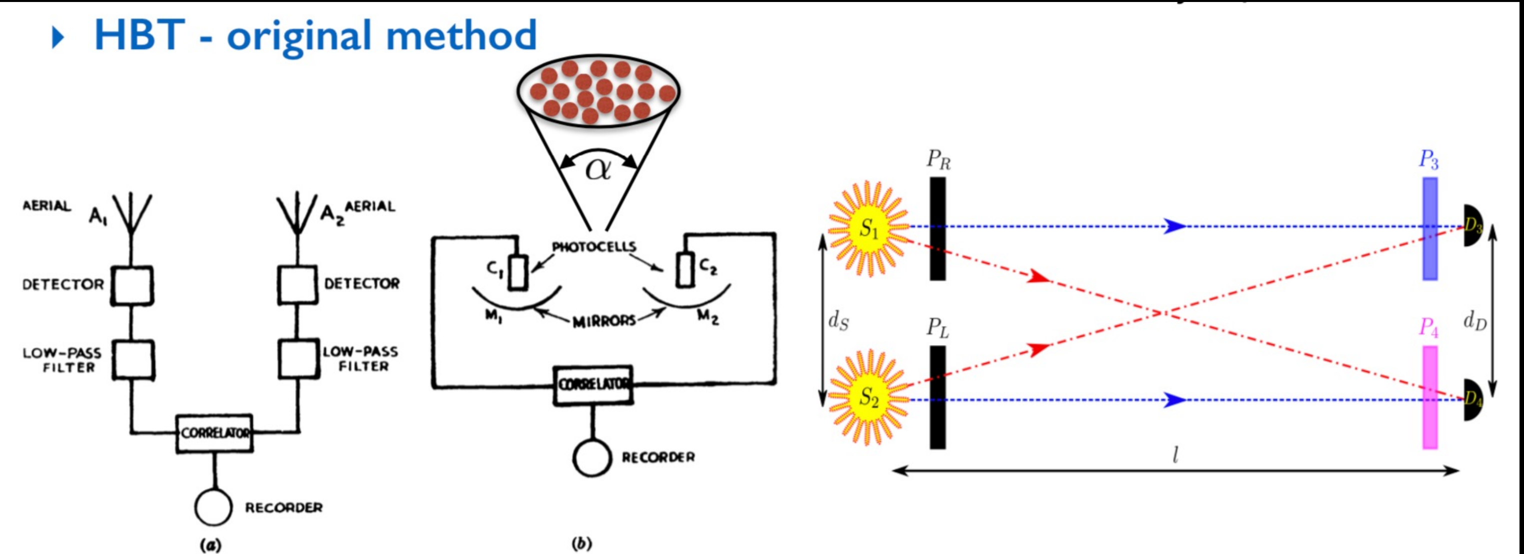


Fig. 1. A new type of radio interferometer (*a*), together with its analogue (*b*) at optical wave-lengths

- What for?

First measurement of the angular diameter of a star.

Interferometric-like configuration with indistinguishable paths, insensible to atmospheric fluctuations.

R. Hanbury Brown and R. Q. Twiss, Nature **177**, 27-32 (1956)

A. Martin *et al.*, EPL **97**, 10003 (2012)

Classical description of the autocorrelation function

- **Classical intensity correlation in the time domain**

$$g^{(2)}(t_1,t_2) = \frac{\langle E^\star(t_1)E^\star(t_2)E(t_2)E(t_1)\rangle}{\sqrt{\langle|E(t_1)|^2\rangle\langle|E(t_2)|^2\rangle}} = \frac{\langle I(t_1)I(t_2)\rangle}{\langle I(t_1)\rangle\langle I(t_2)\rangle}$$

with $I(t_i) = E^\star(t_i)E(t_i) = |E(t_i)|^2$

- **Properties**

Cauchy-Schwarz inequality $\mapsto \langle I(t_1)I(t_2)\rangle^2 \leq \langle I^2(t_1)\rangle\langle I^2(t_2)\rangle$

Stationary regime & $\tau = t_2 - t_1$ $\mapsto \langle I(t)I(t+\tau)\rangle^2 \leq \langle I^2(t)\rangle^2$

$g^{(2)}(0)$ is max in 0
➜ so-called photon bunching $\mapsto g^{(2)}(\tau) \leq g^{(2)}(0)$

Remarking that $\langle I^2(t)\rangle \geq \langle I(t)\rangle^2$ $\mapsto g^{(2)}(0) \geq 1$

Classical $g^{(2)}(0)$ is always greater than 1 !

Practical examples:

- Coherent state

$$P_P(n,\bar{n}) = \frac{\bar{n}e^{-\bar{n}}}{n!}$$

$$g^{(2)}(0) = 1$$

for $\bar{n} \ll 1$ $P_2 = P_1^2/2$

- Thermal state

$$P_T(n,\bar{n}) = \frac{1}{(1+\bar{n})(1+\frac{1}{\bar{n}})^n}$$

$$g^{(2)}(0) = 2$$

for $\bar{n} \ll 1$ $P_2 = P_1^2$

quantum description of the autocorrelation function

- **Quantum description of the EM field** $E(z,t) = E^{\dagger}(z,t) + E(z,t)$

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

$$\mapsto g^{(2)}(\tau) = \frac{\langle : I(t+\tau)I(t) : \rangle}{\langle I(t)\rangle^2}$$

- **Take care !**

$\langle : \; : \rangle$ ➜ the operators are in the **normal order**

$E^{\dagger}(t)$ and $E^{\dagger}(\tau)$ do not commute ➜ Cauchy-Schwarz cannot be applied anymore

➜ $g^{(2)}(0)$ can drop to 0

- **Single mode operation**

$$\mapsto g^{(2)}(0) = \frac{\langle a^{\dagger}a^{\dagger}aa\rangle}{\langle a^{\dagger}a\rangle^2} = \frac{\langle \widehat{n}(\widehat{n}-1)\rangle}{\langle \widehat{n}\rangle^2}$$

with $\widehat{n} = a^{\dagger}a$ photon number operator

$\langle \widehat{n}\rangle$ mean number of photons in the mode

Simple 2-level system:

- Single emitter

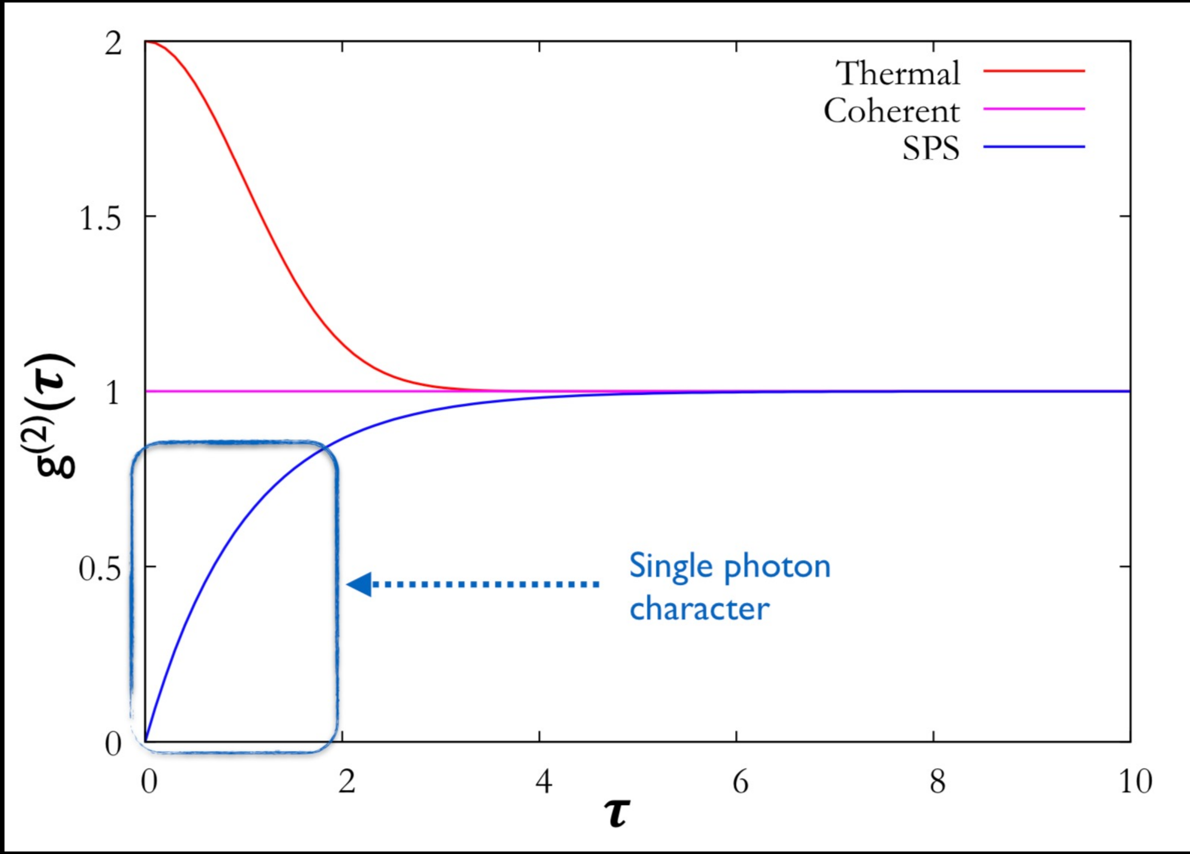
Rate equations show:

$$g^{(2)}(\tau) = 1 - e^{-(\Omega+\Gamma)\tau}$$

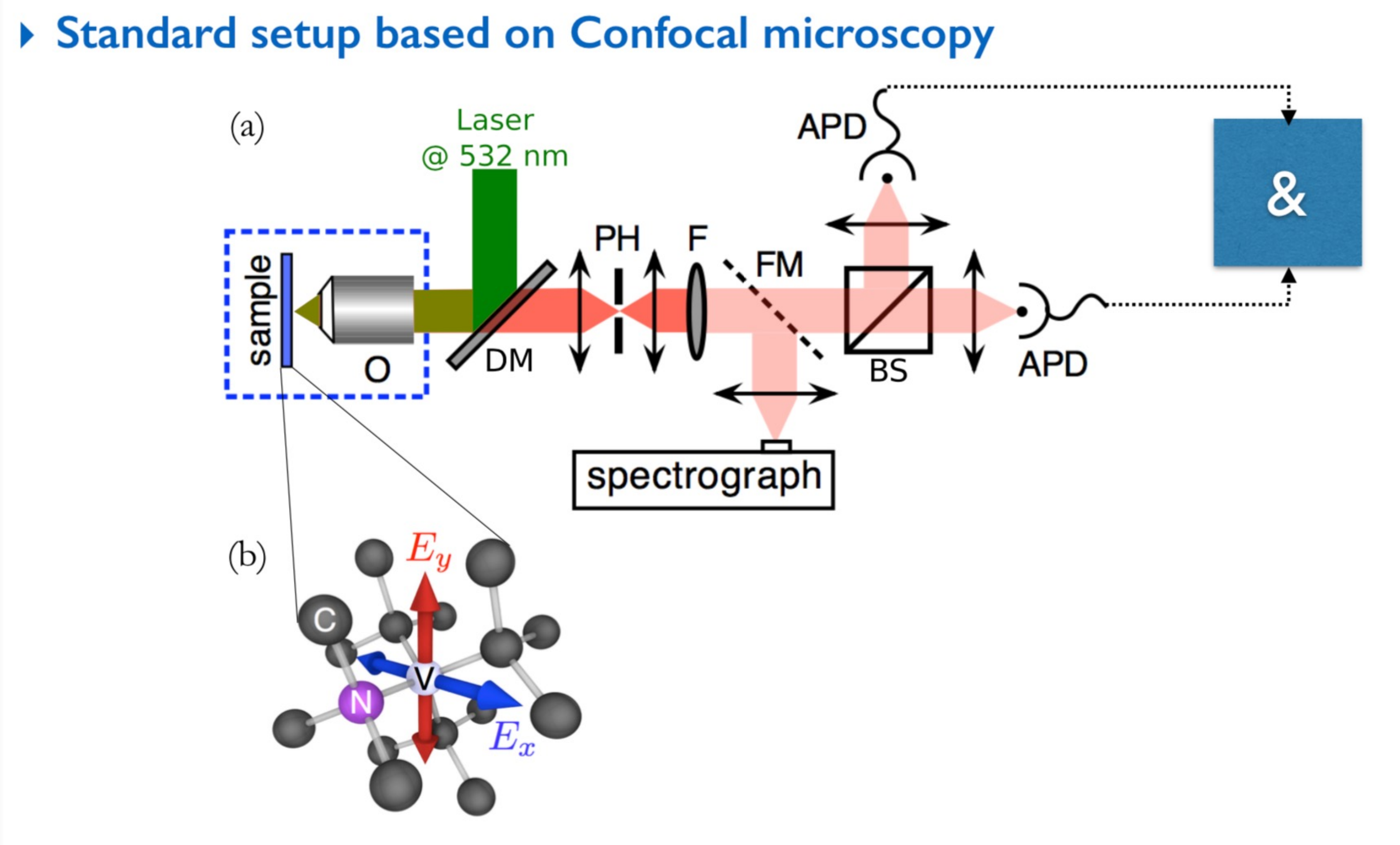
$$\begin{cases} g^{(2)}(0) = 0 \\ g^{(2)}(0) \leq g^{(2)}(\tau) \end{cases}$$

➜ Great !

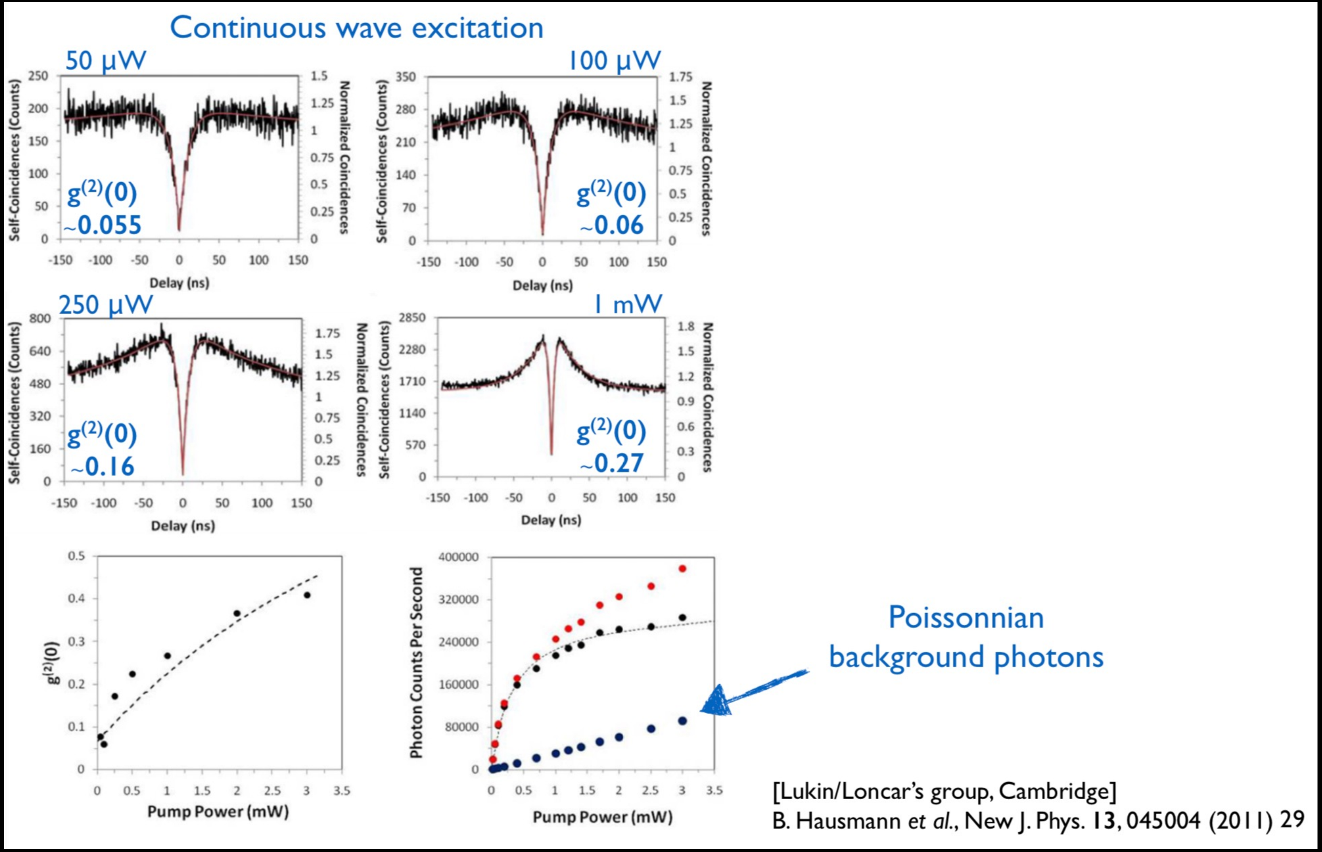
Summary


Thermal
Coherent
SPS
Single photon character
$g^{(2)}(\tau)$
τ
0
0.5
1
1.5
2
0
2
4
6
8
10

True SPS using NV center in diamond

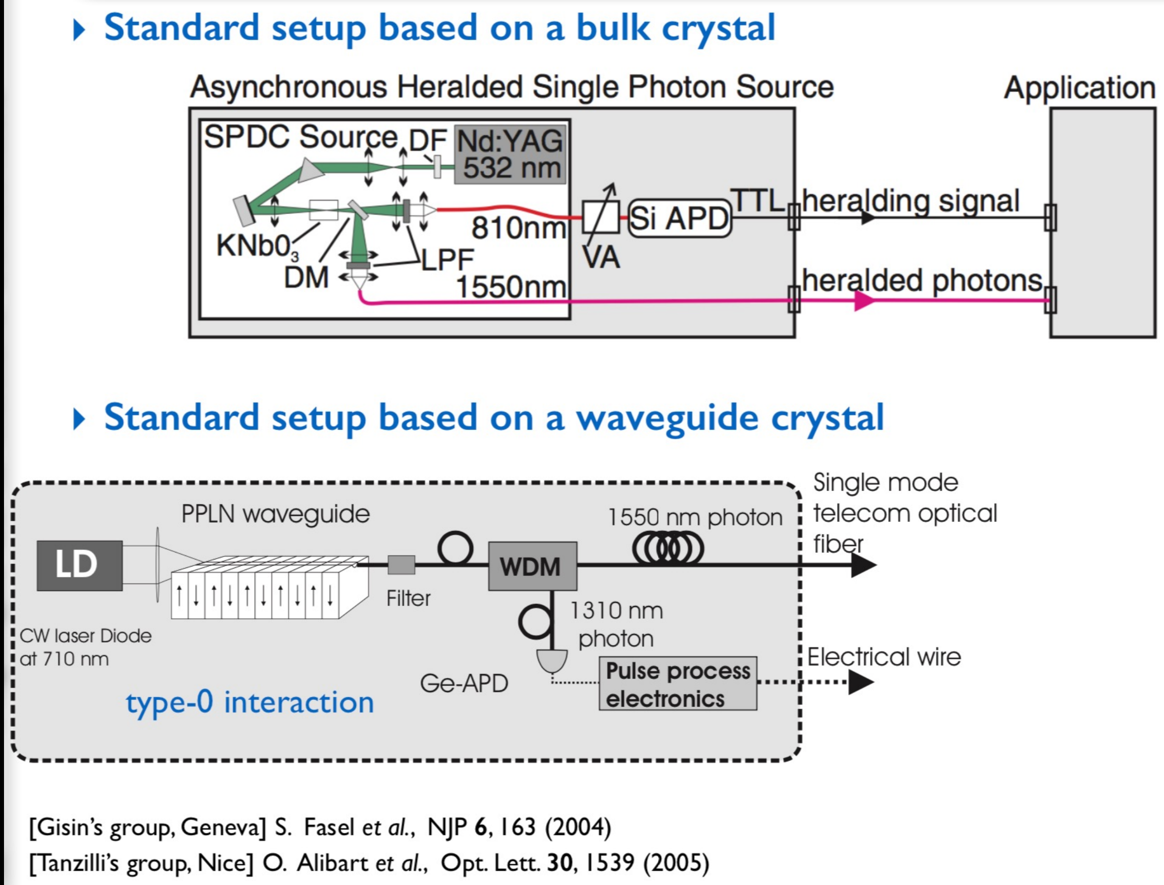


True SPS using NV center in diamond



Increasing the single photon rate comes at the price of decreasing the quality of $g^{(2)}(0)$

Heralded SPS using NL optics

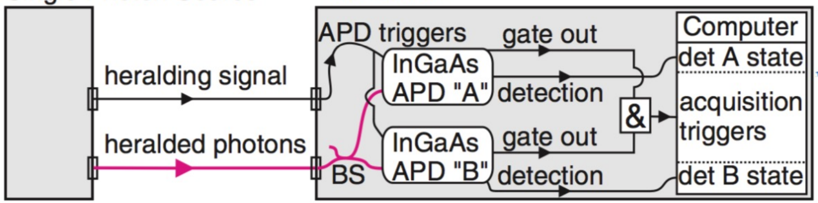


➢ Specificities of HPS:

- Reduces both empty pulses and detection noise.
- Reduces the emission to sub-poissonnian statistics.
- Emission regime is asynchronous.

Heralded SPS using NL optics

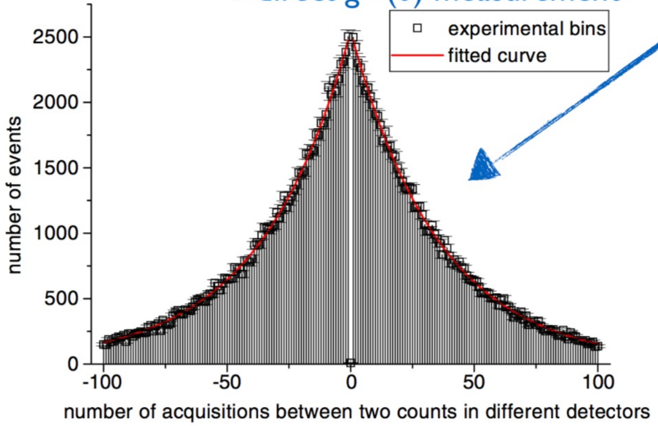
Retrieving $g^{(2)}(0)$ from post data processing

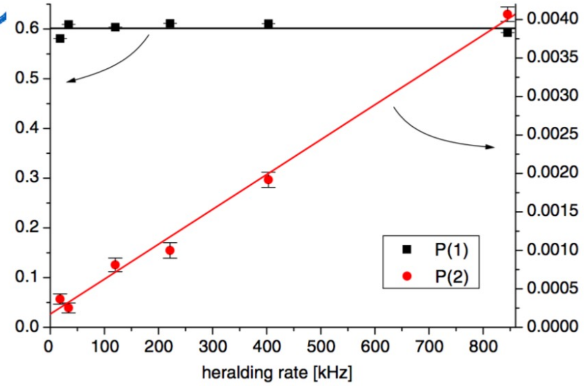


	det A	det B	
	...	...	
no detection	0	0	$n = -1$
start at A	1	0	$n = 0$
no detection	0	0	$n = +1$
invalid start	1	0	$n = +2$
no detection	0	0	$n = +3$
stop at B	0	1	$n = +4$
	...	...	

Results

Same as obtained with "true" SPS
➜ direct $g^{(2)}(0)$ measurement





[Gisin's group, Geneva] S. Fasel *et al.*, NJP **6**, 163 (2004)

34

Heralded SPS using NL optics

Summary

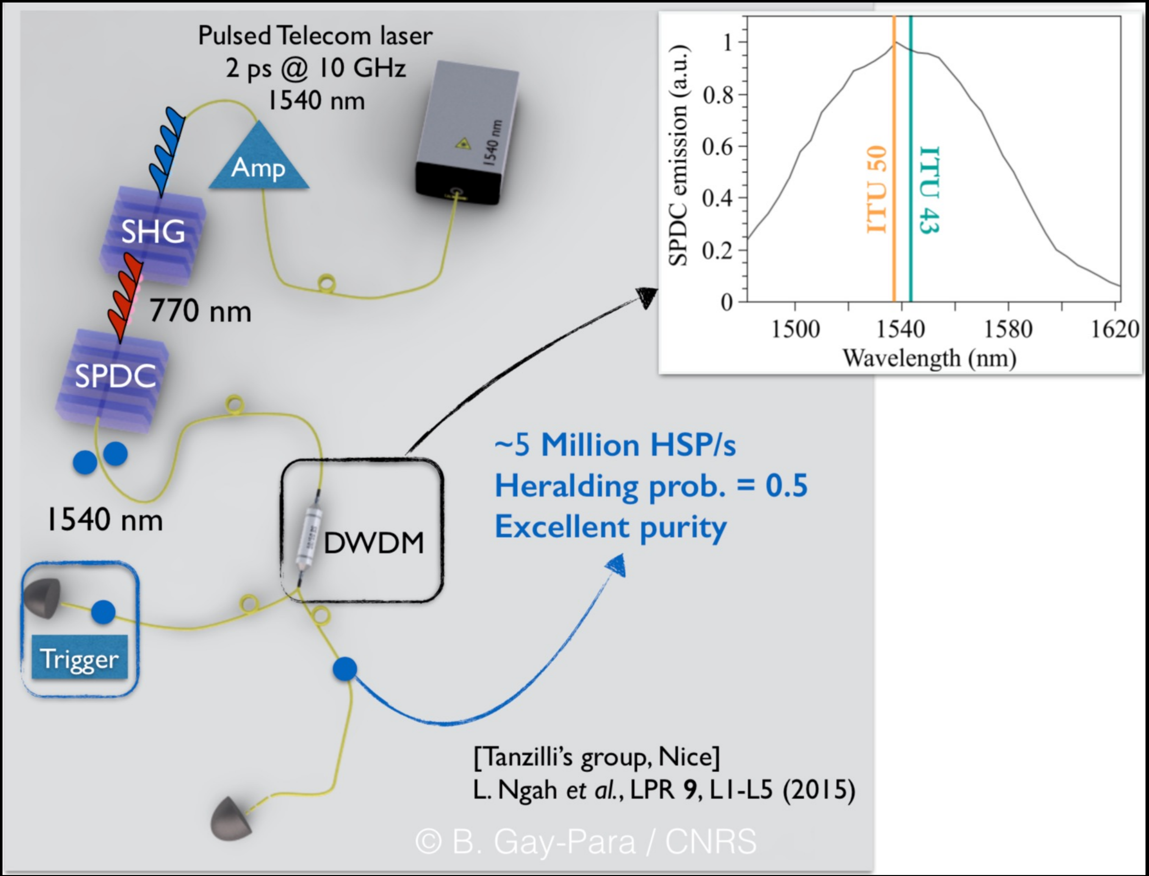
Source	λ (nm)	P0	P1	P2	$g^{(2)}(0)$	H rate (kc/s)
Waveguide	1550 / 1310	0.63	0.37	7.10^{-3}	0.08	~100
Waveguide	1550 / 810	0.4	0.6	-	2.10^{-3} - 1	0.4 - 1000
Bulk	1550 / 810	0.39	0.61	2.10^{-4} -4.10^{-3}	2.10^{-3} - 2.10^{-2}	20 - 800

[Tanzilli's group, Nice] O. Alibart *et al.*, Opt. Lett. **30**, 1539 (2005)
[Gisin's group, Geneva] S. Fasel *et al.*, NJP **6**, 163 (2004)
[Silberhorn's group, Paderborn] S. Krapick *et al.*, NJP **15**, 033010 (2013)

From this old comparison table we can see that over a 10 years effort we notice a quick saturation in the achievable heralding rate…

How to go beyond those results?

Heralded SPS using NL optics



The solution was to increase dramatically the repetition rate!

Heralded SPS using NL optics

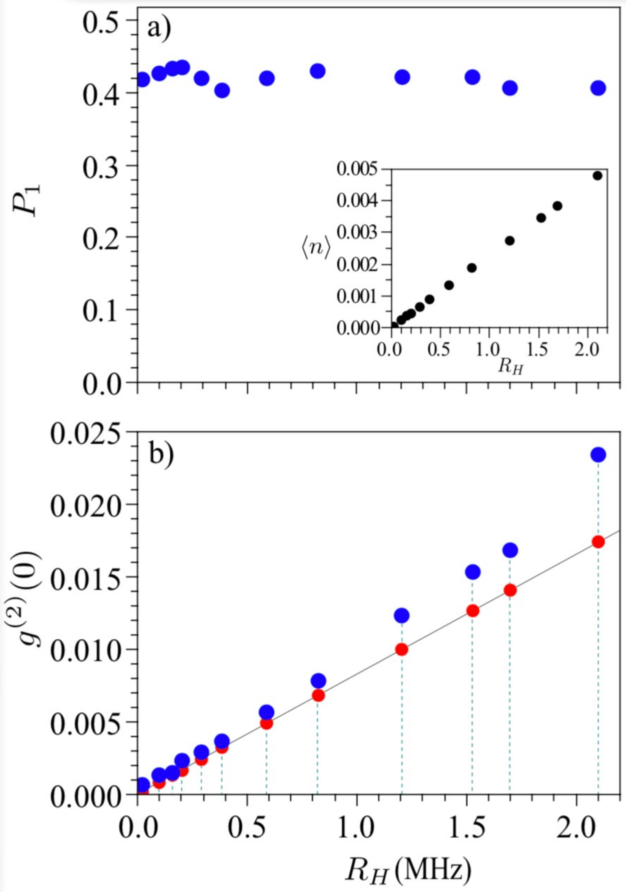


Table 1 Experimental results for different HSPS realizations. For each group, only the values corresponding to the highest measured R_H have been reported.

	P_1	η_D	R_H	$\langle n \rangle$	$g^{(2)}(0)$
Nice	0.42	0.17	2.1 MHz	0.005	0.023
Geneva [11]	0.45	0.50	4.4 MHz	0.1	0.18[a]
Paderborn [9]	0.60	0.55	105 kHz	–	0.40
Turin [25]	0.13	0.40	~10 kHz[b]	–	0.0050
Vienna [13]	0.82	0.95	6 kHz	–	–
Tokyo [16]	<0.3	0.70	~150 kHz[b]	0.00021	–
Nice[c]	0.5	0.90	15 MHz	0.005	$\lesssim$0.020

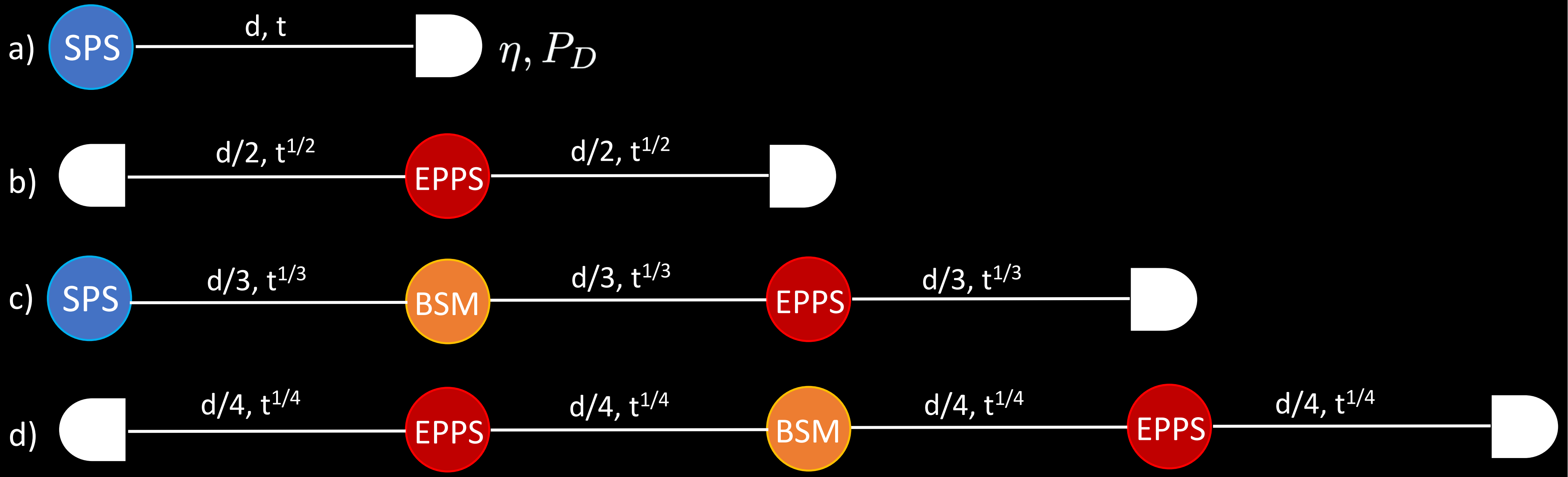
[a]theoretically calculated. [b]estimated from reported data and P_1. [c]expected values.

[Zbinden's group, Geneva] E. Pomarico *et al.*, OPEX **20**, 23846 (2012)

Context of today's quantum communication

➢ Exploiting single qbits and ebits

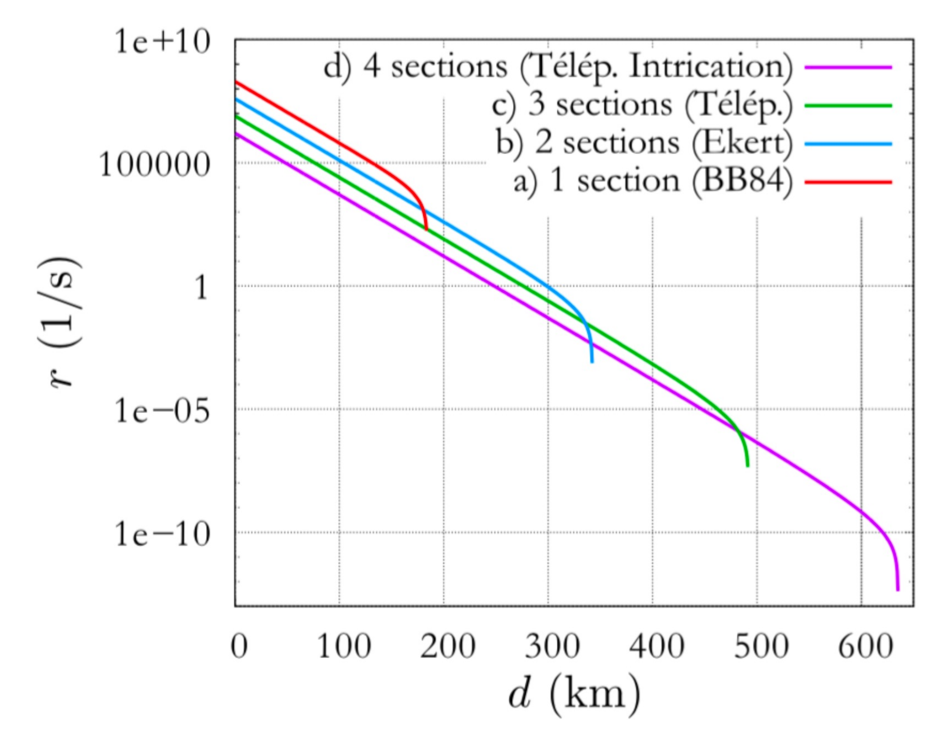
Distribution of quantum bits of information using single photon and entangled photon pair sources over long distances.



Context of today's quantum communication

- Exploiting single qbits and ebits

One can show that with N sections of length d/N the probabilities of a true and false detection are:



$$P_D = \eta^N t$$

$$P_{noise} = \left[(1-\eta t^{1/N})P_{DC} + \eta t^{1/N}\right]^N - \eta^N t$$

Collins, D., N. Gisin et H. De Riedmatten. 2005, «Quantum relays for long distance quantum cryptography», *J. Mod. Opt.*, vol. **52**, p. 735–753

Introduction

Cryptography

Quantum Key Distribution

Commercial QKD

QKD – Protocols

Discrete Variable QKD

- BB84
- BBM92

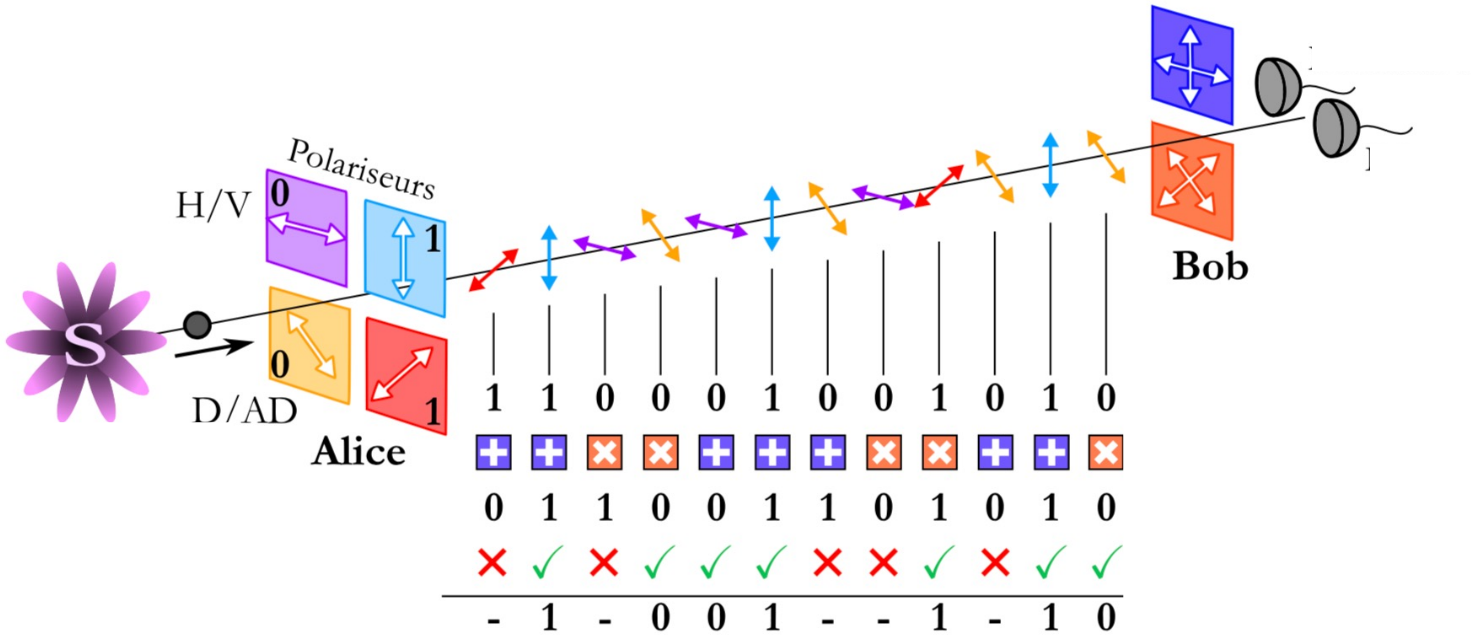
Continuous Variable QKD

- Gaussian Protocols
- Discrete-Modulation Protocols

Distribute Phase Reference QKD

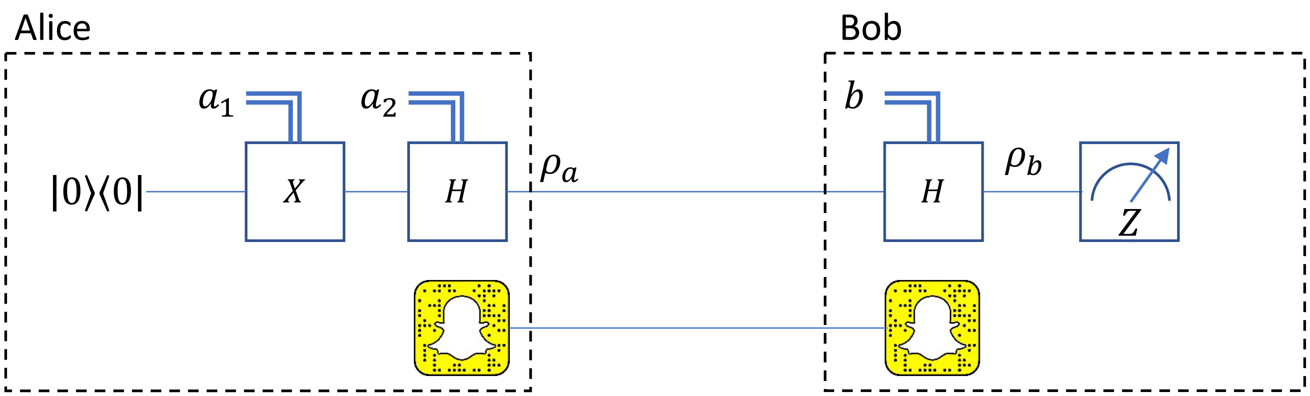
- COW
- DPS

BB84 Review



Polariseurs
H/V
0
1
0
1
D/AD
Alice
Bob
1 1 0 0 0 1 0 0 1 0 1 0
0 1 1 0 0 1 1 0 1 0 1 0
- 1 - 0 0 1 - - 1 - 1 0

BB84 Review

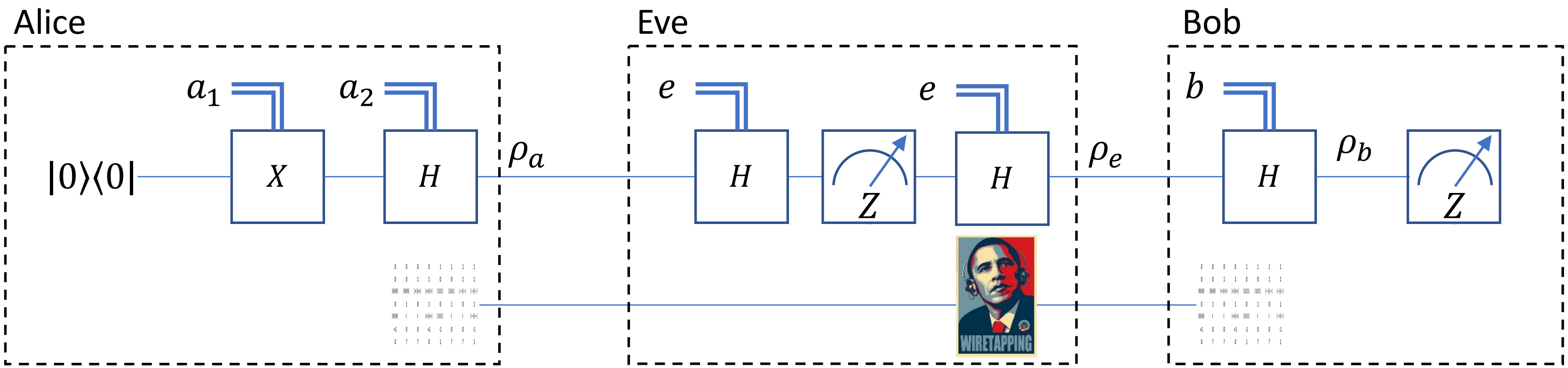


- $a_1, a_2, b \in \{0,1\}$ chosen randomly
- Need classical communications channel to compare a_2, b
- Only use outcomes where $a_2 = b$ – called sifting
- Repeat many times to build up key

a_1
a_2
ρ_a
b
ρ_b
$\mathrm{tr}(\rho_b Z)$
Bit Value

C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8. New York, 1984

BB84 Review – Eve Attacks



a_1	0	0	0	0	1	1	1	1
$a_2 = b$	0	0	1	1	0	0	1	1
ρ_a	$\|0\rangle\langle 0\|$	$\|0\rangle\langle 0\|$	$\|+\rangle\langle +\|$	$\|+\rangle\langle +\|$	$\|1\rangle\langle 1\|$	$\|1\rangle\langle 1\|$	$\|-\rangle\langle -\|$	$\|-\rangle\langle -\|$
e	0	1	0	1	0	1	0	1
ρ_e	$\|0\rangle\langle 0\|$	I	I	$\|+\rangle\langle +\|$	$\|1\rangle\langle 1\|$	I	I	$\|-\rangle\langle -\|$
$\mathrm{tr}(\rho_b Z)$	+1	0	0	+1	-1	0	0	-1
Bit Value	0	?	?	0	1	?	?	1

- Can expect error $\delta = 25\%$ (? Correct 50% of the time)
- Alice & Bob need to publicly announce some bits to determine error rate – stop if too high

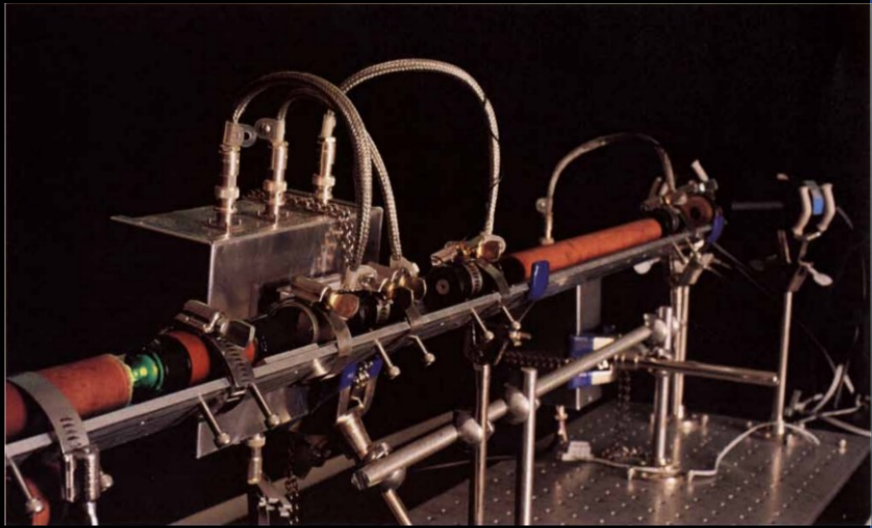
BB84 Questions

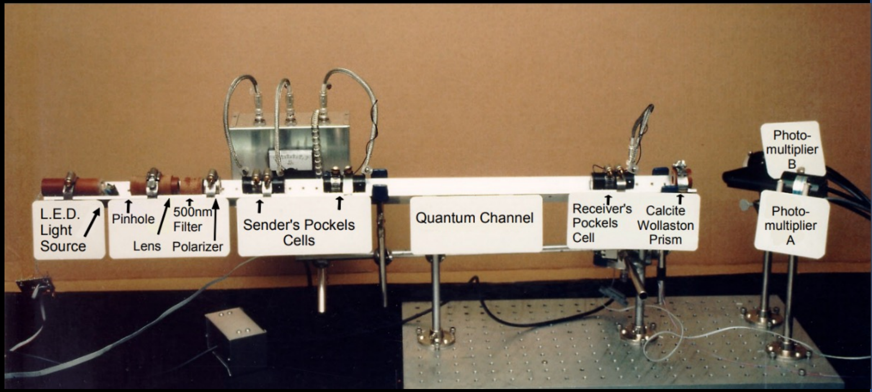
This description raises some questions for implementation

- What if Eve performs another type of attack?
- What happens if Eve performs a collective attack?
- What happens if Eve has some sort of memory?
- How does this work across lossy channels?
- Experimental imperfections – loss, device imperfections, etc?
- What happens if Eve isn’t confined to her box?

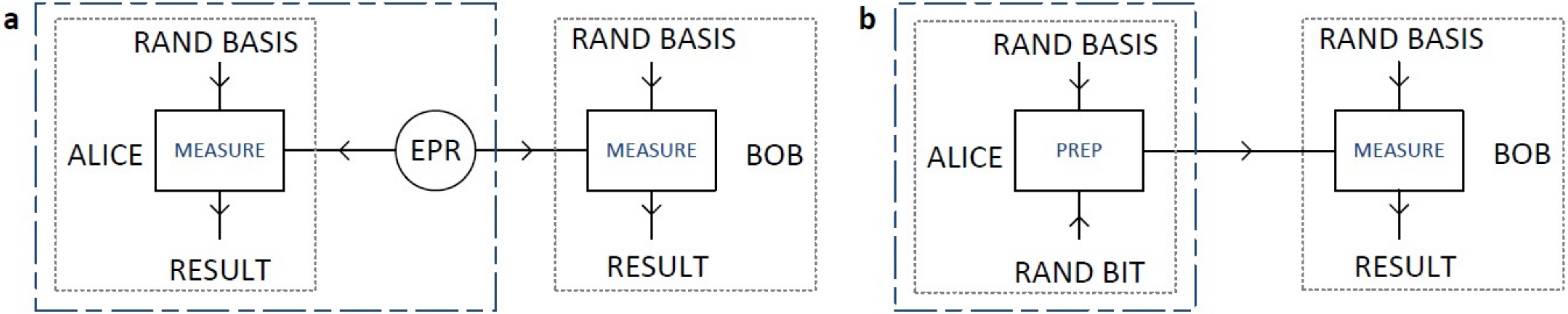
BB84 Questions

"…power supplies make noise, and not the same noise for the different voltages needed for different polarizations... Thus, our prototype was unconditionally secure against any eavesdropper who happened to be deaf!" – Gilles Brassard, Brief History of Quantum Cryptography: A Personal Perspective, quant-ph/0604072

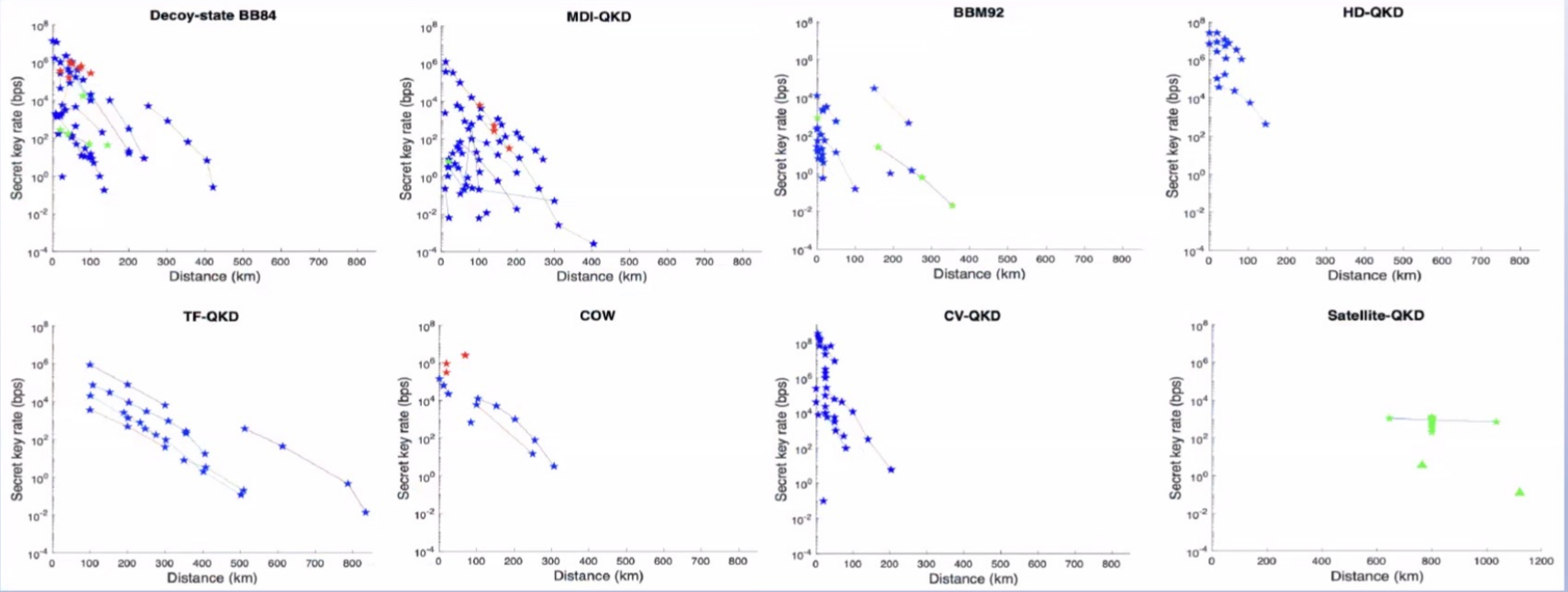




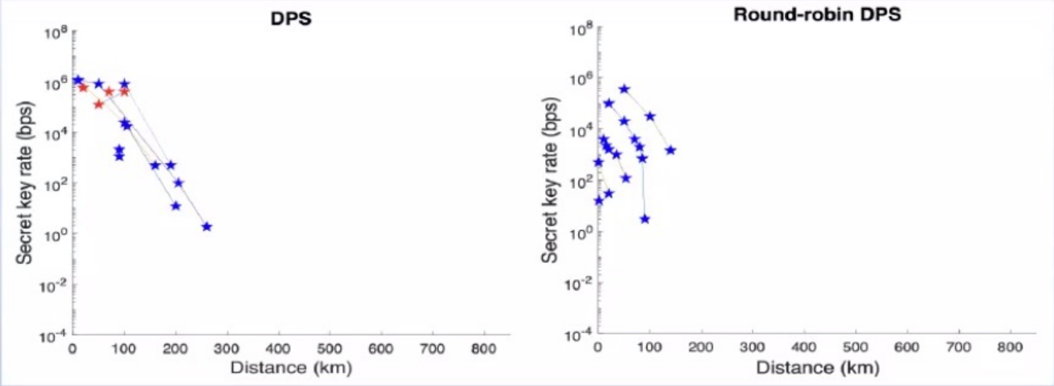
QKD Protocols – BB84 vs BBM92



Performance Evaluation: Demonstrated secret key rates



Performance Evaluation: Demonstrated secret key rates



Decoy-state BB84	Max distance	Max rate
Restricted attacks	421 km – 0.25 bps (Finite Collective)	13.72 Mbps - 400m (Finite Collective)
Finite-key & Coherent attacks	240 km – 8.4 bps 1034 km – 700 bps – (satellite)	10 Kbps – 150 km 1.32 Kbps – [600,1000] km (satellite)

MDI-QKD	Max distance	Max rate
Restricted attacks	54 dB loss – 8 bps (Asymptotic)	1.257 Mbps – 2.33 dB loss (Asymptotic)
Finite-key & Coherent attacks	404 km – 3.2×10^{-4} bps	6 Kbps – 42 km

TF-QKD	Max distance	Max rate
Restricted attacks	81.2 dB – 0.0176 Kbps (Asymptotic)	425.7 Kbps – 100 km (Asymptotic)
Finite-key & Coherent attacks	833.8 km – 1.4×10^{-2} bps	20.6 Kbps – 101 km

DPS	Max distance	Max rate
Restricted attacks	260 km – 1.85 bps (Asymptotic individual)	1.16 Mbps – 10 km (Asymptotic individual)
Finite-key & Coherent attacks	-	-

Round-robin DPS	Max distance	Max rate
Restricted attacks	140 km – 1.45 Kbps (Asymptotic)	360 Kbps – 50 km (Asymptotic)
Finite-key & Coherent attacks	90 km – 3 bps	20 Kbps -50 km

BBM92	Max distance	Max rate
Restricted attacks	71 dB – 0.02 bps (Asymptotic) (free-space) 248 km – 1.4 bps (Asymptotic)	30 Kbps – 30 dB (Asymptotic)
Finite-key & Coherent attacks	1120 km – 0.12 bps (satellite)	1120 km – 0.12 bps (satellite)

HD-QKD	Max distance	Max rate
Restricted attacks	43 km–1.2 Mbps (Finite Collective)	26 Mbps – 0.1 dB (Finite Collective)
Finite-key & Coherent attacks	145 km -0.42 Kbps	26.2 Mbps – 4 dB

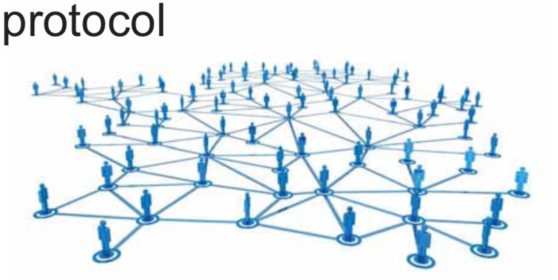
CV-QKD	Max distance	Max rate
Restricted attacks	202.81 km – 6 bps (Finite Collective)	327 Mbps – 5 km (Asymptotic)
Finite-key & Coherent attacks	-	-

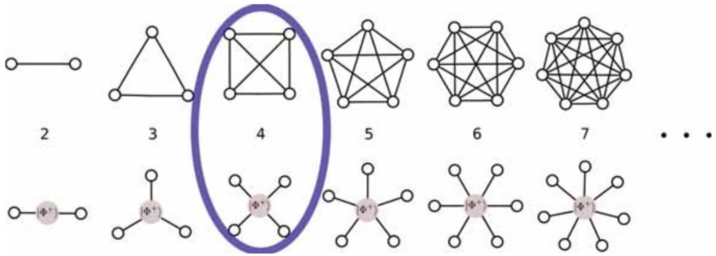
QKD Networks

QKD is inherently a point to point / peer to peer protocol

Mostly with 2 party implementations

Networks are a challenge!



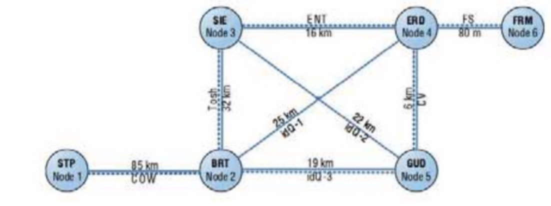


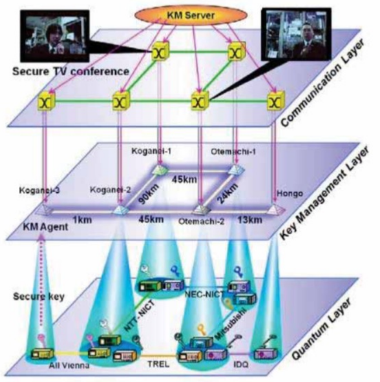
Fully connected networks are harder

QKD Networks

- Trusted nodes (i.e. lower security)
- Complex and resource hungry

E.g. Tokyo, Vienna and China networks





CGTN news

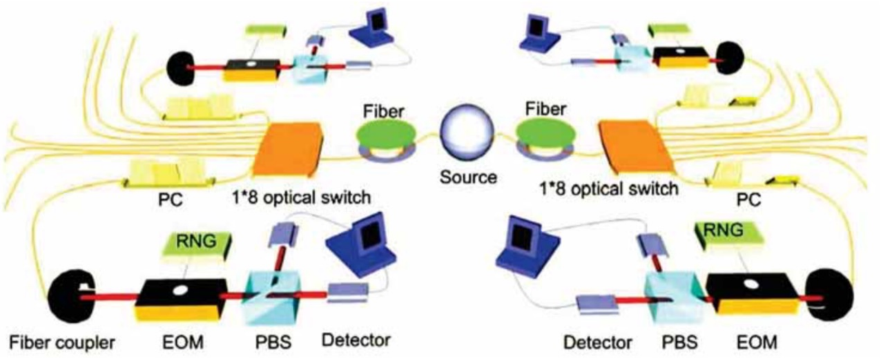
Sasaki, M., et al., Optics Express 19.11 (2011): 10387-10409
Peev et al, New Journal of Physics 11 (2009) 075001

http://spectrum.ieee.org/telecom/security/chinas-2000km-quantum-link-is-almost-complete

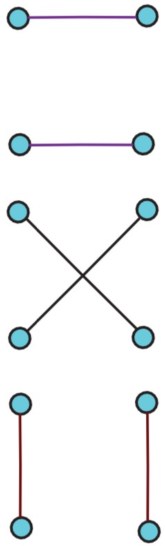
QKD Networks

E.g. Access networks

- Single source
- Many users



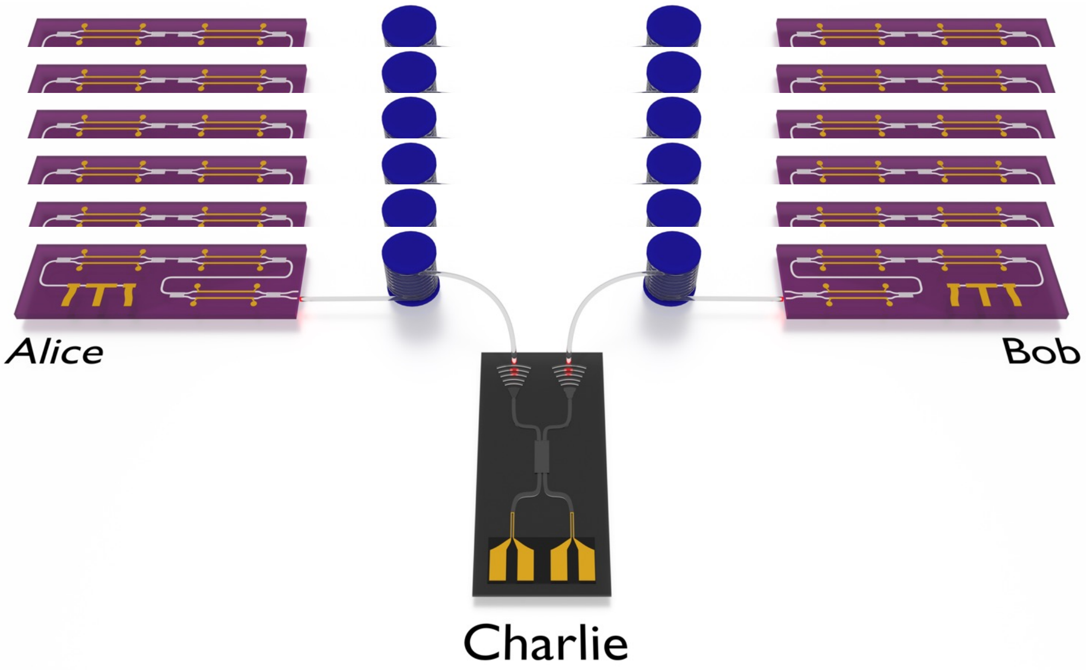
- Active switching (slow, no simultaneous access)
- Limited connectivity
- Not anonymous



B. Frohlich, et al. Nature 501, 69 (2013)

MDI QKD for Networks

- Resource sharing and scalability
  - Detection, time tagging and switching can be centralised
- N fibres instead of $\frac{1}{2}N(N-1)$
  - Reduced resources for fully connected graph
- Trusted node not required
- Cheap transmitters give access to quantum secured network



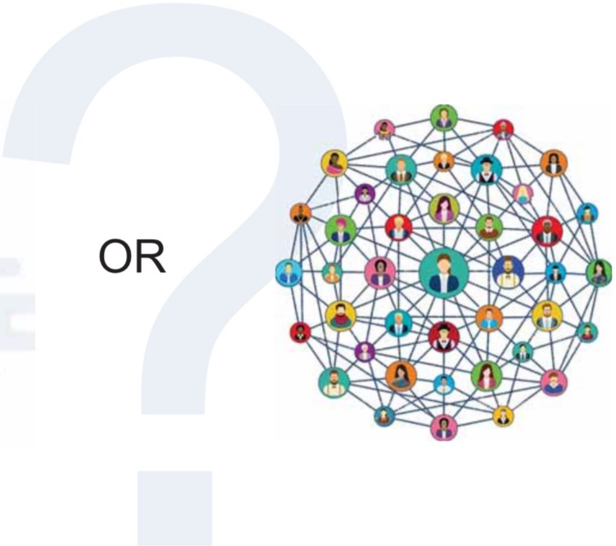
Integrated Switches

QKD between two parties is complex enough!

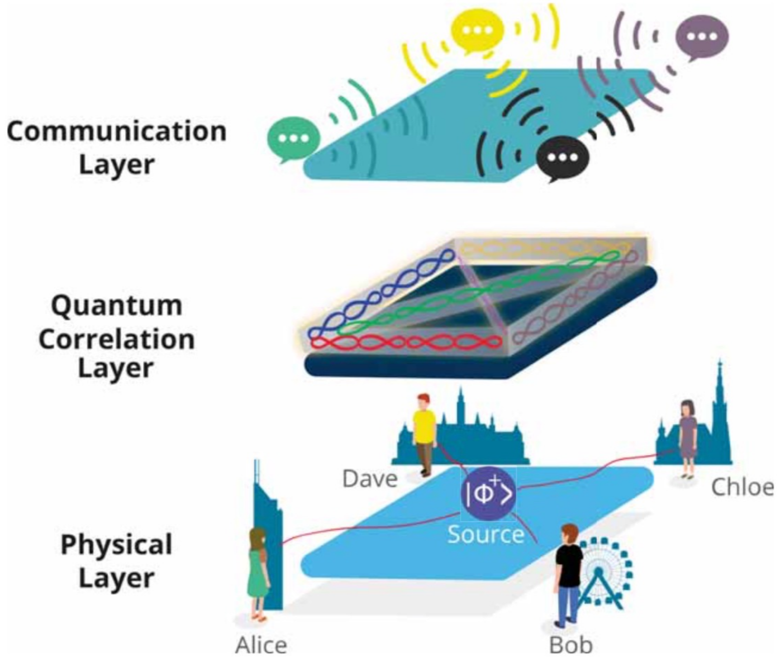
How can we connect

OR

OR



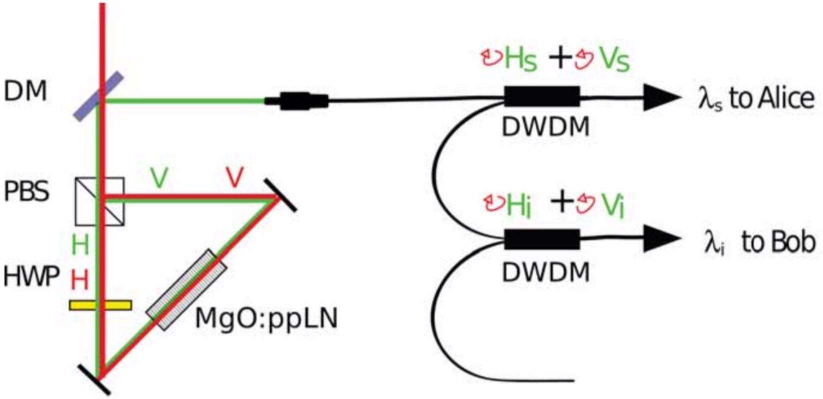
4 User entanglement distribution quantum network



Every user talks to every other user simultaneously

Share a different bi-partite entangled state between each pair of users

A single source of entanglement serves all users via just one fibre each

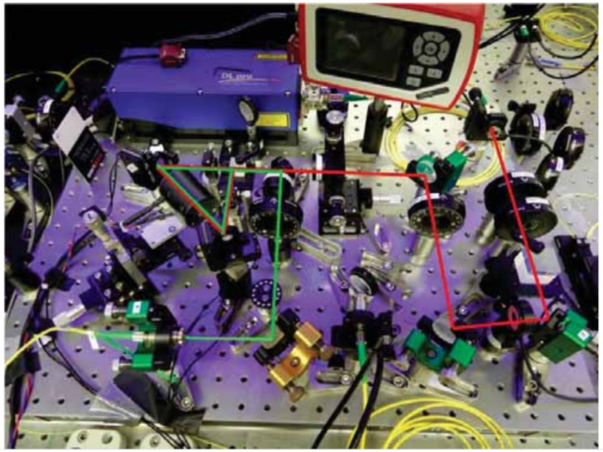


$$V_p \rightarrow V_s V_i$$

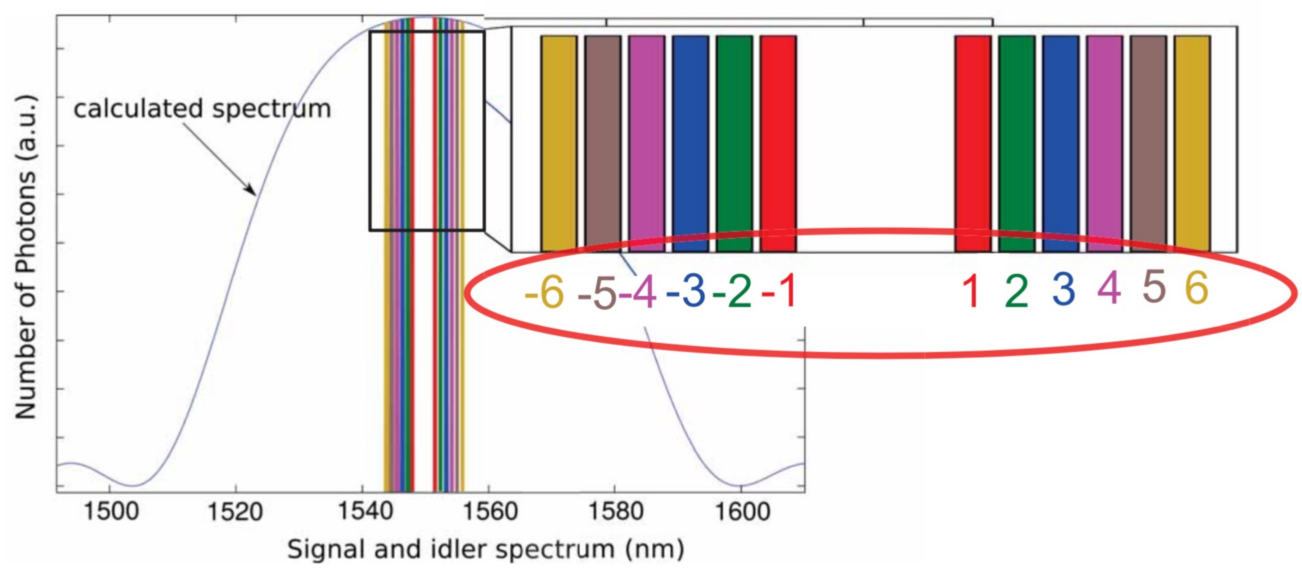
$$|\Phi\rangle = |\circlearrowright\rangle + e^{i\varphi}|\circlearrowleft\rangle$$

$$|\Phi^+\rangle = |H_s H_i\rangle + |V_s V_i\rangle$$

- Type 0
- Ultra bright
- Broadband



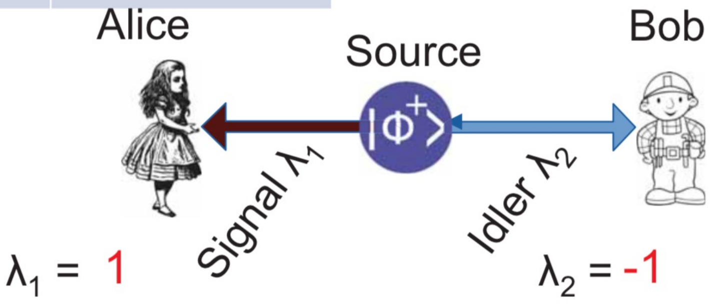
Nature 564 (7735), 225



Nature 564 (7735), 225

Key to creating the network is the method of combining wavelength channels

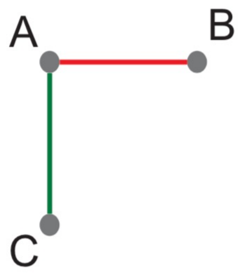
Alice	Bob	Chloe	Dave
1	-1		



Nature 564 (7735), 225

Key to creating the network is the method of combining wavelength channels

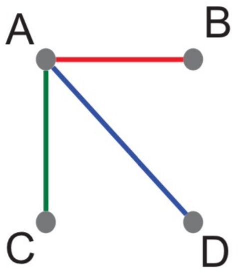
Alice	Bob	Chloe	Dave
1	-1	-2	
2			
3			



Nature 564 (7735), 225

Key to creating the network is the method of combining wavelength channels

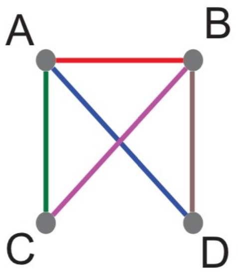
Alice	Bob	Chloe	Dave
1	-1	-2	-3
2			
3			



Nature 564 (7735), 225

Key to creating the network is the method of combining wavelength channels

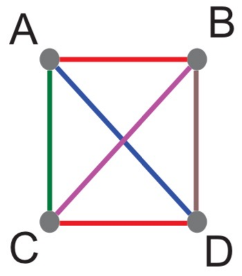
Alice	Bob	Chloe	Dave
1	-1	-2	-3
2	4	-4	-5
3	5		



Nature 564 (7735), 225

Key to creating the network is the method of combining wavelength channels

Alice	Bob	Chloe	Dave
1	-1	-2	-3
2	4	-4	-5
3	5	6	-6



Now we have a fully connected entanglement based network

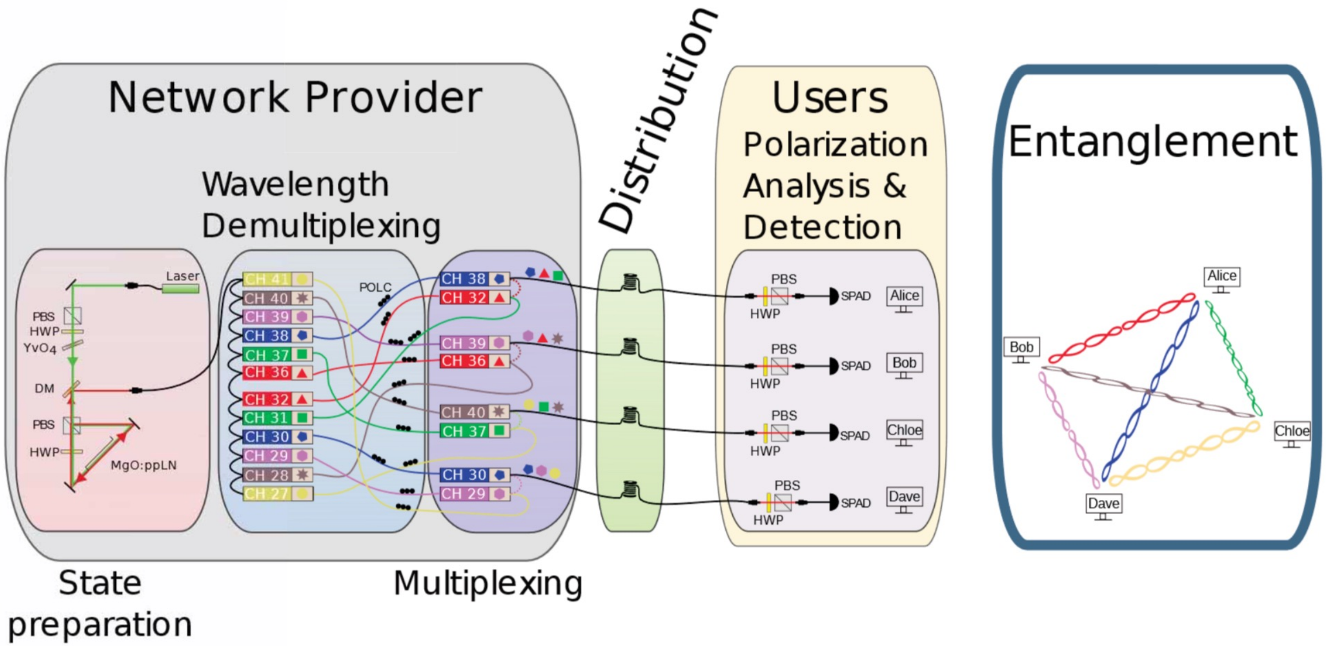
Nature 564 (7735), 225

Key to creating the network is the method of combining wavelength channels

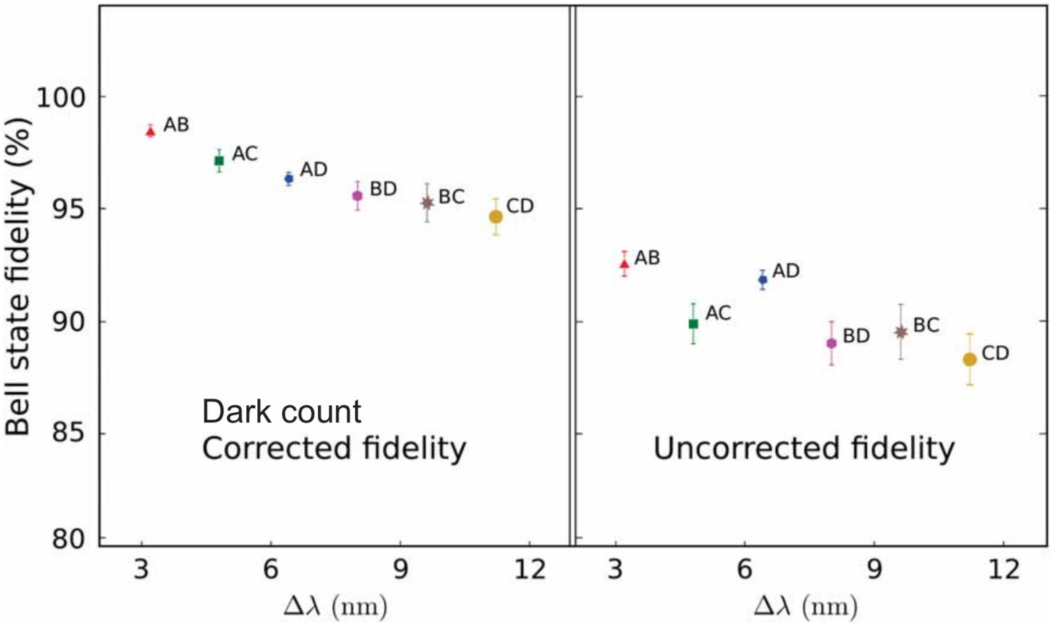
Alice	Bob	Chloe	Dave
1	-1	-2	-3
2	4	-4	-5
3	5	6	-6

As simple as choosing who gets which wavelength!

Nature 564 (7735), 225



Nature 564 (7735), 225



Every one shares bi-partite entanglement

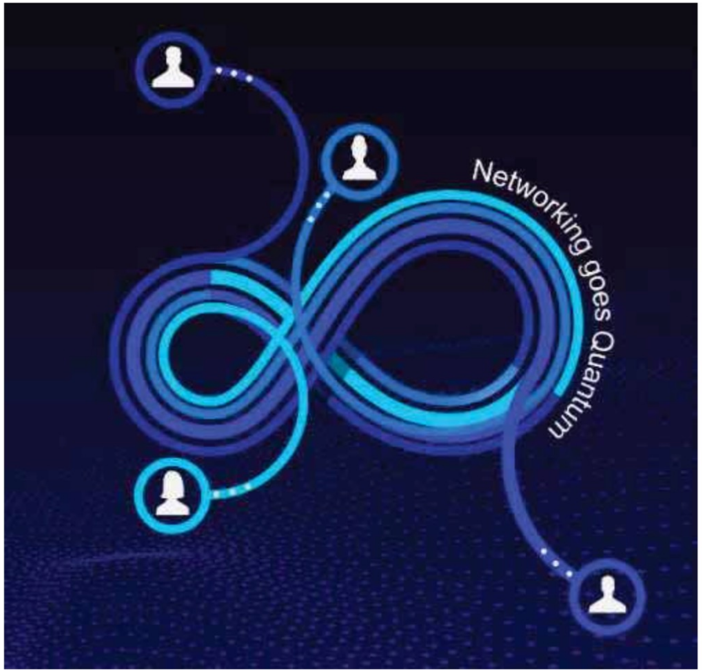
Network feasible despite noise.

1.5 Kcps dark, ≈1% detection efficiency,

1 ns jitter.

Nature 564 (7735), 225

8 User metropolitan quantum networks



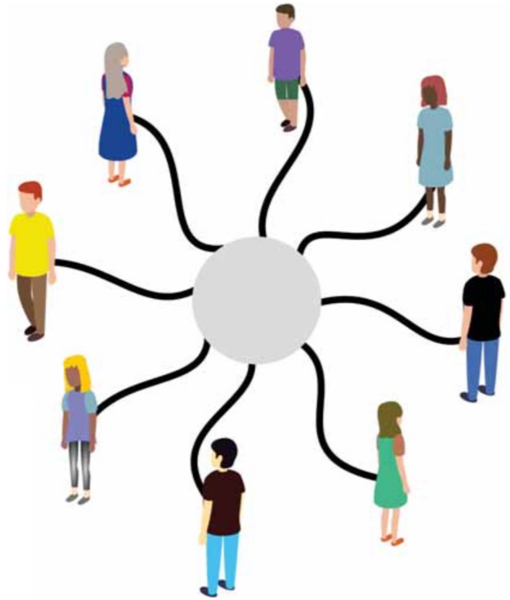
Double the number of users

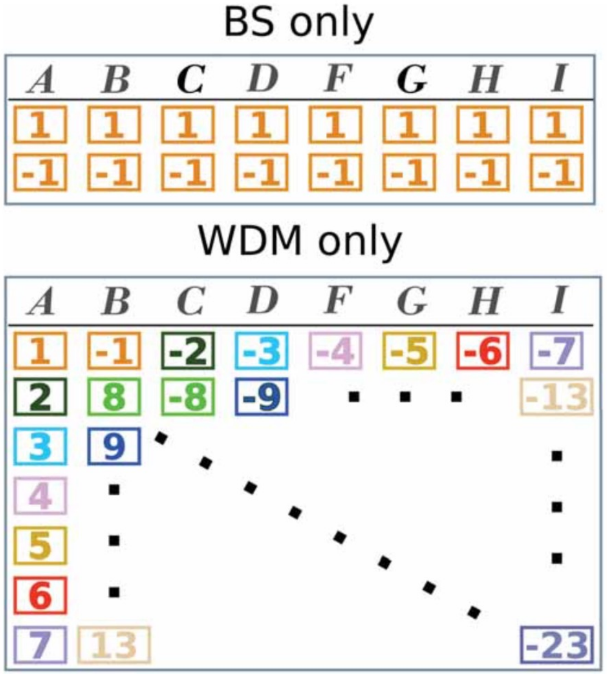
Improve scaling

Go from entanglement distribution to full QKD

Demonstrate QKD in real environments

Incorporate traffic management





Uses *n*-fold BS, every link has *1/2ⁿ* loss due to BS. User side filtering impossible

Uses *n(n-1)* wavelength channels. User side filtering can completely reverse adverse effects of multiplexing

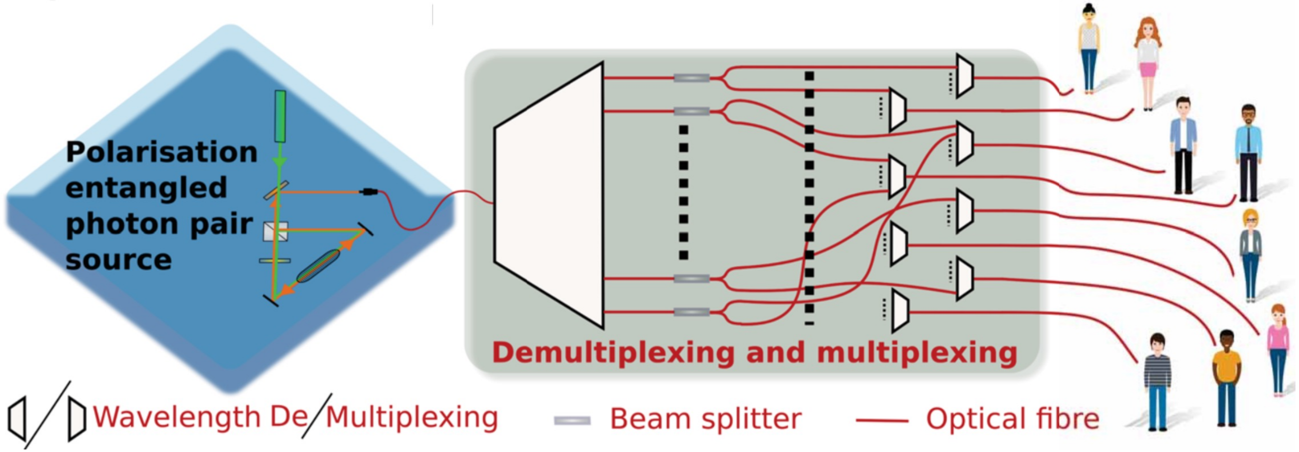
New J. Phys., vol. 13, p. 063039, 6 2011, Nature, vol. 501, pp. 69, 9 2013, Nature, vol. 385, pp. 47, 1997
Nature 564 (7735), 225

Combining both solutions to **improve scaling**

Subgroups

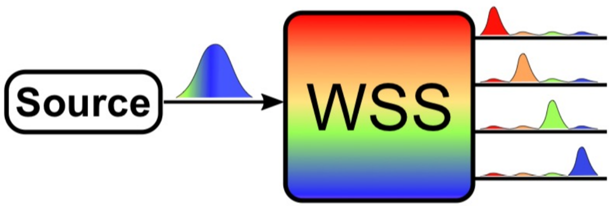
A	*B*	*C*	*D*	*F*	*G*	*H*	*I*
8	-8	-7	-6	8	-8	-7	-6
7	5	-5	-4	7	5	-5	-4
6	4	3	-3	6	4	3	-3
2	2	1	1	-2	-2	-1	-1

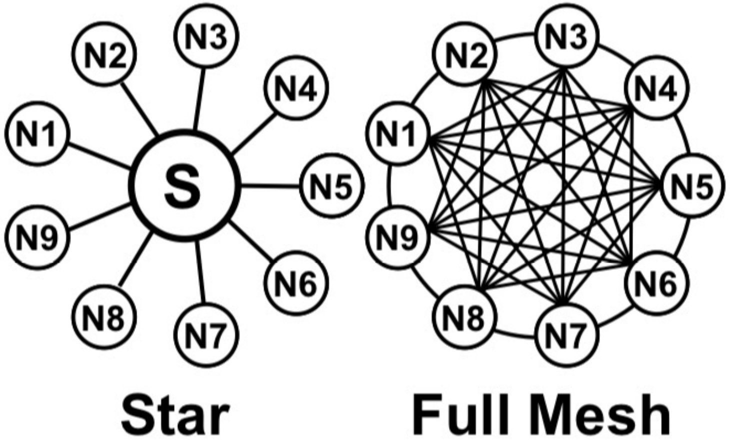
Divide network into identical subgroups each with a WDM only topology. Additional channels used to interconnect subgroups. Combines above topologies. Uses $2n$ wavelength channels

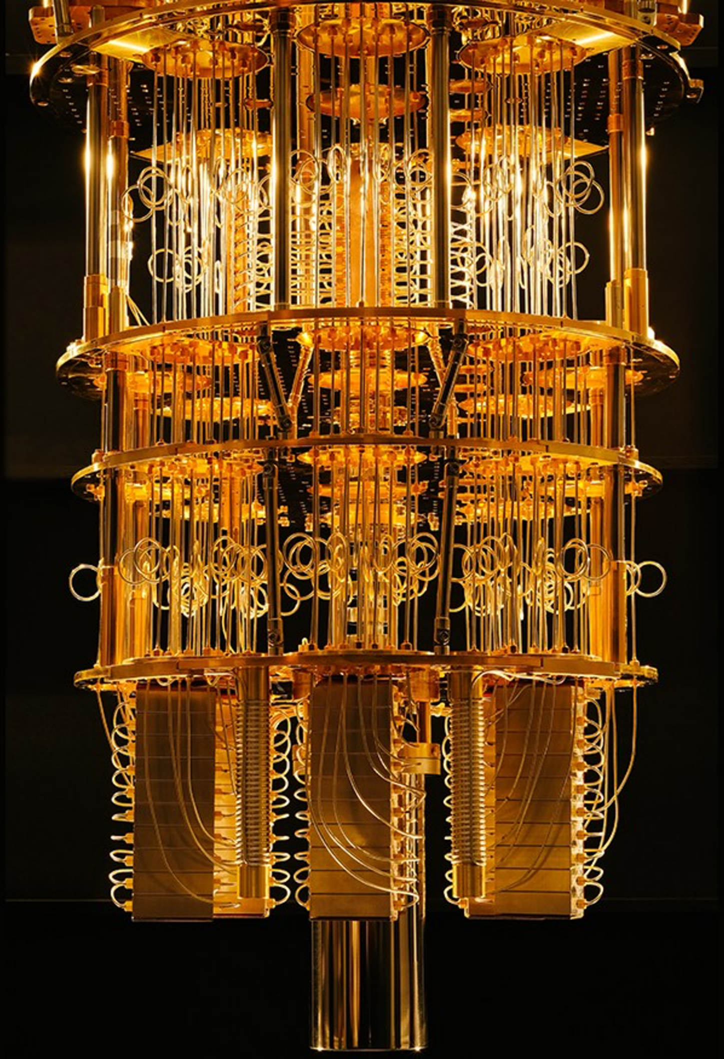


Entanglement-based QKD

There are many different quantum protocols for key distribution. The entanglement-based protocols are the only ones offering the unique feature of sharing of sharing a key between all users of a given topology without having to establish a physical link. They all inherit the correlations by being connected to the same source of entanglement.







Thank you for your attention !

Let's keep in touch !

LinkedIn → Djeylan Aktas, PhD
E-mail → Djeylan.aktas@savba.sk