DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION WITH SINGLE-PHOTON SOURCES

Alejandro Mattar, Janek Kolodynski, Daniel Cavalcanti, Antonio Acin

ICFO – The Institute of Photonic Sciences, Barcelona, Spain

Paul Skrzypczyk

University of Bristol, UK

Konrad Banaszek

University of Warsaw, Poland

Quantum Optics IX

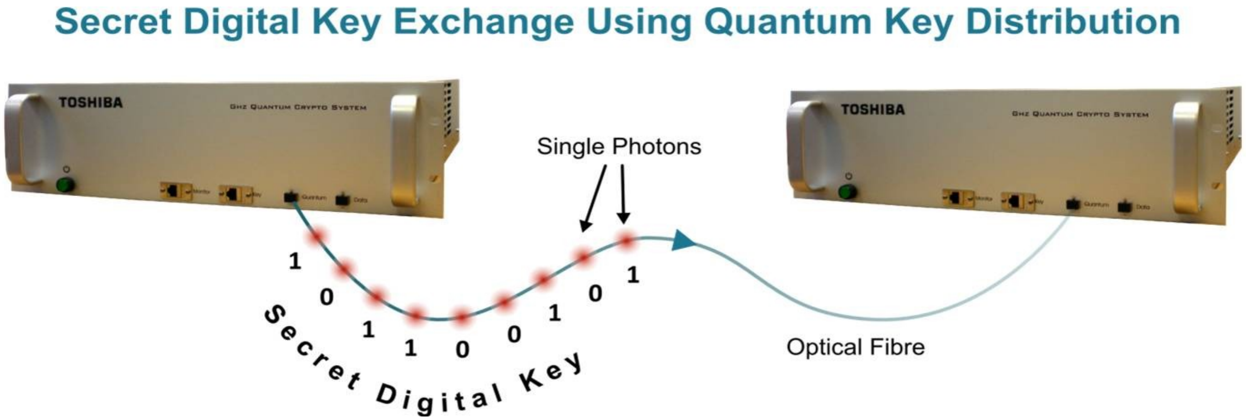
17-23.09.2017, Gdańsk, Poland

WHAT IS THE CURRENT STATUS OF QUANTUM KEY DISTRIBUTION?

IT IS COMMERCIALLY AVAILABLE…

COMPANIES SUCH AS TOSHIBA, MAGIQ, ID QUANTIQUE… :

Alice
A



Bob
B

Commercial devices implementing BB84, SARG, COW (iDQ),… protocols.

OK, BUT THE ABOVE IMPLEMENTATIONS HAVE BEEN “HACKED”?

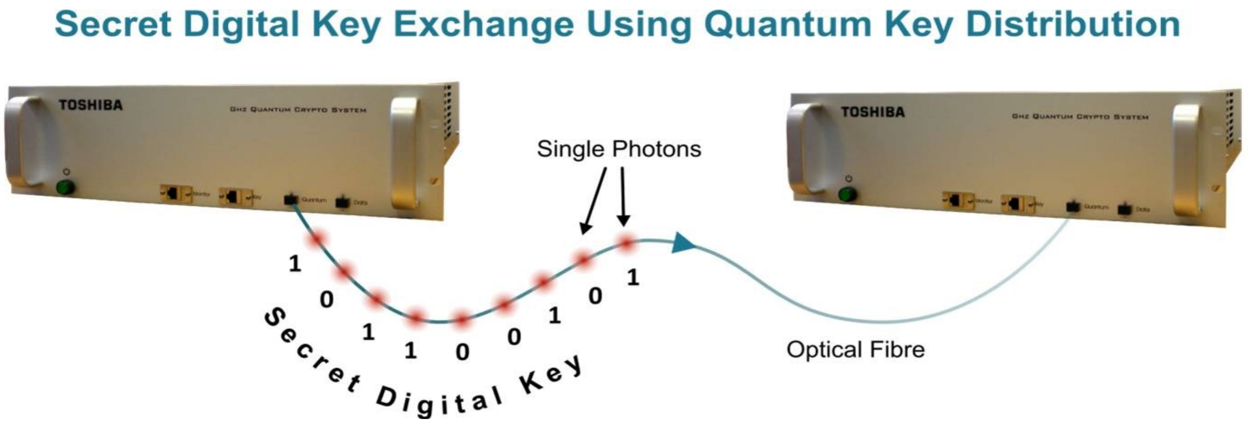
RESEARCHERS WERE ABLE TO EAVESDROP AND CAPTURE THE KEY WITHOUT LEAVING ANY TRACE!

IT IS THE DEVICES THAT HAVE BEEN CRACKED AND NOT THE CONCEPT OF QKD!

[*Lydersen et al.*, **Nature Photonics 4 (2010)**]

“HACKING” QUANTUM KEY DISTRIBUTION

Alice
A



Bob
B

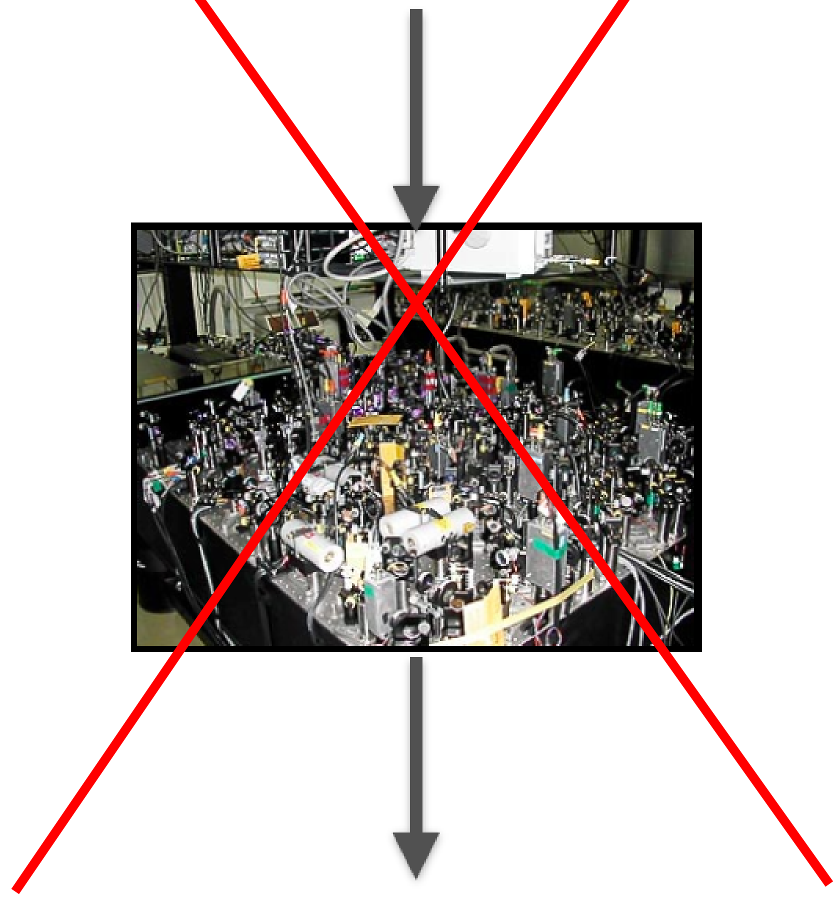
(devices implementing any BB84, SARG, COW (iDQ) QKD protocols)

- After the end of the *key distribution* protocol devices announce:
  “A **secure** key has been successfully established and reads #$%#$&….”
- This means that the **error rate** has been verified to be below a certain threshold (**$< \varepsilon\%$**), which “**guarantees**” by laws of quantum physics that no-one can have access to the key.
- Ok, but this **$\varepsilon\%$** is derived **assuming a particular (quantum mechanical) model of the devices** importantly modelling: *optical fibres*, *detectors*, *electronics*, *losses*, *detection inefficiencies* etc.
- **HACKING:**
  Explore other degrees of freedom that are not accounted for in the model, whose presence invalidates the proofs of security.

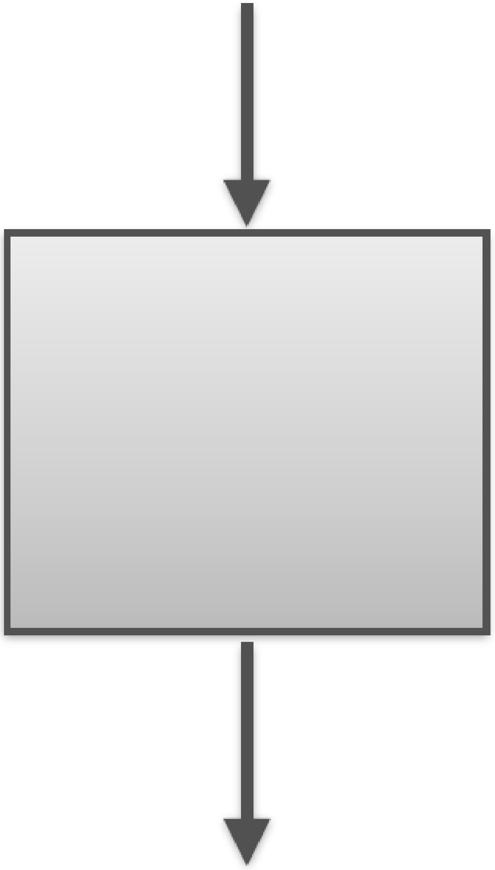
IT IS ALL ABOUT THE MISMATCH BETWEEN THE THEORETICAL REQUIREMENTS AND THE IMPLEMENTATION!

IS THERE A WAY AROUND THIS?

Solution A:
Control all the underlying quantum processes inside the device.

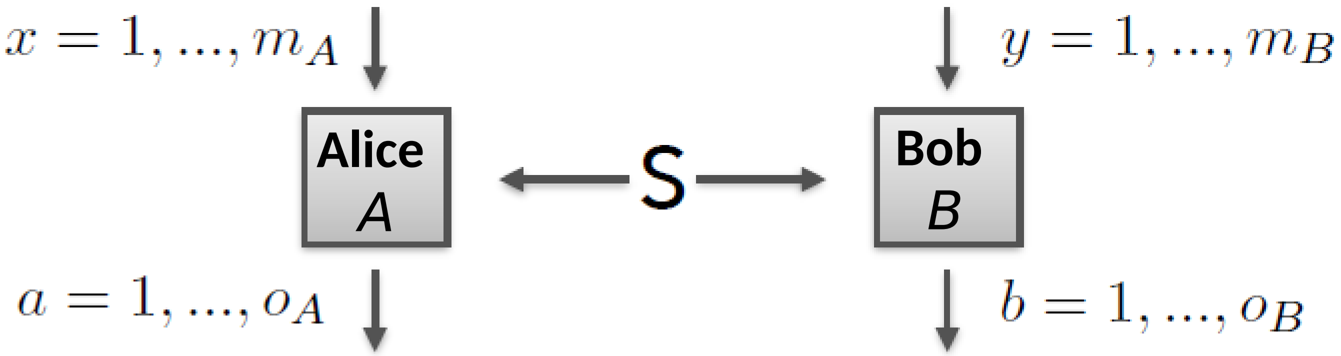


Solution B:
Make no assumptions about the internal working of the device.



SOLUTION B: DEVICE-INDEPENDENT (DI) APPROACH

Treat the devices as **black boxes** with:
- **input** buttons {*x*,*y*} (*QKD: randomly chosen measurement settings*)
- **output** bulbs {*a*,*b*} (*QKD: outcomes of the implemented measurements*):



$$P(a, b|x, y)$$

Assure the security basing on the **probability distribution (*behaviour*)** $P(a, b|x, y)$ that Alice and Bob may reconstruct from some subset of data using the classical authorised channel (*they call one another*).

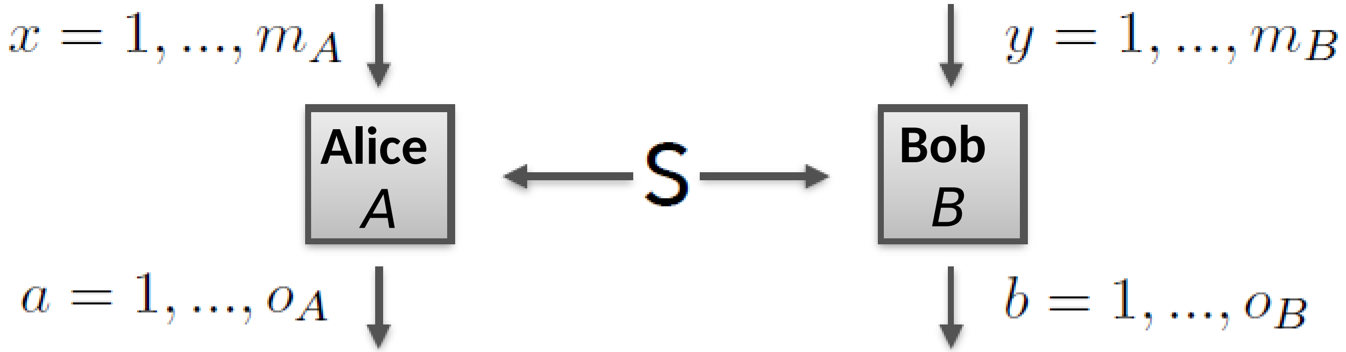
This is possible as $P(a, b|x, y)$ ideally exhibits **non-local correlations** that cannot be explained with **classical physics** but only with **quantum mechanics** → **Bell violation**.

DRAWBACK:
Such approach is very **sensitive to noise**. After introducing imperfections (*transmission*, *detection losses*, *etc.*) in devices, the *correlations quickly become classically explainable* **(detection loophole)**.

[*Acin et al.* **Phys. Rev. Lett. 97 (2007)**, *Barrett et al.*, **Phys. Rev. Lett. 95 (2005)**]

BELL VIOLATION IN 2 SLIDES

At each round of the test, Alice and Bob perform measurements x and y on some part of a system S and retrieve outcomes a and b:



$x = 1, \dots, m_A$

$y = 1, \dots, m_B$

Alice
A

S

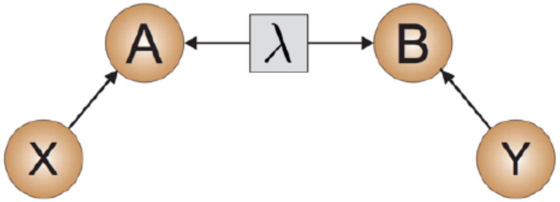
Bob
B

$a = 1, \dots, o_A$

$b = 1, \dots, o_B$

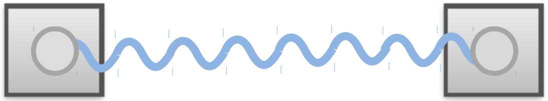
$$P(a, b|x, y)$$

- **Classical** explanation of correlations – **Local Hidden Variable Model** (LHVM):



$$P_L(a, b|x, y) = \sum_{\lambda} p(\lambda)\, p_\lambda(a|x)\, p_\lambda(b|y)$$

- **Quantum mechanics** allows for stronger **nonlocal** correlations to be shared:



$$P_Q(a, b|x, y) = \mathrm{Tr}\{\rho_{AB}\ M_{a|x} \otimes M_{b|y}\}$$

(...much richer structure)

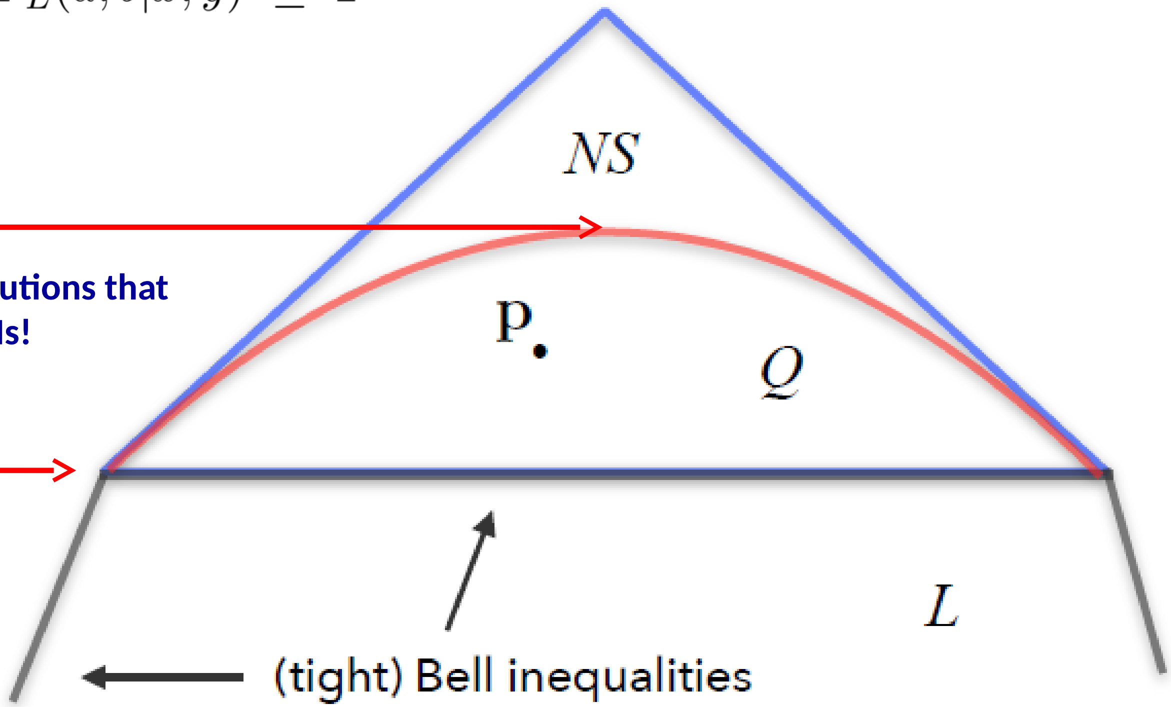
BELL INEQUALITIES - GEOMETRIC REPRESENTATION

Bell inequality S – upper bound on a (linear) functional of the *behaviour*

$$\sum_{a,b,x,y} S_{a,b,x,y}\, P_L(a,b|x,y) \;\leq\; S_L$$ ← a constant valid for **all** LHVMs

e.g., **CHSH** inequality (**2 inputs, 2 outcomes**): $S_{a,b,x,y} = (-1)^{a+b+xy}$ $\quad S_L = 2$

$$\sum_{a,b,x,y} (-1)^{a+b+xy}\, P_L(a,b|x,y) \;\leq\; 2$$



$S_Q = 2\sqrt{2}$ →

Quantum mechanics allows for distributions that are not explainable by LHVMs!

$S_L = 2$ →

← (tight) Bell inequalities

$\mathbf{p} = \{\; P(a,b|x,y) \;\}$ $\quad$ ($o_A\, o_B\, m_A\, m_B$ elements)

[*Bell J.*, **Physics 1 (1964)**]

GUESSING PROBABILITY OF AN EAVESDROPPER

For a given **Bell inequality** S and its **violation** S_{obs} by the **observed behaviour** $\mathbf{p}_{obs}$ one can explicitly calculate the **guessing probability**, i.e.,

The maximal probability that an eavesdropper correctly guesses the outcome of a box (A) can upper bounded for a particular S by:

$$P_{guess}(S) \quad = \quad \max \; P(a|x)$$

$$\text{s.t.} \; \begin{cases} \sum_{a,b,x,y} S_{a,b,x,y} \, P(a,b|x,y) \; = \; S_{obs}[\mathbf{p}_{obs}] \\ P(a,b|x,y) \in Q \end{cases}$$

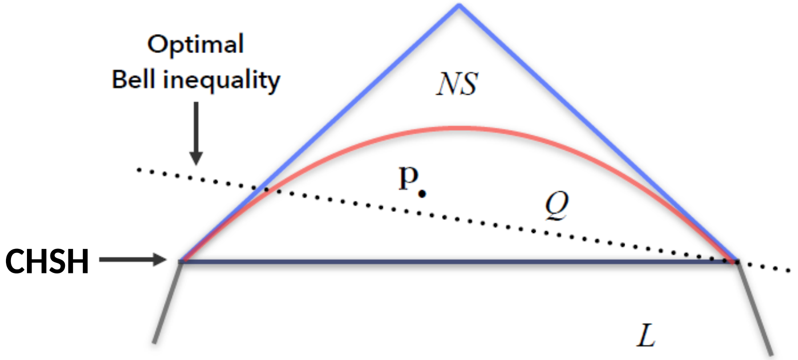
Quantum set Q is a convex space but not a simplex

need Semi-Definite Programming (SDP) tricks, i.e., the NPA hierarchy.

[*Navascues et al.*, **PRL 98 (2007)**]

Furthermore, one should **optimise over all Bell inequalities** to make the guessing probability (and, hence, the *power of eavesdropper*) as **small** as possible.

$$P_{guess} := \min_{S} \; P_{guess}(S)$$

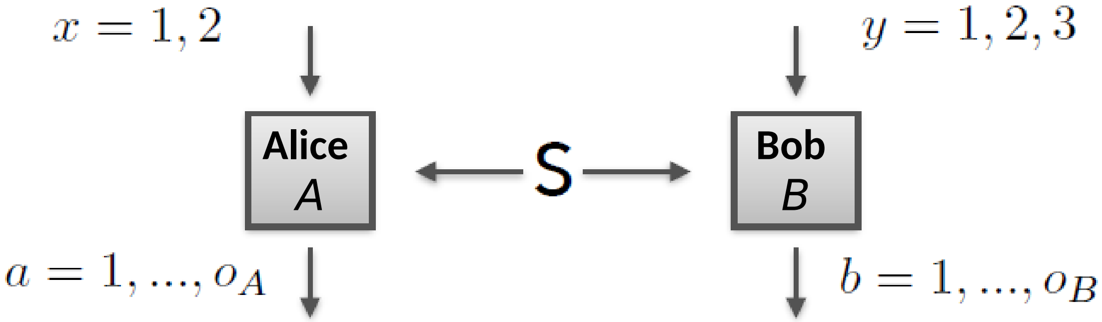


A ***convex*** problem – again efficiently solvable by an **SDP**

[*Colbeck R.*, **PhD Thesis, Cambridge (2009)**; *Pironio et al.*, **Nature 464 (2010)**]

KEY RATE IN DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION

DI-QKD protocol:



- All rounds for which $y \neq 3$ are used to generate $\mathbf{p} = \{P(a, b|x, y)\}$.
- From $\mathbf{p}$ Alice and Bob construct (as discussed before) P_{guess}.
- Rounds in which $x=1$ and $y=3$ are used to generate the key.
- The key rate of the DI-QKD protocol is lower-bounded by:

$$\boxed{r \geq -\log_2(P_{guess}) - H(x = 1|y = 3)}$$

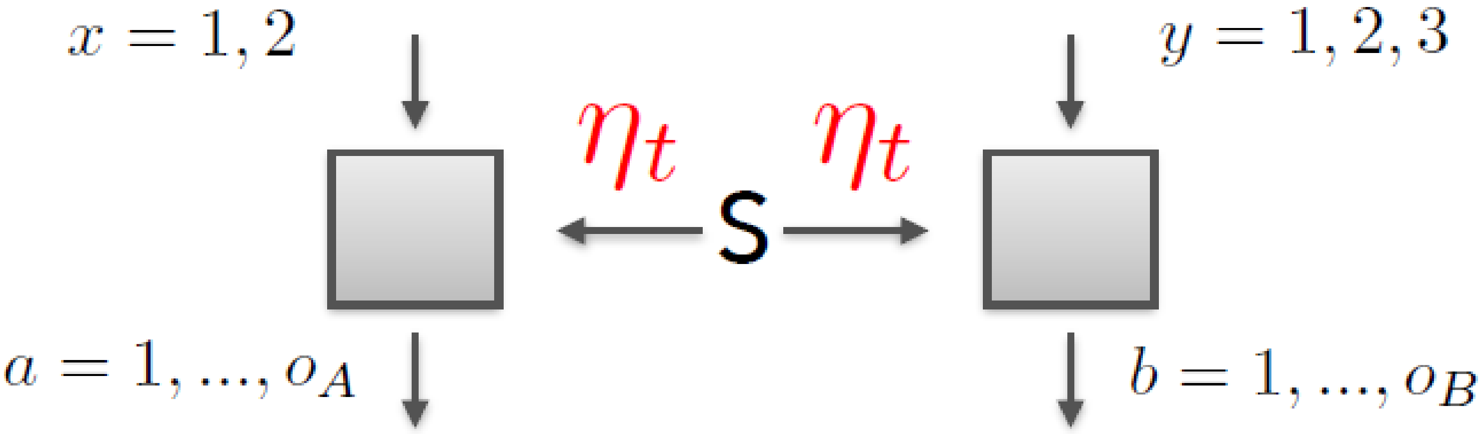
power of the eavesdropper to know the key

bits that have to be published during the error correction step in QKD

It is not just enough to violate a Bell inequality to do DIQKD !!

[*Masanes et al.* **Nat. Comms 2** (2011), *Pironio* et al. **PRX 3** (2013)]
[*Vazirani & Viddick* **PRL 113** (2014), *Arnon-Friedman* et al. arXiv:**1607.01797**]

PROBLEM 1: OF TRANSMISSION LOSSES



Loss in optic fibres decays exponentially with distance: $\eta_t = \mathrm{e}^{-L/L_{att}}$

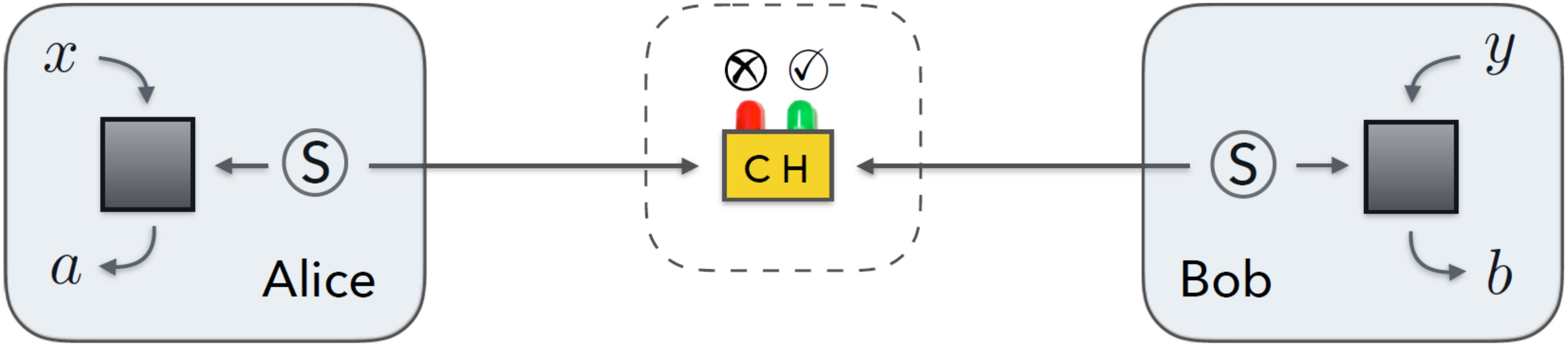
With $L_{att} = 22\ km$, for a distance $L = 10\ km$ we have: $\eta_t \approx 60\%$

- **66% is the fundamental limit to violate any Bell Inequality (not to mention DIQKD) ▮▮**
- **For long distance communications we should not hope for technological progress to resolve the problem…**

SOLUTION 1:
HERALDING (WITHOUT OPENING THE DETECTION LOOPHOLE)

Side-Heralding (*a'la amplification*)**:**

Central-Heralding (*a'la entanglement swapping, quantum repeaters*)**:**



PROBLEM 2:

"STANDARD HERALDING" WITH SPONTANEOUS PHOTON-PAIR SOURCES IS OF NO USE!

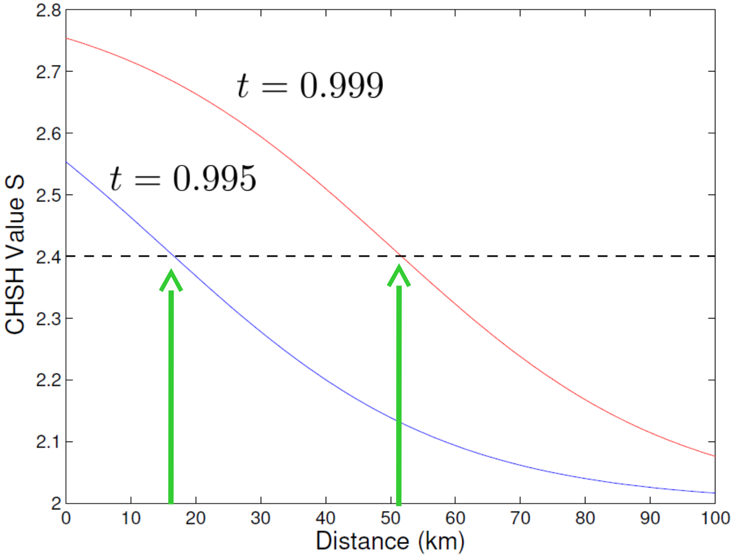
Imagine that *Alice* and *Bob* share (inside the boxes) an **entangled** photon-pair produced in **spontaneous parametric down-conversion (SPDC)** process with heralding implemented via, e.g., "*qubit amplification*" ($t \approx 1$) [*Gisin et al.* **PRL 105 (2010)**]:

$$\rho_{AB} = (1-p)(1-t)^2\,|vac\rangle\langle vac| + p\,\eta_t t(1-t)\,|\psi_-\rangle\,\langle\psi_-|$$

Let us consider the **CHSH value of Bell violation**: $S = 2\left[1 + \frac{p\,\eta_t\,t\,(\sqrt{2}-1)}{(1-p)(1-t)+p\,\eta_t\,t}\right]$

CHSH value S exponentially quickly approaches the local value $S_L = 2$ with distance.

[**intuition:** *vacuum terms always eventually dominate as they are O(1) in p.*]



$$\eta_t = \mathrm{e}^{-\frac{D}{D_{att}}}$$

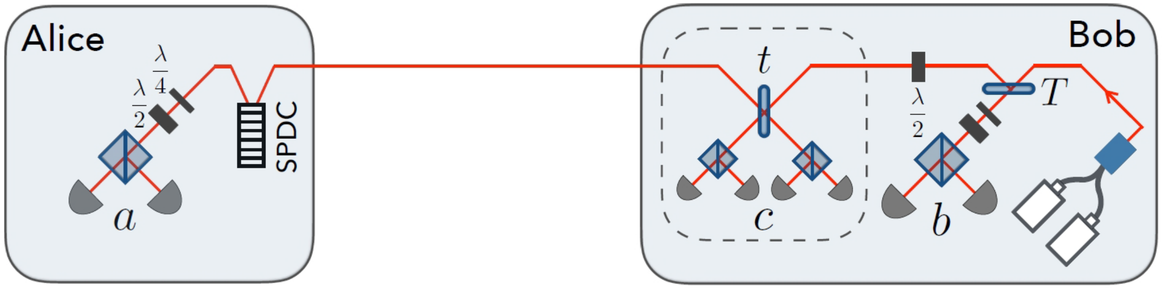
← $S \approx 2.4$ required for **positive key rates**, $r > 0$.

SOLUTION 2:

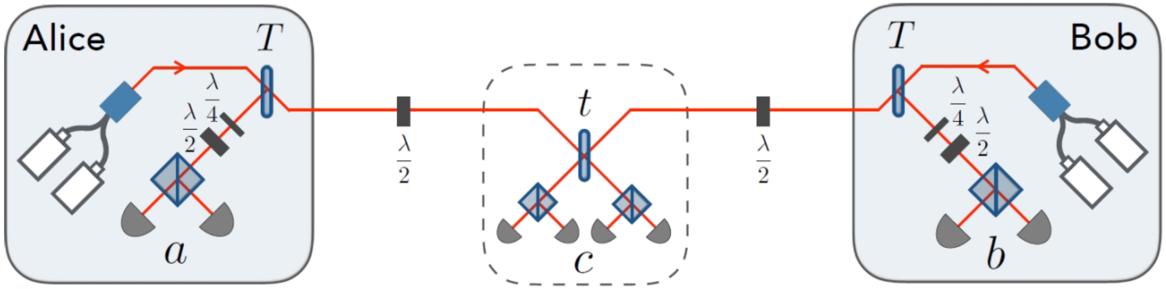
EMPLOY SINGLE-PHOTON SOURCES !!!

DIQKD SCHEMES WITH SIDE- AND CENTRAL-HERALDING

Side-Heralding (1 SPDC, 2 SPSs) [“*Qubit amplifier*” inspired by *Pitkanen et al.* **PRA 84 (2011)**]:



Central-Heralding (4 SPSs) [“*Quantum repeater*” inspired by *Lasota et al.* **PRA 90 (2014)**]:



OPTIMIZING PARAMETERS t, T FOR EACH SCHEME, ASSUMING SOURCES:

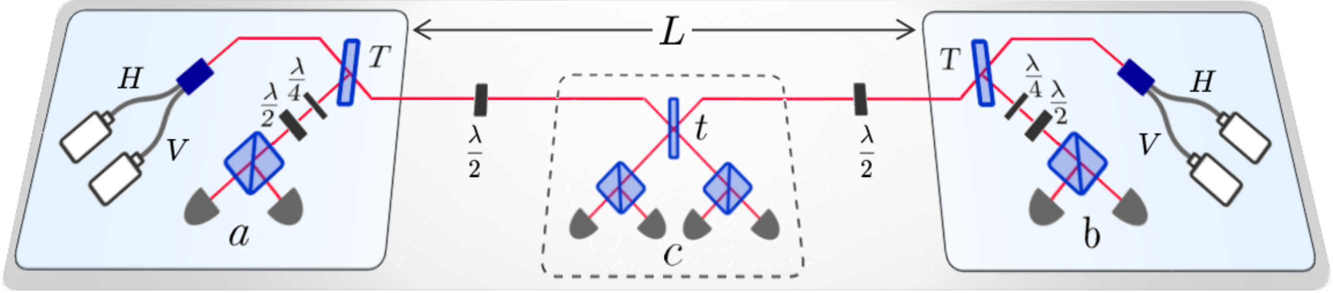
$$\sigma = \sum_{n=1}^{\infty} p^{n-1} |n\rangle\langle n| \ \ (\text{with } p = 10^{-4})$$

DIQKD Scheme:	Side-heralding (SH)	Central-heralding (CH)
Critical detection efficiency $\eta_d^\star$ *(diqkd)*	94.9%	94.3%
Critical detection efficiency $\eta_d^\star$ *(nonloc.)*	74.3%	69.2%
Noise robustness (nonloc.)	31.2%	35.7%
Secret key per heralded round (bit fraction ≤ 1*)*	0.82	0.95

η_d ← **detection efficiency inside one (Alice or Bob) lab** (*fibre coupling, transmission to detectors, detectors inefficiencies*).

DIQKD CH-SCHEME PERFORMANCE

Central-heralding (CH) scheme:



DIQKD Key rates:

Assumptions:

$\eta_d = 0.95$

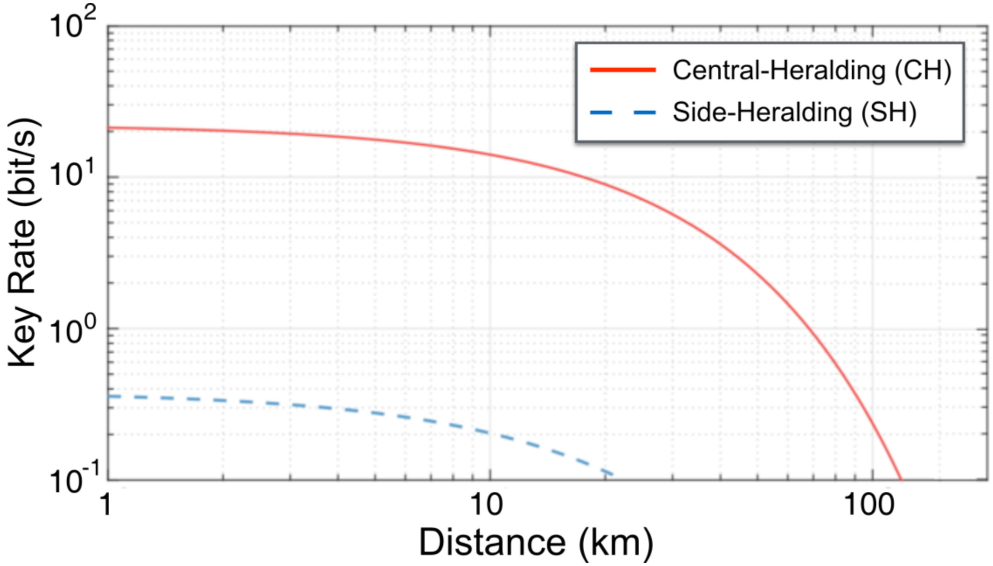
$D_{att} = 22\,\mathrm{km}^{-1}$

$p_{\mathrm{SPS}} = p_{\mathrm{SPDC}} = 10^{-4}$

$R_{\mathrm{SPS}} = 100\,\mathrm{MHz}$

$R_{\mathrm{SPDC}} = 10\,\mathrm{GHz}$

Note that the effective rates of SPDCs and SPs are the same!



MAIN MESSAGE:

If already now we were able to get the effective detection efficiency of a device *(i.e., all single-photon creation, source-detector transmission and detection efficiencies combined)* **up to *95%*, we would be able to do DIQKD over 50kms at a rate 1bit/sec!**