What theorists should know when working with experimentalists

Marcos Curty
University of Vigo

QCrypt 2013

Outline

- Motivation
- Characterisation of experimental components
- QKD with decoy states (asymptotic case)
- Parameter estimation (finite case)
- Side-channels

Motivation

MOTIVATION

From a theoretically point of view, a QKD system is rather simple. For instance, in the BB84 protocol:

Signals sent by Alice:	$\updownarrow$	$\leftrightarrow$	⤢	⤡	$\leftrightarrow$	⤡	⤡
Bob's measurements:	$+$	$\times$	$\times$	$+$	$+$	$\times$	$+$
Bob's results:	$\updownarrow$	⤢	⤢	$\leftrightarrow$	$\leftrightarrow$	⤡	$\updownarrow$
Sifted bits:	1	×	0	×	0	1	×

C.H. Bennett and G. Brassard, Proc. IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, (IEEE, New York), p. 175 (1984).

MOTIVATION

From a theoretically point of view, a QKD system is rather simple. For instance, in the BB84 protocol:

Signals sent by Alice:	↕	↔	⤢	⤡	↔	⤡	⤡
Bob's measurements:	✛	⤧	⤧	✛	✛	⤧	✛
Bob's results:	↕	⤢	⤢	↔	↔	⤡	↕
Sifted bits:	1	×	0	×	0	1	×

C.H. Bennett and G. Brassard, Proc. IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, (IEEE, New York), p. 175 (1984).

Secret key rate:

$$K \propto 1 - h(e_{\text{bit}}) - h(e_{\text{phase}})$$

P.W. Shor and J. Preskill, PRL 85, 441 (2000).

MOTIVATION

In practice, however, the situation looks less simple.

QPN 5505 commercial QKD system from MagiQ Technologies (Image taken from http://www.vad1.com)

MOTIVATION

In practice, however, the situation looks less simple.

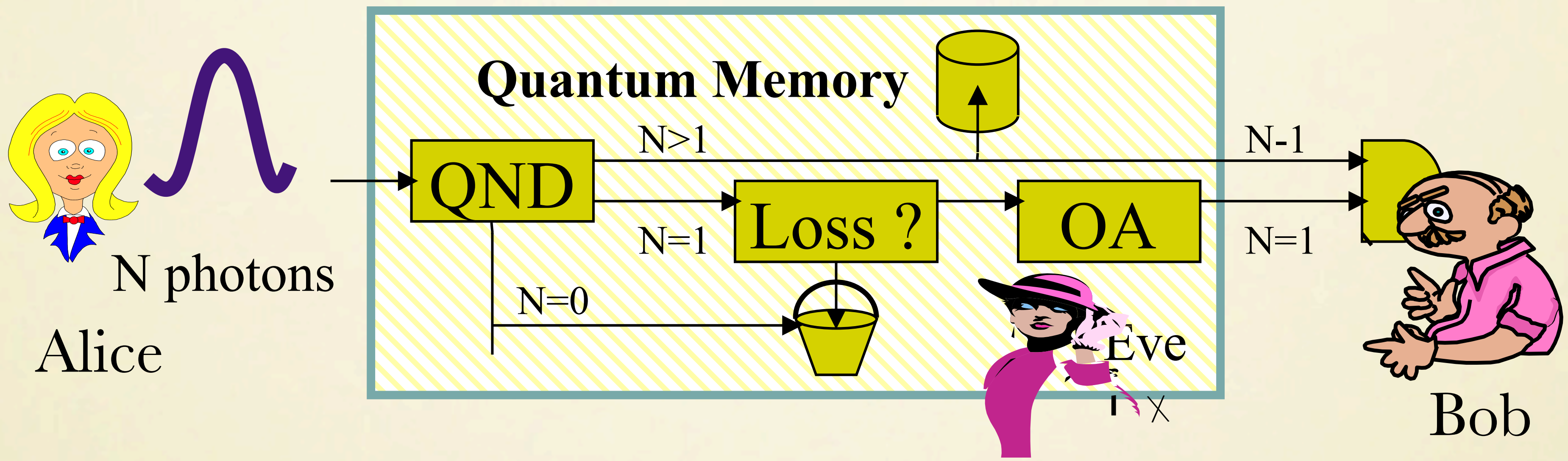
For instance:

- Alice can emit signals that contain more than one photon prepared in the same polarisation state.
- Bob's detectors can output a double ``click'' due, for example, to dark counts.

QPN 5505 commercial QKD system from MagiQ Technologies (Image taken from http://www.vad1.com)

MOTIVATION

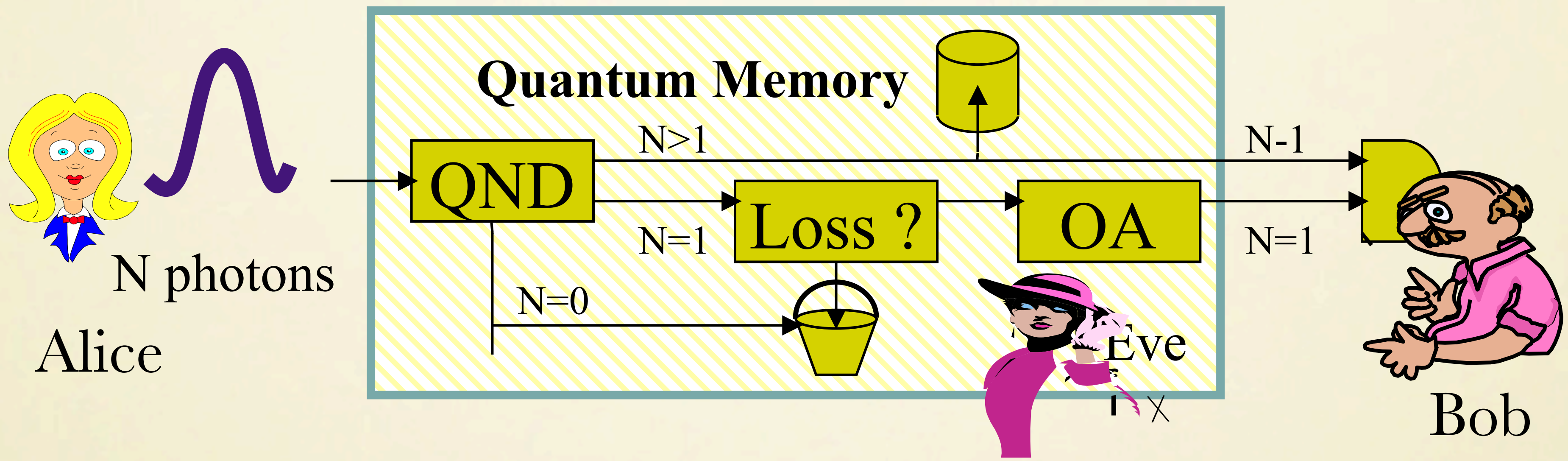
Example: Photon number splitting (PNS) attack.

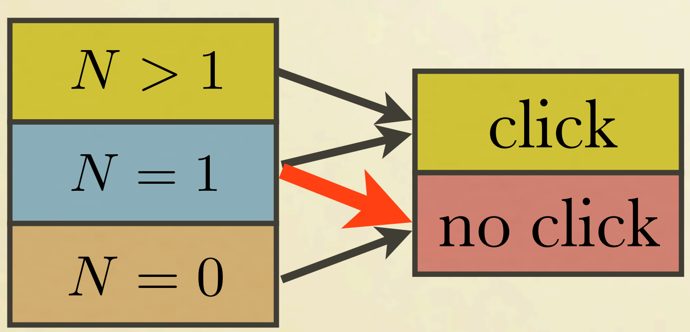


B. Huttner et al., PRA 51, 1863 (1995); G. Brassard et al., PRL 85, 1330 (2000).

MOTIVATION

Example: Photon number splitting (PNS) attack.





Eve has full information about the part of the key generated from multi-photon signals

$$K \leq p_{\text{exp}} - p_{\text{multi}}$$

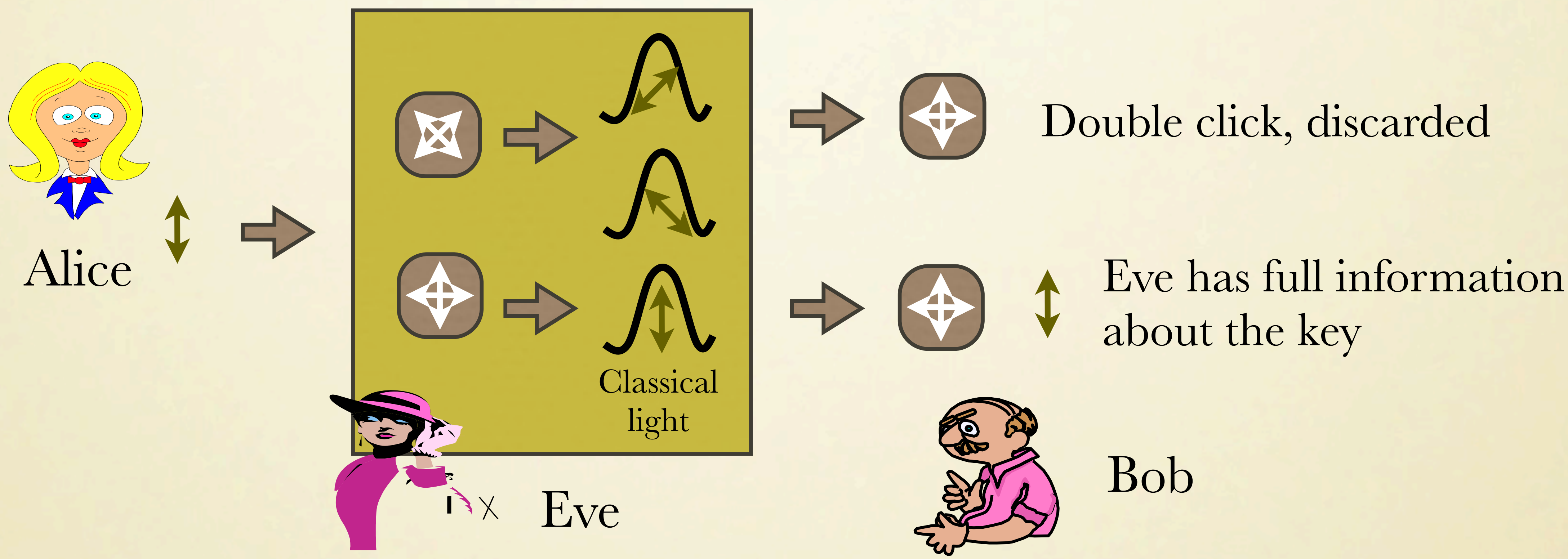
B. Huttner et al., PRA 51, 1863 (1995); G. Brassard et al., PRL 85, 1330 (2000).

MOTIVATION

Example: Exploiting double-clicks (if Bob discards them).

MOTIVATION

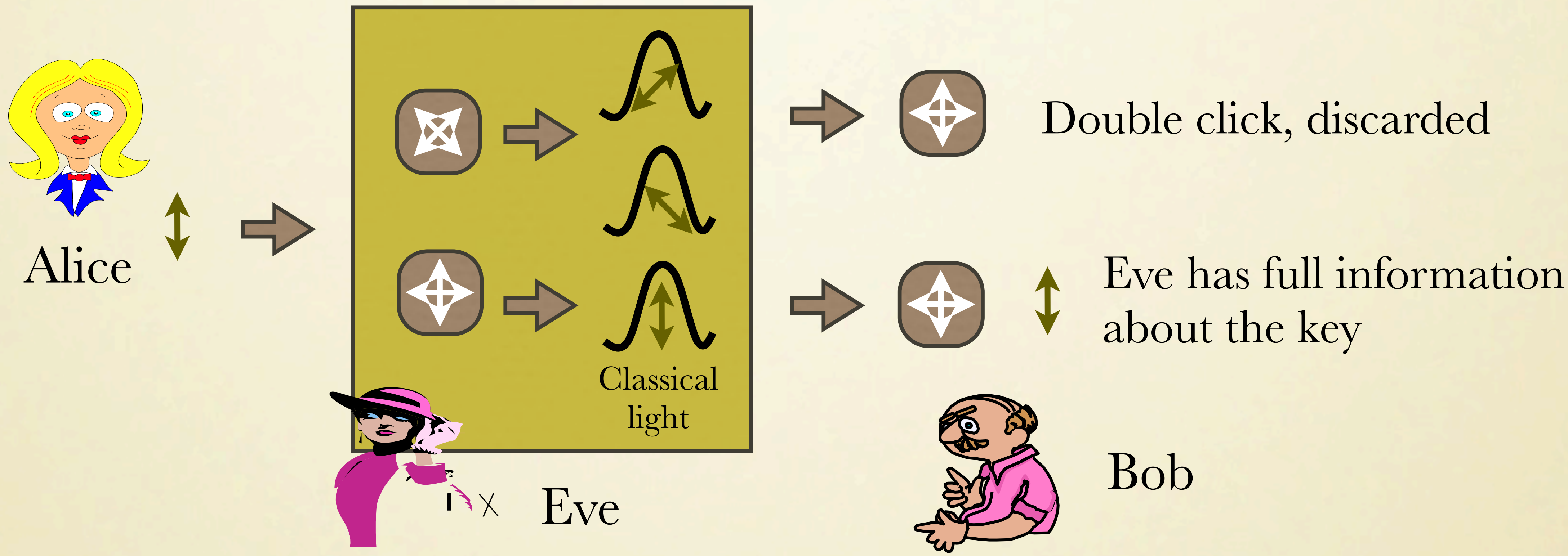
Example: Exploiting double-clicks (if Bob discards them).



As a result, Bob's detection efficiency is basis dependent.

MOTIVATION

Example: Exploiting double-clicks (if Bob discards them).



As a result, Bob's detection efficiency is basis dependent.

There is a gap between theory and practice. Theorists have to develop security proofs that can be applied to the experimental realisations.

Characterisation of experimental components

Characterisation of practical devices

Phase-randomised weak coherent pulses:

Characterisation of practical devices

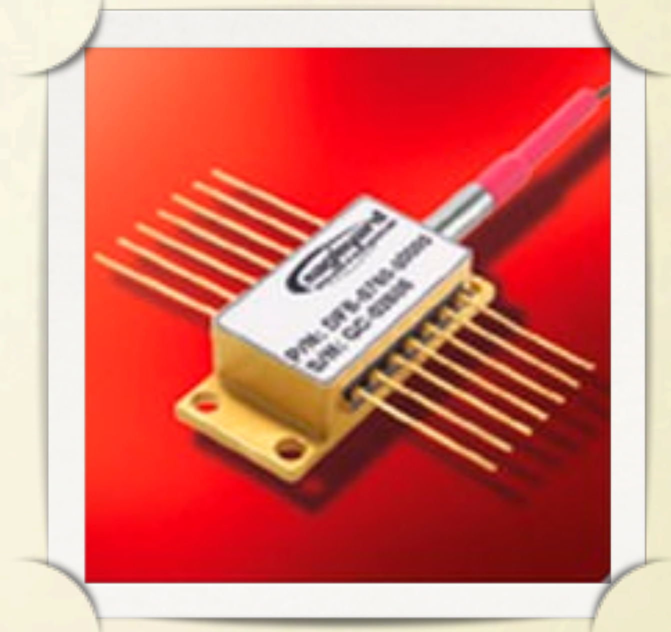
<u>Phase-randomised weak coherent pulses:</u>

Coherent states: $$|\alpha e^{i\phi}\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{(\alpha e^{i\phi})^n}{\sqrt{n!}}|n\rangle$$

$$|n\rangle = \frac{1}{\sqrt{n!}}(a^\dagger)^n|0\rangle$$

Characterisation of practical devices

<u>Phase-randomised weak coherent pulses:</u>



Coherent states: $|\alpha e^{i\phi}\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{(\alpha e^{i\phi})^n}{\sqrt{n!}} |n\rangle$

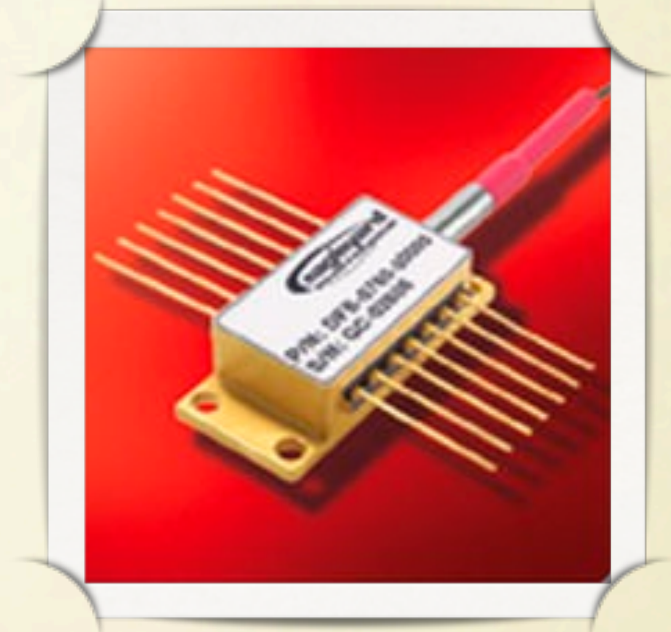
$$|n\rangle = \frac{1}{\sqrt{n!}} (a^\dagger)^n |0\rangle$$

If the phase is randomised, we have:

$$\mu = |\alpha|^2$$

$$\rho = \frac{1}{2\pi} \int_\phi |\alpha e^{i\phi}\rangle\langle \alpha e^{i\phi}| \mathrm{d}\phi = e^{-|\alpha|^2} \sum_{n=0}^{\infty} \frac{|\alpha|^{2n}}{n!} |n\rangle\langle n| = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle\langle n|$$

Characterisation of practical devices



Phase-randomised weak coherent pulses:

Coherent states: $|\alpha e^{i\phi}\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{(\alpha e^{i\phi})^n}{\sqrt{n!}} |n\rangle$

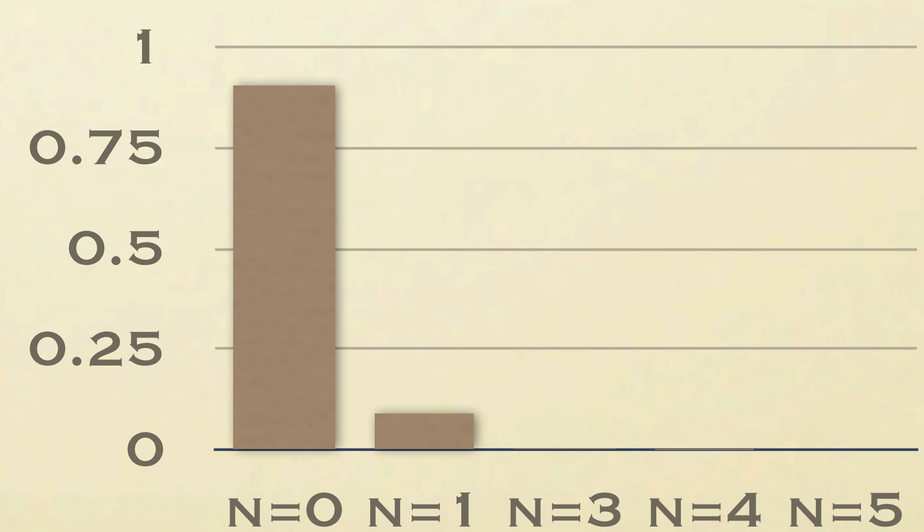
$$|n\rangle = \frac{1}{\sqrt{n!}} (a^\dagger)^n |0\rangle$$

If the phase is randomised, we have:

$$\mu = |\alpha|^2$$

$$\rho = \frac{1}{2\pi} \int_\phi |\alpha e^{i\phi}\rangle\langle \alpha e^{i\phi}| \mathrm{d}\phi = e^{-|\alpha|^2} \sum_{n=0}^{\infty} \frac{|\alpha|^{2n}}{n!} |n\rangle\langle n| = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle\langle n|$$

Photon number statistics when the intensity $\mu = 0.1$



Characterisation of practical devices

The BB84 signals can then be described as:

$$\rho_i = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n_i\rangle\langle n_i| \quad \text{with} \quad |n_i\rangle = \frac{1}{\sqrt{n!}} (a_i^\dagger)^n |0\rangle$$

with $i \in \{\mathrm{H}, \mathrm{V}, +45^\circ, -45^\circ\}$

Characterisation of practical devices

The BB84 signals can then be described as:

$$\rho_i = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n_i\rangle\langle n_i| \quad \text{with} \quad |n_i\rangle = \frac{1}{\sqrt{n!}} (a_i^\dagger)^n |0\rangle$$

with $i \in \{\mathrm{H}, \mathrm{V}, +45°, -45°\}$

The creation operators a_i can be expressed as a function of two creation operators b_1, b_2 associated to orthogonal polarisations:

creation operators

$$a_{\mathrm{H}}^\dagger = \frac{1}{\sqrt{2}}\left(b_1^\dagger + b_2^\dagger\right)$$

$$a_{\mathrm{V}}^\dagger = \frac{1}{\sqrt{2}}\left(b_1^\dagger - b_2^\dagger\right)$$

$$a_{+45^\circ}^\dagger = \frac{1}{\sqrt{2}}\left(b_1^\dagger + i b_2^\dagger\right)$$

$$a_{-45^\circ}^\dagger = \frac{1}{\sqrt{2}}\left(b_1^\dagger - i b_2^\dagger\right)$$

Characterisation of practical devices

The BB84 signals can then be described as:

$$\rho_i = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n_i\rangle\langle n_i| \quad \text{with} \quad |n_i\rangle = \frac{1}{\sqrt{n!}} (a_i^\dagger)^n |0\rangle$$

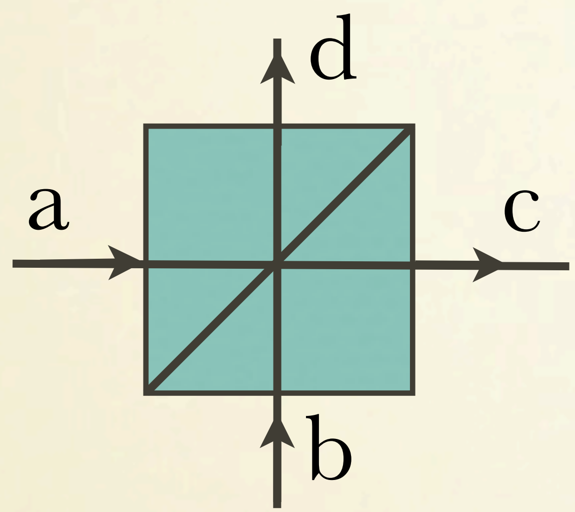
with $i \in \{\mathrm{H}, \mathrm{V}, +45^\circ, -45^\circ\}$

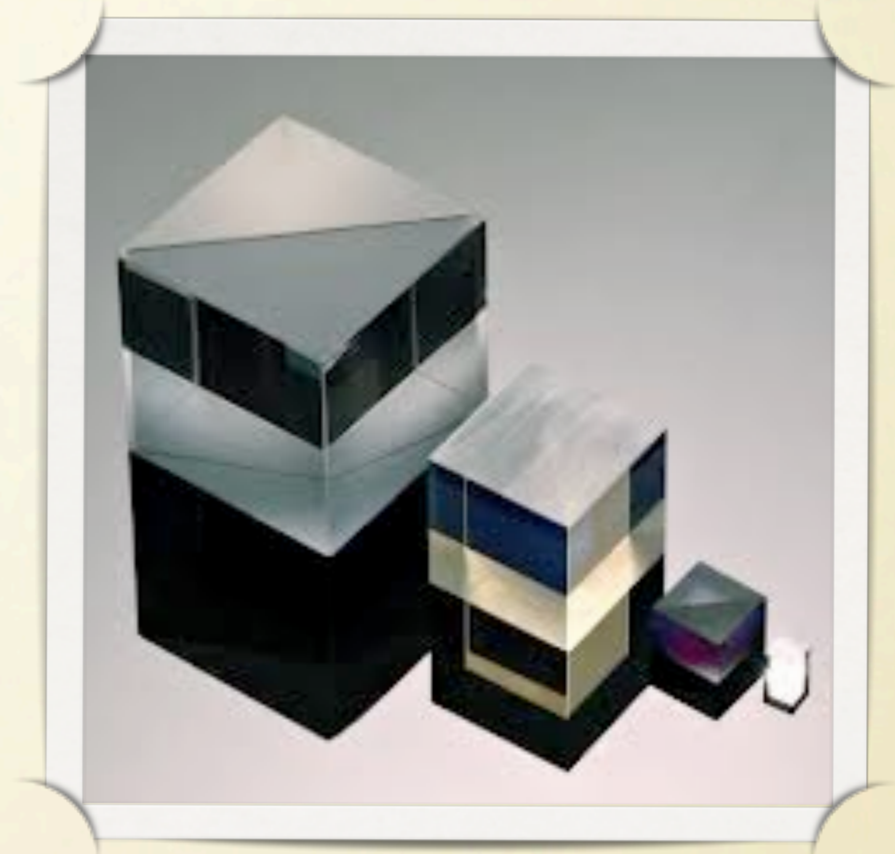
The creation operators a_i can be expressed as a function of two creation operators b_1, b_2 associated to orthogonal polarisations:

creation operators	*single photon components*
$a_{\mathrm{H}}^\dagger = \frac{1}{\sqrt{2}}\left(b_1^\dagger + b_2^\dagger\right)$	$\lvert 1_{\mathrm{H}}\rangle = a_{\mathrm{H}}^\dagger \lvert 0\rangle = \frac{1}{\sqrt{2}}\left(\lvert 1,0\rangle + \lvert 0,1\rangle\right)$
$a_{\mathrm{V}}^\dagger = \frac{1}{\sqrt{2}}\left(b_1^\dagger - b_2^\dagger\right)$	$\lvert 1_{\mathrm{V}}\rangle = a_{\mathrm{V}}^\dagger \lvert 0\rangle = \frac{1}{\sqrt{2}}\left(\lvert 1,0\rangle - \lvert 0,1\rangle\right)$
$a_{+45^\circ}^\dagger = \frac{1}{\sqrt{2}}\left(b_1^\dagger + i b_2^\dagger\right)$	$\lvert 1_{+45^\circ}\rangle = a_{+45^\circ}^\dagger \lvert 0\rangle = \frac{1}{\sqrt{2}}\left(\lvert 1,0\rangle + i\lvert 0,1\rangle\right)$
$a_{-45^\circ}^\dagger = \frac{1}{\sqrt{2}}\left(b_1^\dagger - i b_2^\dagger\right)$	$\lvert 1_{-45^\circ}\rangle = a_{-45^\circ}^\dagger \lvert 0\rangle = \frac{1}{\sqrt{2}}\left(\lvert 1,0\rangle - i\lvert 0,1\rangle\right)$

Characterisation of practical devices

Beam-splitters (BS):





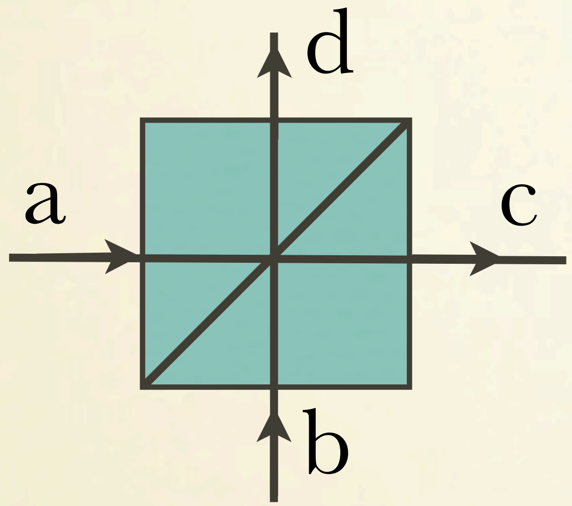
There are two input modes and two output modes

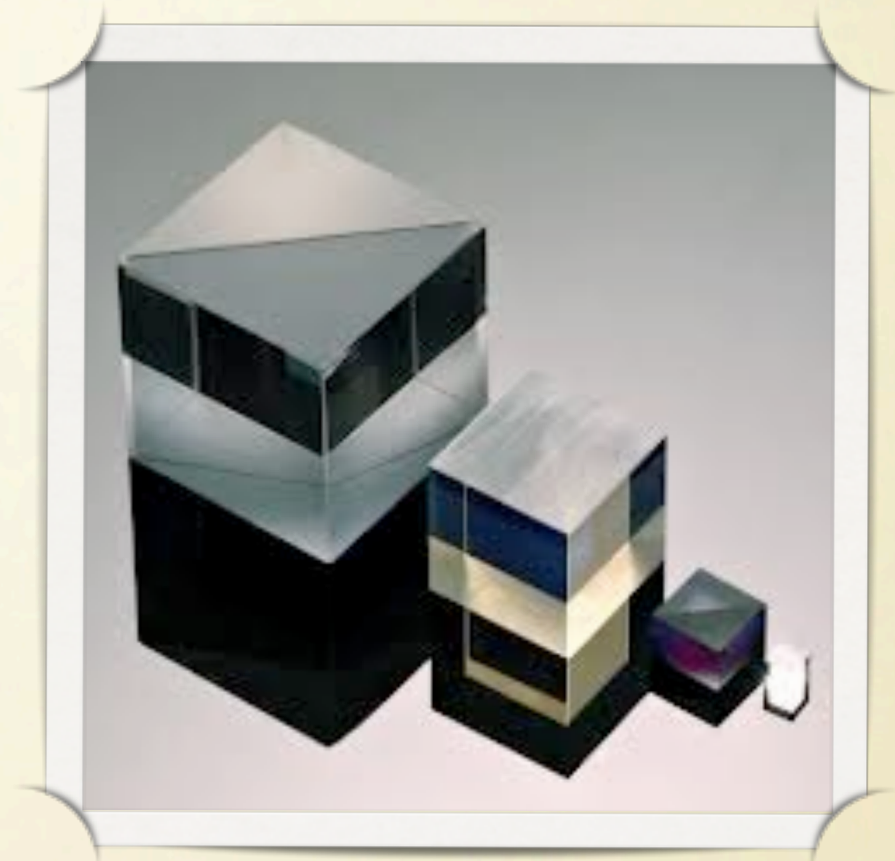
If we neglect for the moment absorption and other imperfections:

$$\begin{pmatrix} a^\dagger \\ b^\dagger \end{pmatrix} = e^{i\phi} \begin{pmatrix} te^{i\phi_t} & re^{i\phi_r} \\ -re^{-i\phi_r} & te^{-i\phi_t} \end{pmatrix} \begin{pmatrix} c^\dagger \\ d^\dagger \end{pmatrix}$$

Characterisation of practical devices

Beam-splitters (BS):





There are two input modes and two output modes

If we neglect for the moment absorption and other imperfections:

$$\begin{pmatrix} a^\dagger \\ b^\dagger \end{pmatrix} = e^{i\phi} \begin{pmatrix} te^{i\phi_t} & re^{i\phi_r} \\ -re^{-i\phi_r} & te^{-i\phi_t} \end{pmatrix} \begin{pmatrix} c^\dagger \\ d^\dagger \end{pmatrix}$$

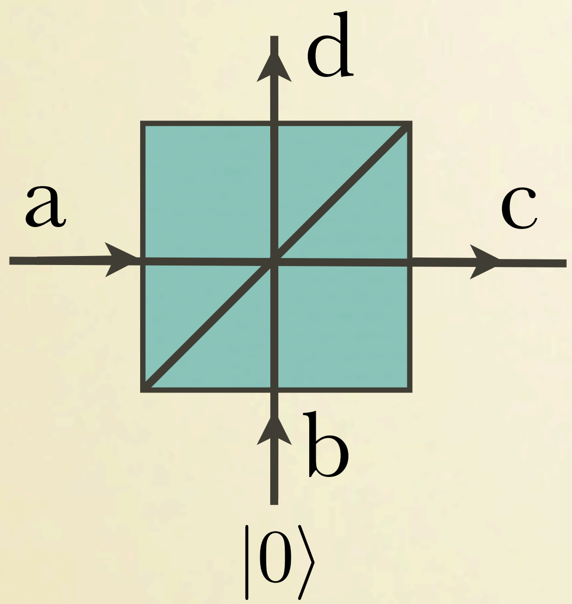
50:50 BS $\Rightarrow$ $$\begin{pmatrix} a^\dagger \\ b^\dagger \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} c^\dagger \\ d^\dagger \end{pmatrix}$$

Characterisation of practical devices

Modelling the losses in the quantum channel (beam-splitter):

Characterisation of practical devices

Modelling the losses in the quantum channel (beam-splitter):



$$\begin{pmatrix} a^\dagger \\ b^\dagger \end{pmatrix} = \begin{pmatrix} \sqrt{\eta_{\text{channel}}} & \sqrt{1-\eta_{\text{channel}}} \\ -\sqrt{1-\eta_{\text{channel}}} & \sqrt{\eta_{\text{channel}}} \end{pmatrix} \begin{pmatrix} c^\dagger \\ d^\dagger \end{pmatrix}$$

$$\begin{cases} a^\dagger = \sqrt{\eta_{\text{channel}}}c^\dagger + \sqrt{1-\eta_{\text{channel}}}d^\dagger \\ b^\dagger = -\sqrt{1-\eta_{\text{channel}}}c^\dagger + \sqrt{\eta_{\text{channel}}}d^\dagger \end{cases}$$

where $\eta_{\text{channel}} = 10^{-\frac{\alpha d}{10}}$, with:

α represents the loss coefficient of the channel measured in dB/km (e.g. in an optical fibre $\alpha = 0.2$ dB/km)

d is the transmission distance measured in km.

Tuesday, August 6, 13

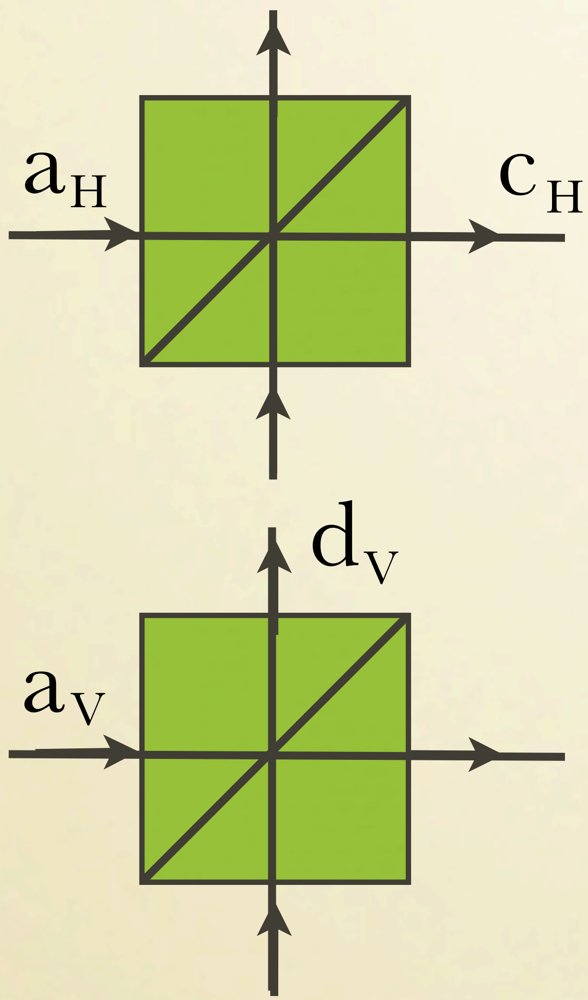
Characterisation of practical devices

Polarised beam-splitters (PBS):

Characterisation of practical devices

Polarised beam-splitters (PBS):

Separate polarisation into spatial modes

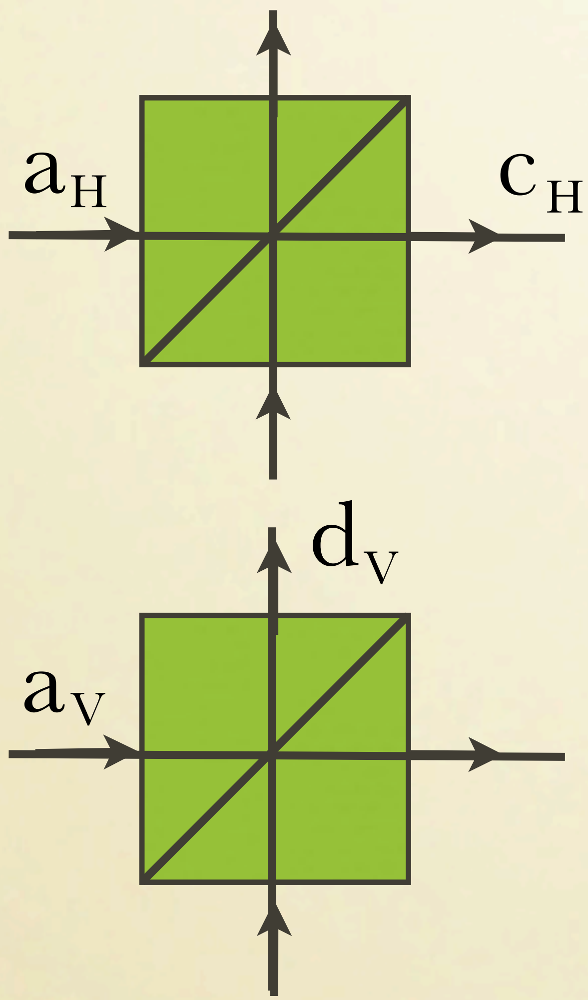


$$a_{\mathrm{H}}^{\dagger} = c_{\mathrm{H}}^{\dagger}$$
$$a_{\mathrm{V}}^{\dagger} = d_{\mathrm{V}}^{\dagger}$$

Characterisation of practical devices

Polarised beam-splitters (PBS):

Separate polarisation into spatial modes

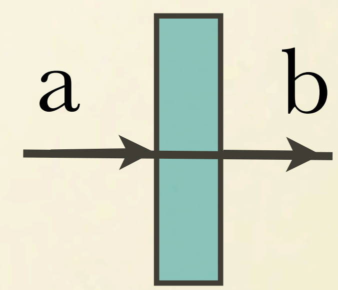


$$a_{\rm H}^\dagger = c_{\rm H}^\dagger$$

$$a_{\rm V}^\dagger = d_{\rm V}^\dagger$$

Half wave plate (HWP):

Performs a polarisation transformation



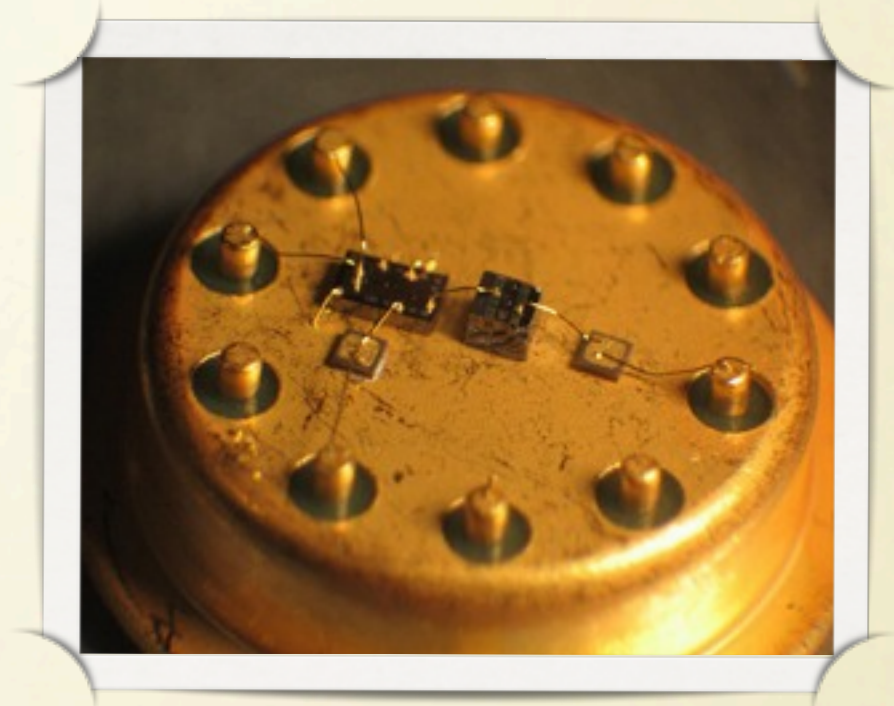
$$\begin{pmatrix} a_{+45^\circ}^\dagger \\ a_{-45^\circ}^\dagger \end{pmatrix} = \frac{e^{-i\pi/4}}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \begin{pmatrix} b_{+45^\circ}^\dagger \\ b_{-45^\circ}^\dagger \end{pmatrix}$$

$$a_{+45^\circ}^\dagger = b_{\rm V}^\dagger$$

$$a_{-45^\circ}^\dagger = -ib_{\rm H}^\dagger$$

Characterisation of practical devices

Threshold detectors:



They provide only two possible outcomes:

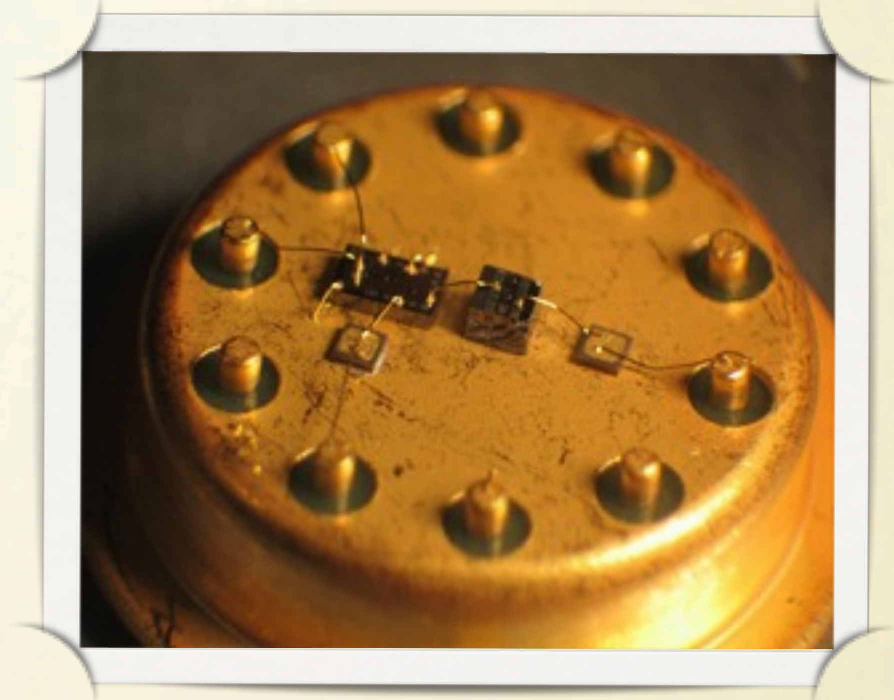
- "**Click**": At least one photon is detected

- "**No click**": No photon is detected

They are characterised by their detection efficiency $\eta_{\rm det}$, their dark count rate $p_{\rm dark}$ (which is, to good approximation, independent of the incoming signals), their dead-time, afterpulses, ...

Characterisation of practical devices

Threshold detectors:



They provide only two possible outcomes:

- "**Click**": At least one photon is detected
- "**No click**": No photon is detected

They are characterised by their detection efficiency η_{det} , their dark count rate p_{dark} (which is, to good approximation, independent of the incoming signals), their dead-time, afterpulses, ...

For simplicity, if we only consider their detection efficiency and dark count rate

$$D_{\mathrm{noclick}} = (1 - p_{\mathrm{dark}}) \sum_{n=0}^{\infty} (1 - \eta_{\mathrm{det}})^n |n\rangle\langle n|$$

$$D_{\mathrm{click}} = 1 - D_{\mathrm{noclick}}$$

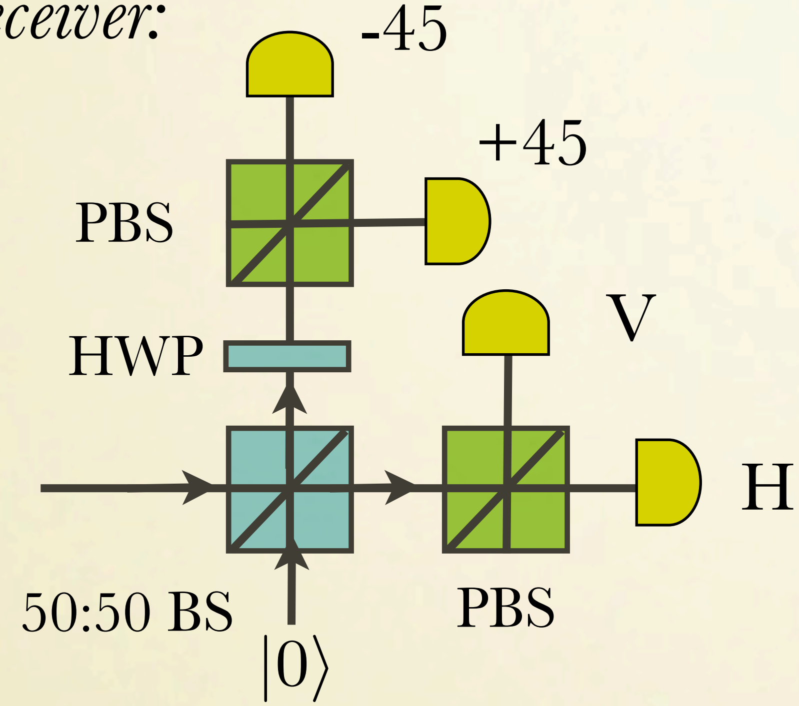
Characterisation of practical devices

Example: BB84 receiver.

Characterisation of practical devices

Example: BB84 receiver.

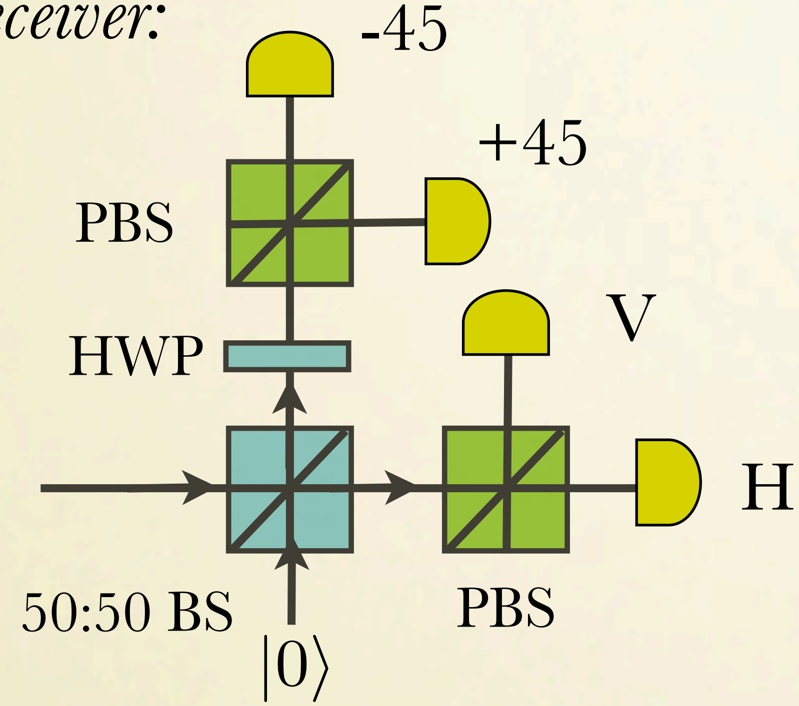
Passive receiver:



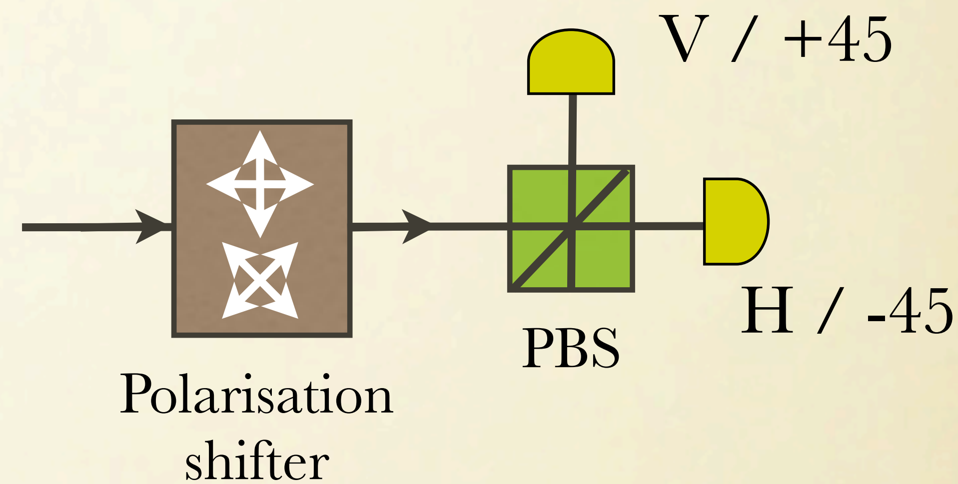
Characterisation of practical devices

Example: BB84 receiver.

Passive receiver:



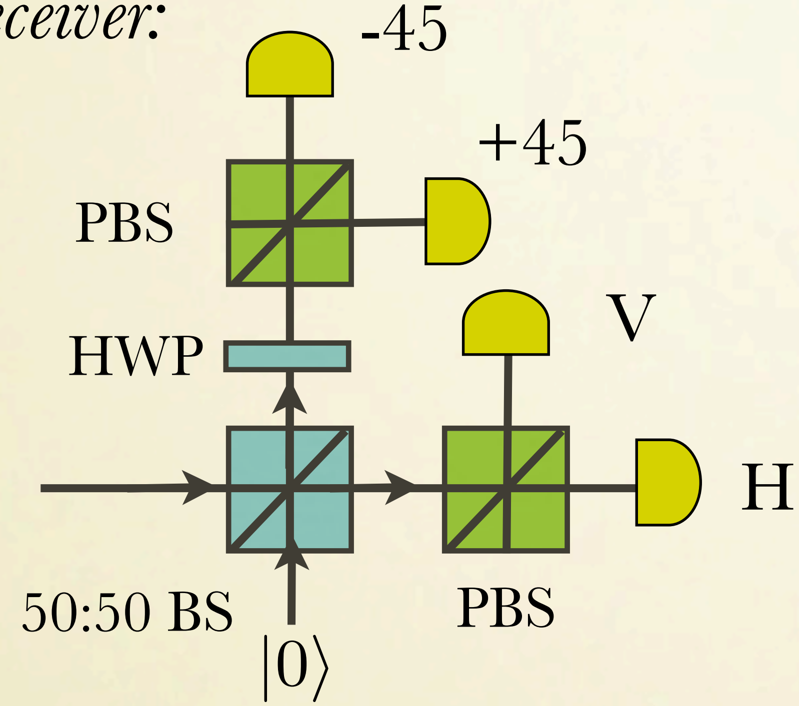
Active receiver:



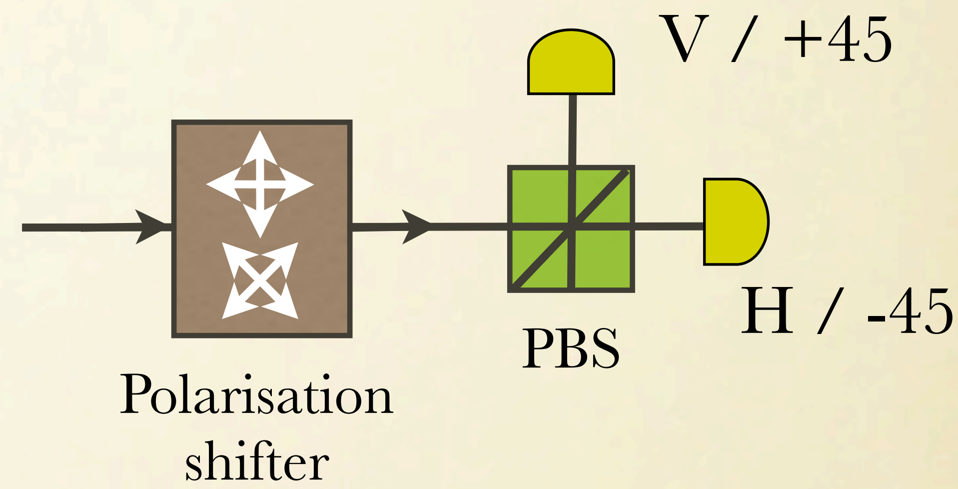
Characterisation of practical devices

Example: BB84 receiver.

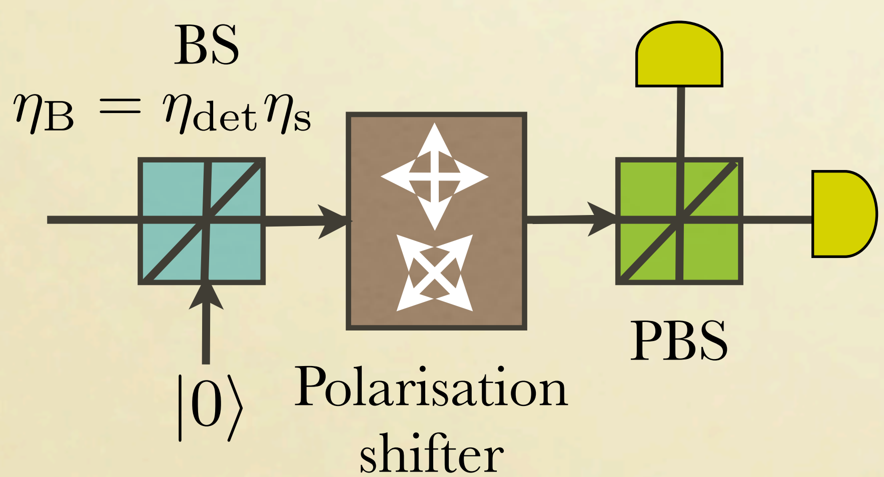
Passive receiver:



Active receiver:



If we consider, for the moment, that all detectors have the same efficiency:



$$D_{\mathrm{noclick}} = (1 - p_{\mathrm{dark}})|0\rangle\langle 0|$$

$$D_{\mathrm{click}} = 1 - D_{\mathrm{noclick}}$$

η_{B} : Transmittance of the optical components within Bob's measurement device and the detector efficiency

Characterisation of practical devices

Example: Gain of a signal state

Characterisation of practical devices

Example: Gain of a signal state

The gain Q is defined as the probability that a signal state sent by Alice produces at least one "click" in Bob's detection apparatus

$$\rho = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle\langle n| \quad \Rightarrow \quad Q = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} Y_n$$

The **yield** Y_n of an n-photon state is the conditional probability of a detection event on Bob's side given that Alice sent an n-photon state

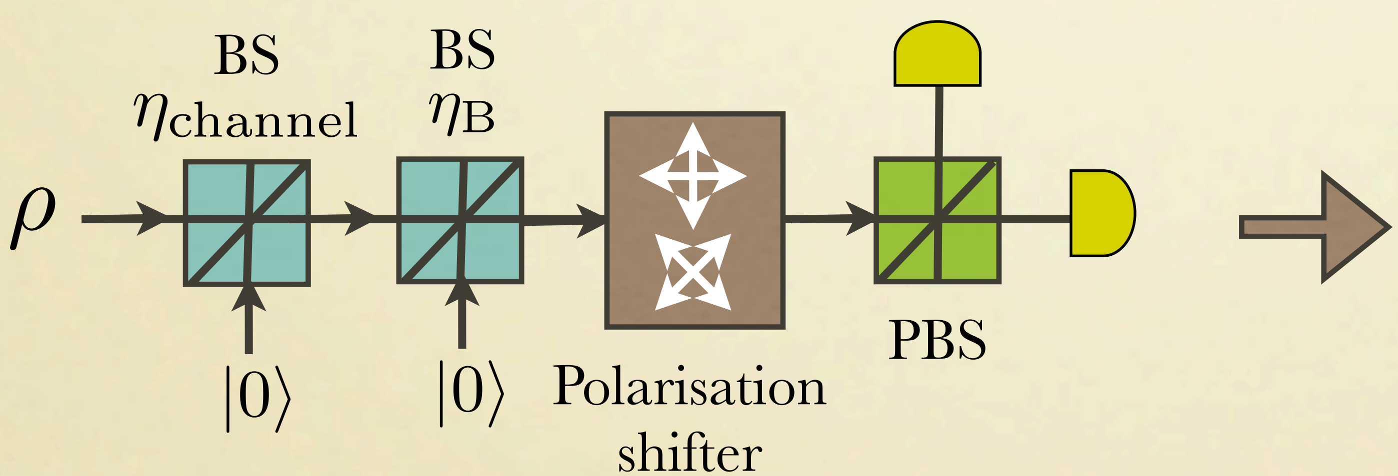
Characterisation of practical devices

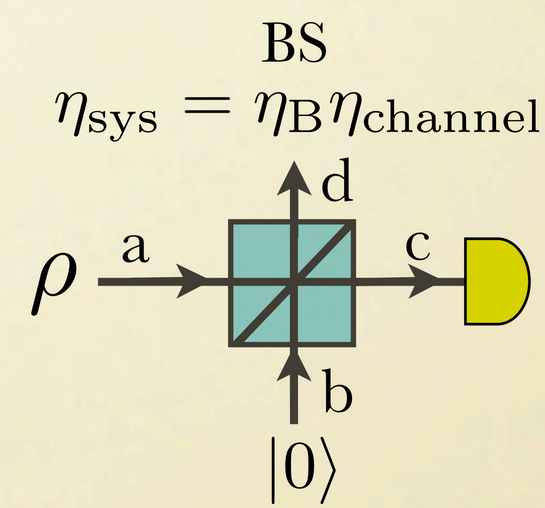
Example: Gain of a signal state

The gain Q is defined as the probability that a signal state sent by Alice produces at least one "click" in Bob's detection apparatus

$$\rho = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle\langle n| \quad \Rightarrow \quad Q = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} Y_n$$

The **yield** Y_n of an n-photon state is the conditional probability of a detection event on Bob's side given that Alice sent an n-photon state

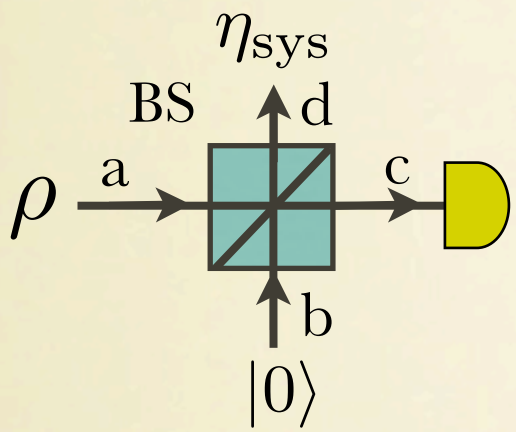




$$D_{\mathrm{noclick}} = (1 - p_{\mathrm{dark}})^2 |0\rangle\langle 0|$$

$$D_{\mathrm{click}} = 1 - D_{\mathrm{noclick}}$$

Characterisation of practical devices



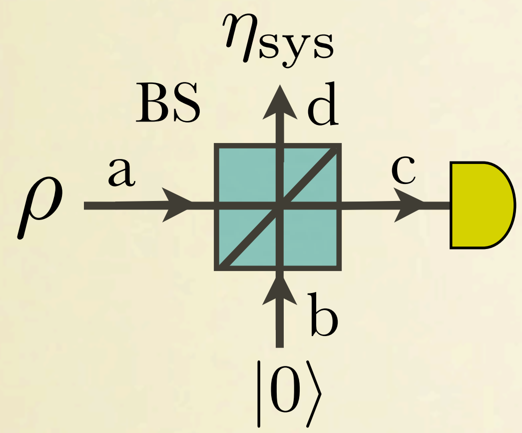
$$|n\rangle_a = \frac{1}{\sqrt{n!}}(a^\dagger)^n|0\rangle \xrightarrow[\text{BS}]{} |n\rangle_{cd} = \frac{1}{\sqrt{n!}}(\sqrt{\eta_{\rm sys}}c^\dagger + \sqrt{1-\eta_{\rm sys}}d^\dagger)^n|0\rangle$$

$$|n\rangle_{cd} = \sum_{k=0}^{n}\sqrt{\binom{n}{k}}\sqrt{\eta_{\rm sys}}^{\,n-k}\sqrt{1-\eta_{\rm sys}}^{\,k}|n-k,k\rangle_{cd}$$

Here we have used the fact that

$$|n-k\rangle_c = \frac{1}{\sqrt{(n-k)!}}(c^\dagger)^{n-k}|0\rangle \quad \text{and} \quad |k\rangle_d = \frac{1}{\sqrt{k!}}(d^\dagger)^k|0\rangle$$

Characterisation of practical devices



$$|n\rangle_a = \frac{1}{\sqrt{n!}}(a^\dagger)^n|0\rangle \quad \underset{\text{BS}}{\Longrightarrow} \quad |n\rangle_{cd} = \frac{1}{\sqrt{n!}}(\sqrt{\eta_{\text{sys}}}c^\dagger + \sqrt{1-\eta_{\text{sys}}}d^\dagger)^n|0\rangle$$

$$|n\rangle_{cd} = \sum_{k=0}^{n}\sqrt{\binom{n}{k}}\sqrt{\eta_{\text{sys}}}^{\,n-k}\sqrt{1-\eta_{\text{sys}}}^{\,k}|n-k,k\rangle_{cd}$$

Here we have used the fact that

$$|n-k\rangle_c = \frac{1}{\sqrt{(n-k)!}}(c^\dagger)^{n-k}|0\rangle \quad \text{and} \quad |k\rangle_d = \frac{1}{\sqrt{k!}}(d^\dagger)^k|0\rangle$$

$$\begin{aligned}
Y_n &= \mathrm{Tr}[|n\rangle_{cd}\langle n|(D_{\text{click}}\otimes 1_d)] \\
&= 1 - \mathrm{Tr}[|n\rangle_{cd}\langle n|(D_{\text{noclick}}\otimes 1_d)] \\
&= 1-(1-p_{\text{dark}})^2\mathrm{Tr}[|n\rangle_{cd}\langle n|(|0\rangle_c\langle 0|\otimes 1_d)] \\
&= 1-(1-p_{\text{dark}})^2(1-\eta_{\text{sys}})^n
\end{aligned}$$

$\langle n|m\rangle = \delta_{nm}$

Characterisation of practical devices

Given that: $Y_n = 1 - (1 - p_{\mathrm{dark}})^2 (1 - \eta_{\mathrm{sys}})^n$

$$Q = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} Y_n \Rightarrow Q = 1 - (1 - p_{\mathrm{dark}})^2 e^{-\mu \eta_{\mathrm{sys}}}$$

The gain is directly observed in the experiment.

Characterisation of practical devices

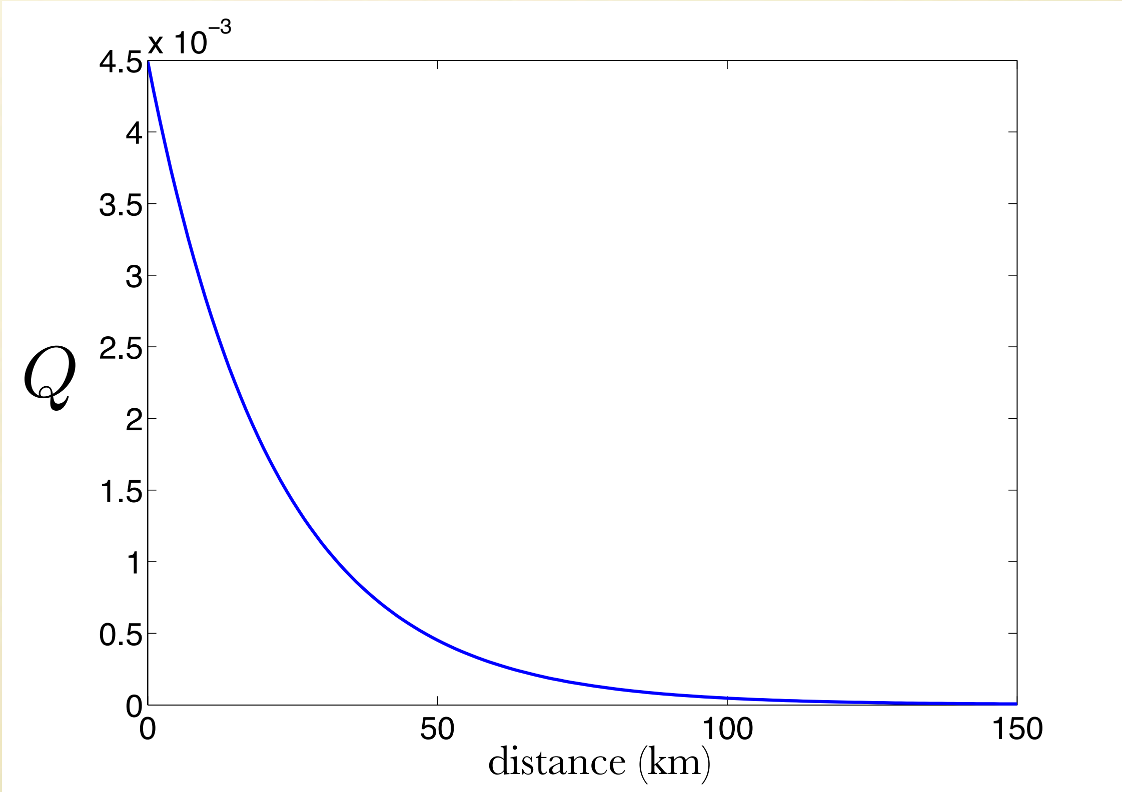
Given that: $Y_n = 1 - (1 - p_{\mathrm{dark}})^2 (1 - \eta_{\mathrm{sys}})^n$

$$Q = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} Y_n \Rightarrow Q = 1 - (1 - p_{\mathrm{dark}})^2 e^{-\mu \eta_{\mathrm{sys}}}$$

The gain is directly observed in the experiment.

<u>Example:</u>

$$p_{\mathrm{dark}} = 10^{-6}$$
$$\mu = 0.1$$
$$\eta_{\mathrm{B}} = 0.045$$
$$\alpha = 0.2 \text{ dB/km}$$

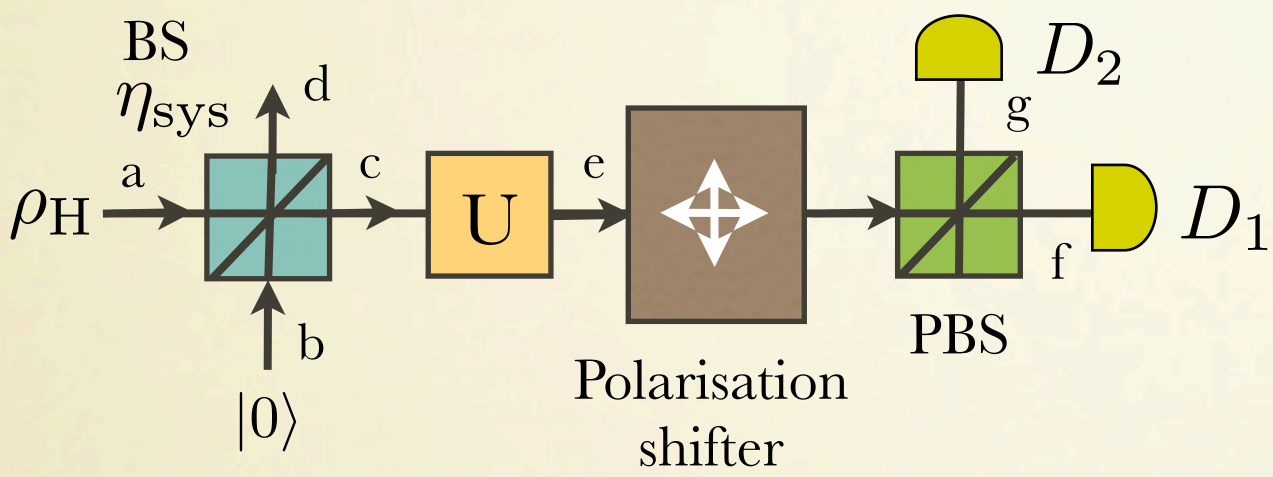


Characterisation of practical devices

Example: Error rate

Characterisation of practical devices

Example: Error rate

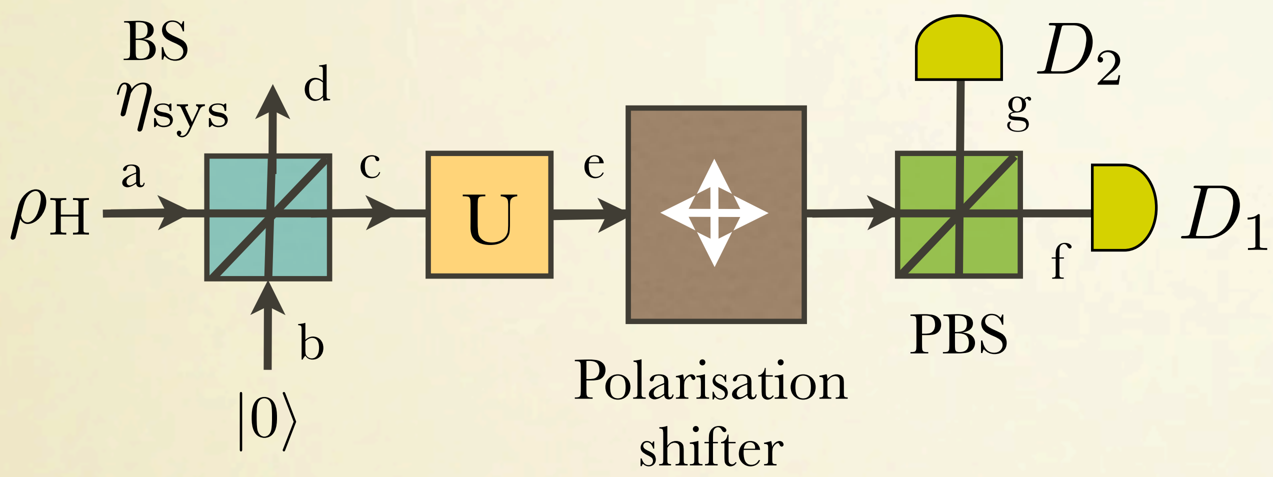


Misalignment in the channel:

$$\begin{pmatrix} c_{\rm H}^\dagger \\ c_{\rm V}^\dagger \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} e_{\rm H}^\dagger \\ e_{\rm V}^\dagger \end{pmatrix}$$

Characterisation of practical devices

Example: Error rate



Misalignment in the channel:

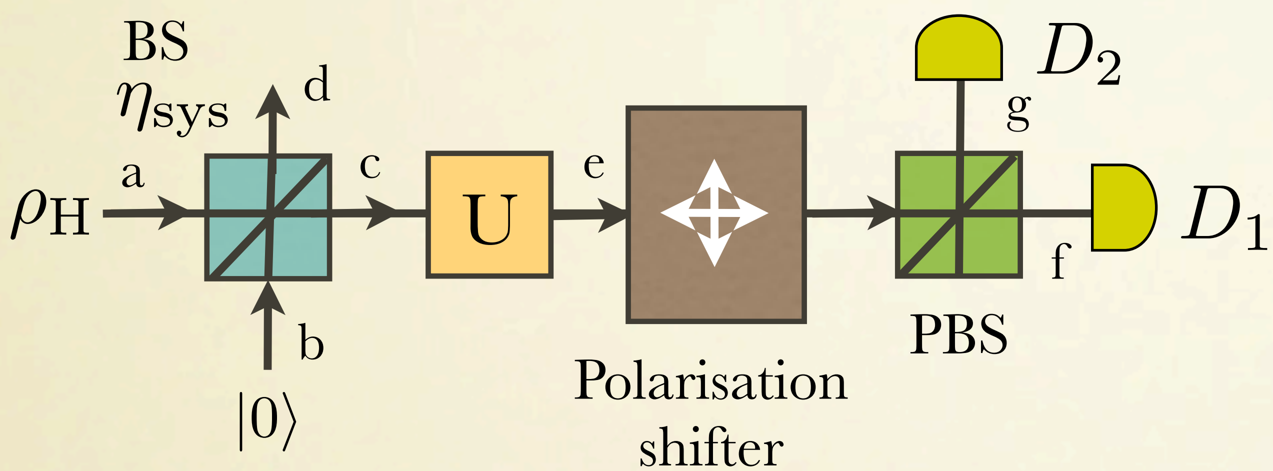
$$\begin{pmatrix} c_{\rm H}^\dagger \\ c_{\rm V}^\dagger \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} e_{\rm H}^\dagger \\ e_{\rm V}^\dagger \end{pmatrix}$$

The error rate can be written as: $E = \dfrac{1}{Q} e^{-\mu} \displaystyle\sum_{n=0}^{\infty} \frac{\mu^n}{n!} Y_n e_n$

$Y_n e_n$: Probability that a n-photon signal produces a detected event associated with an error

Characterisation of practical devices

Example: Error rate



Misalignment in the channel:

$$\begin{pmatrix} c_{\text{H}}^\dagger \\ c_{\text{V}}^\dagger \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} e_{\text{H}}^\dagger \\ e_{\text{V}}^\dagger \end{pmatrix}$$

The error rate can be written as: $E = \frac{1}{Q} e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} Y_n e_n$

$Y_n e_n$: Probability that a n-photon signal produces a detected event associated with an error

$$Y_n e_n = \mathrm{Tr}\left[\left(D_{1,\text{noclick}} \otimes D_{2,\text{click}} \otimes 1_d + \frac{1}{2} D_{1,\text{click}} \otimes D_{2,\text{click}} \otimes 1_d \right) |n\rangle_{dfg}\langle n| \right]$$

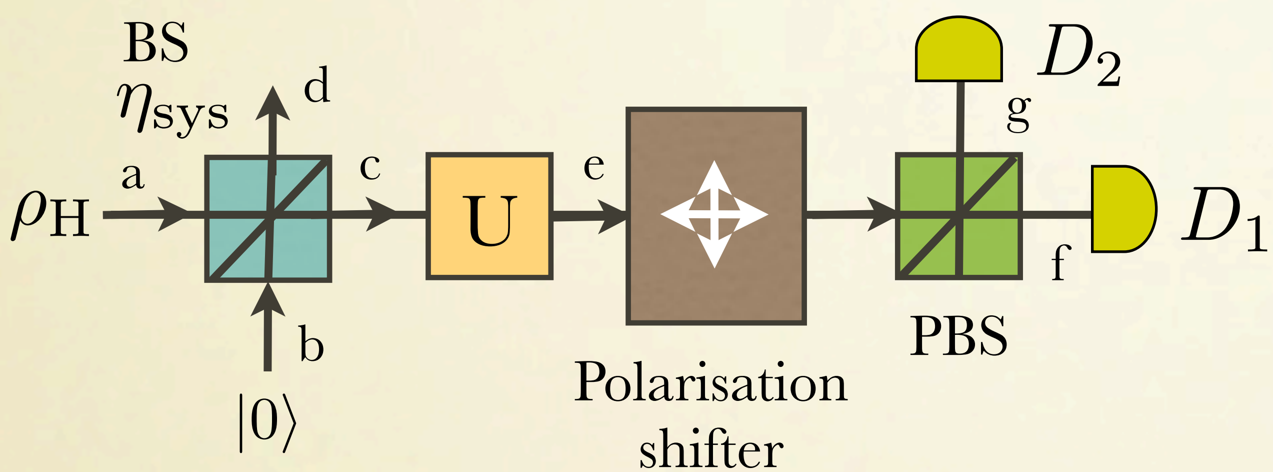
Double clicks are associated to random single clicks

Characterisation of practical devices

Now we calculate: $|n\rangle_{dfg}$

Characterisation of practical devices

Now we calculate: $|n\rangle_{dfg}$



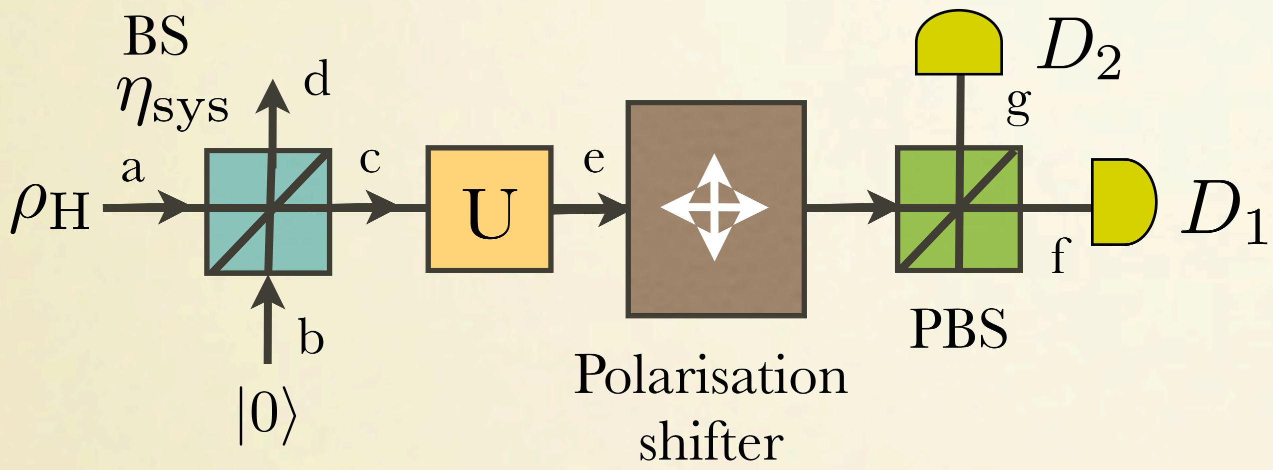
Input state: $\rho_{\text{H}} = |n\rangle\langle n|_{\text{H}}$

with

$$|n\rangle_{\text{H}} = \frac{1}{\sqrt{n!}}(a_{\text{H}}^{\dagger})^n|0\rangle$$

Characterisation of practical devices

Now we calculate: $|n\rangle_{dfg}$



Input state: $\rho_{\text{H}} = |n\rangle\langle n|_{\text{H}}$
with

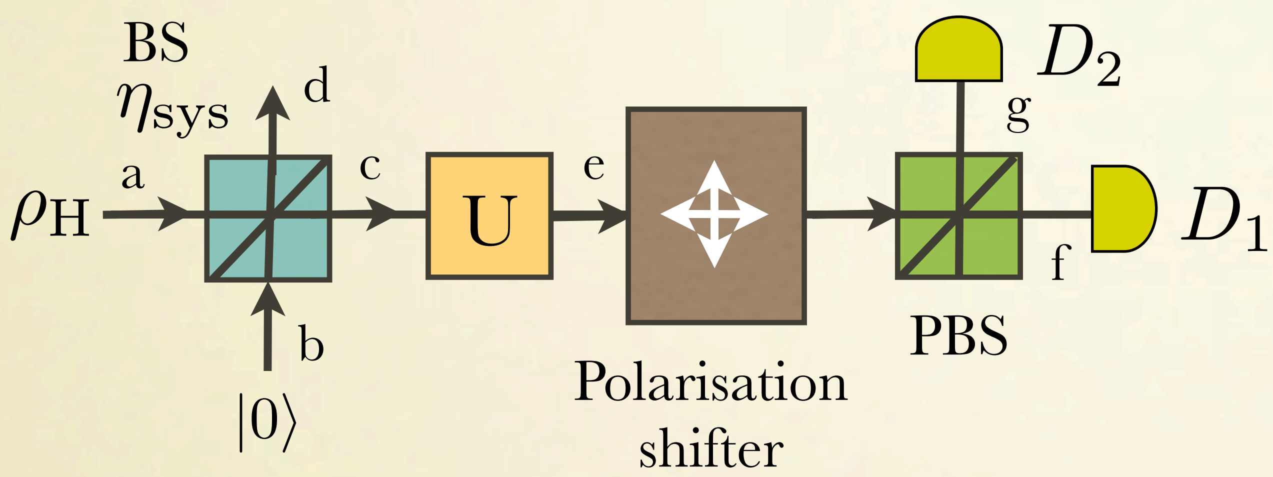
$$|n\rangle_{\text{H}} = \frac{1}{\sqrt{n!}}(a_{\text{H}}^\dagger)^n|0\rangle$$

$$a_{\text{H}}^\dagger \xrightarrow{\text{BS}} \sqrt{\eta_{\text{sys}}}c_{\text{H}}^\dagger + \sqrt{1-\eta_{\text{sys}}}d_{\text{H}}^\dagger \xrightarrow{\text{U}} \sqrt{\eta_{\text{sys}}}\left(\cos\theta e_{\text{H}}^\dagger - \sin\theta e_{\text{V}}^\dagger\right) + \sqrt{1-\eta_{\text{sys}}}d_{\text{H}}^\dagger$$

$$\xrightarrow{\text{PBS}} \sqrt{\eta_{\text{sys}}}\left(\cos\theta f_{\text{H}}^\dagger - \sin\theta g_{\text{V}}^\dagger\right) + \sqrt{1-\eta_{\text{sys}}}d_{\text{H}}^\dagger$$

Characterisation of practical devices

Now we calculate: $|n\rangle_{dfg}$



Input state: $\rho_{\text{H}} = |n\rangle\langle n|_{\text{H}}$

with

$$|n\rangle_{\text{H}} = \frac{1}{\sqrt{n!}}(a^\dagger_{\text{H}})^n|0\rangle$$

$$a^\dagger_{\text{H}} \xrightarrow{\text{BS}} \sqrt{\eta_{\text{sys}}}c^\dagger_{\text{H}} + \sqrt{1-\eta_{\text{sys}}}d^\dagger_{\text{H}} \xrightarrow{\text{U}} \sqrt{\eta_{\text{sys}}}\left(\cos\theta e^\dagger_{\text{H}} - \sin\theta e^\dagger_{\text{V}}\right) + \sqrt{1-\eta_{\text{sys}}}d^\dagger_{\text{H}}$$

$$\xrightarrow{\text{PBS}} \sqrt{\eta_{\text{sys}}}\left(\cos\theta f^\dagger_{\text{H}} - \sin\theta g^\dagger_{\text{V}}\right) + \sqrt{1-\eta_{\text{sys}}}d^\dagger_{\text{H}}$$

$$|n\rangle_{dfg} = \sum_{k=0}^{n}\sum_{l=0}^{n-k}\sqrt{\frac{n!}{k!l!(n-k-l)!}}\sqrt{\eta_{\text{sys}}}^{\,n-k}\sqrt{1-\eta_{\text{sys}}}^{\,k}(\cos\theta)^{n-k-l}(-\sin\theta)^l|k,n-k-l,l\rangle_{d_{\text{H}},f_{\text{H}},g_{\text{V}}}$$

Characterisation of practical devices

Characterisation of practical devices

$$Y_n e_n = \mathrm{Tr}\left[\left(\underbrace{D_{1,\mathrm{noclick}} \otimes D_{2,\mathrm{click}} \otimes 1_d + \frac{1}{2} D_{1,\mathrm{click}} \otimes D_{2,\mathrm{click}} \otimes 1_d}_{D} \right) |n\rangle_{dfg}\langle n| \right]$$

$$\Downarrow \quad \begin{aligned} D_{\mathrm{noclick}} &= (1 - d_{\mathrm{dark}})|0\rangle\langle 0| \\ D_{\mathrm{click}} &= 1 - D_{\mathrm{noclick}} \end{aligned}$$

Characterisation of practical devices

$$Y_n e_n = \mathrm{Tr}\left[\underbrace{\left(D_{1,\mathrm{noclick}} \otimes D_{2,\mathrm{click}} \otimes 1_d + \frac{1}{2} D_{1,\mathrm{click}} \otimes D_{2,\mathrm{click}} \otimes 1_d \right)}_{D} |n\rangle_{dfg}\langle n| \right]$$

$$D_{\mathrm{noclick}} = (1 - d_{\mathrm{dark}})|0\rangle\langle 0|$$

$$D_{\mathrm{click}} = 1 - D_{\mathrm{noclick}}$$

$$D = \frac{1}{2}\Big[1_{dfg} + (1 - p_{\mathrm{dark}})(1_d \otimes |0\rangle\langle 0|_f \otimes 1_g - 1_d \otimes 1_f \otimes |0\rangle\langle 0|_g)$$
$$-(1 - p_{\mathrm{dark}})^2 (1_d \otimes |0\rangle\langle 0|_f \otimes |0\rangle\langle 0|_g) \Big]$$

Characterisation of practical devices

$$Y_n e_n = \mathrm{Tr}\left[\left(\underbrace{D_{1,\text{noclick}} \otimes D_{2,\text{click}} \otimes 1_d + \frac{1}{2} D_{1,\text{click}} \otimes D_{2,\text{click}} \otimes 1_d}_{D}\right) |n\rangle_{dfg}\langle n|\right]$$

$$D_{\text{noclick}} = (1 - d_{\text{dark}})|0\rangle\langle 0|$$

$$D_{\text{click}} = 1 - D_{\text{noclick}}$$

$$D = \frac{1}{2}\Big[1_{dfg} + (1 - p_{\text{dark}})(1_d \otimes |0\rangle\langle 0|_f \otimes 1_g - 1_d \otimes 1_f \otimes |0\rangle\langle 0|_g)$$
$$-(1 - p_{\text{dark}})^2 (1_d \otimes |0\rangle\langle 0|_f \otimes |0\rangle\langle 0|_g)\Big]$$

We obtain:

$$Y_n e_n = \frac{1}{2}\Big\{1 + (1 - p_{\text{dark}})\frac{1}{2^n}[(2 - \eta_{\text{sys}} - \eta_{\text{sys}} \cos 2\theta)^n - (2 - \eta_{\text{sys}} + \eta_{\text{sys}} \cos 2\theta)^n]$$
$$-(1 - p_{\text{dark}})^2 (1 - \eta_{\text{sys}})^n\Big\}$$

Characterisation of practical devices

$$E = \frac{1}{Q} e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} Y_n e_n$$

$$= \frac{1}{2Q} \left[1 + (1 - p_{\text{dark}}) \left(e^{-\mu\eta_{\text{sys}} \cos^2\theta} - e^{-\mu\eta_{\text{sys}} \sin^2\theta} \right) - (1 - p_{\text{dark}})^2 e^{-\mu\eta_{\text{sys}}} \right]$$

The error rate is directly observed in the experiment.

Characterisation of practical devices

$$E = \frac{1}{Q} e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} Y_n e_n$$

$$= \frac{1}{2Q} \left[1 + (1 - p_{\text{dark}}) \left(e^{-\mu \eta_{\text{sys}} \cos^2 \theta} - e^{-\mu \eta_{\text{sys}} \sin^2 \theta} \right) - (1 - p_{\text{dark}})^2 e^{-\mu \eta_{\text{sys}}} \right]$$

The error rate is directly observed in the experiment.

<u>Example:</u> BB84 with phase-randomised WCPs

Characterisation of practical devices

$$E = \frac{1}{Q} e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} Y_n e_n$$

$$= \frac{1}{2Q}\left[1 + (1 - p_{\text{dark}})\left(e^{-\mu\eta_{\text{sys}}\cos^2\theta} - e^{-\mu\eta_{\text{sys}}\sin^2\theta}\right) - (1 - p_{\text{dark}})^2 e^{-\mu\eta_{\text{sys}}}\right]$$

The error rate is directly observed in the experiment.

Example: BB84 with phase-randomised WCPs

$$R \geq q\,\{p_1 Y_1 [1 - h(e_1)] - Qh(E)\}$$

q	is the basis-sift factor (***known***)
$p_1 = \mu e^{-\mu}$	is the probability that Alice emits a single-photon state (***known***)
Y_1	is the yield of the single-photon states (***unknown***)
e_1	is the phase error of the single photon states (***unknown***)
Q	is the overall gain of the signal states (***observed***)
E	is the overall error rate of the signal states (***observed***)

D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, Quantum Inf. Comput. 4, 325 (2004).

Characterisation of practical devices

We assume that $Q, E,$ is the same for both basis. Parameter estimation (due to the PNS attack we need to consider the wort-case scenario):

D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, Quantum Inf. Comput. 4, 325 (2004).

Characterisation of practical devices

We assume that $Q, E,$ is the same for both basis. Parameter estimation (due to the PNS attack we need to consider the wort-case scenario):

$$Y_1 = \frac{Q - p_{\text{multi}}}{p_1} \qquad e_1 = \frac{E}{1 - \frac{p_{\text{multi}}}{Q}}$$

where $p_{\text{multi}} = 1 - e^{-\mu} - \mu e^{-\mu}$

D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, *Quantum Inf. Comput.* 4, 325 (2004).

Characterisation of practical devices

We assume that Q, E, is the same for both basis. Parameter estimation (due to the PNS attack we need to consider the wort-case scenario):

$$Y_1 = \frac{Q - p_{\mathrm{multi}}}{p_1} \qquad e_1 = \frac{E}{1 - \frac{p_{\mathrm{multi}}}{Q}}$$

where $p_{\mathrm{multi}} = 1 - e^{-\mu} - \mu e^{-\mu}$

<u>Example:</u>

$p_{\mathrm{dark}} = 10^{-6}$

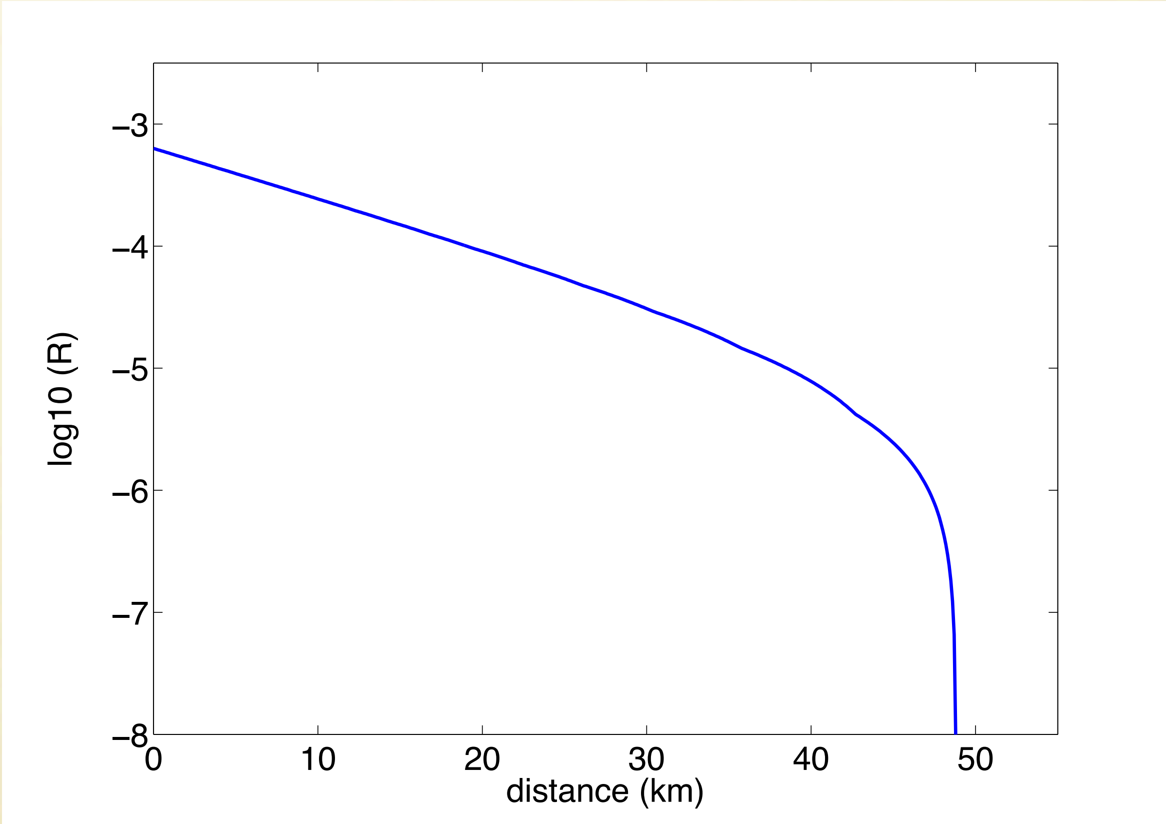
$e_d = \sin^2\theta = 0.015$

$\eta_{\mathrm{B}} = 0.045$

$\alpha = 0.2$ dB/km

$q \approx 1$

μ optimised



D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, Quantum Inf. Comput. 4, 325 (2004).

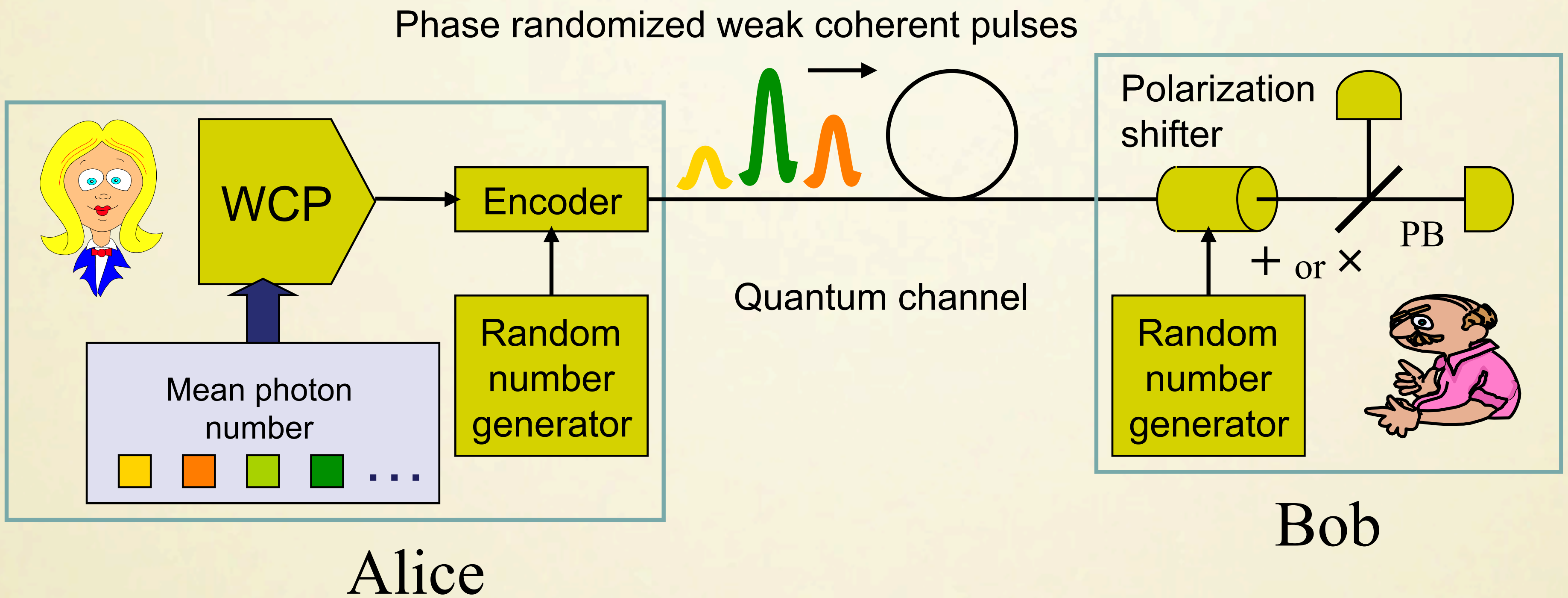
QKD with decoy states (asymptotic case)

QKD WITH DECOY STATES

Motivation: Better estimation of Y_1, e_1.

QKD WITH DECOY STATES

Motivation: Better estimation of Y_1, e_1.



Alice prepares phase-randomised weak coherent pulses whose mean photon number is chosen for each signal from a finite set of possible values.

$$\rho_l = e^{-\mu_l} \sum_{n=0}^{\infty} \frac{\mu_l^n}{n!} |n\rangle\langle n| \quad \text{with} \quad l \in \{\mathrm{s}, \mathrm{d}_1, \mathrm{d}_2, \ldots, \mathrm{d}_\mathrm{N}\}$$

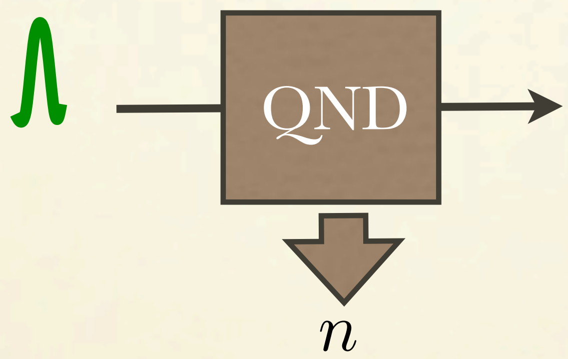
W.-Y. Hwang, PRL 91, 057901 (2003); H.-K. Lo, X. Ma and K. Chen, PRL 94, 230504 (2005); X.-B. Wang, PRL 94, 230503 (2005).

QKD WITH DECOY STATES

Intuition:

In principle Eve can guess the intensity setting l selected by Alice:

$$\rho_l = e^{-\mu_l} \sum_{n=0}^{\infty} \frac{\mu_l^n}{n!} |n\rangle\langle n|$$



$$p(l|n) = p(n|l)\frac{p(l)}{p(n)}$$
$$= e^{\mu_l} \frac{\mu_l^n}{n!} \frac{p(l)}{\sum_l p(l) e^{\mu_l} \mu_l^n / n!}$$

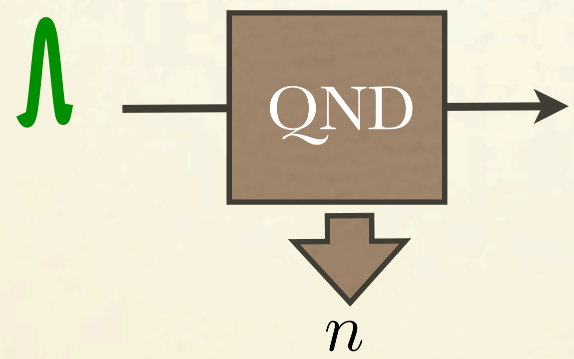
W.-Y. Hwang, PRL 91, 057901 (2003); H.-K. Lo, X. Ma and K. Chen, PRL 94, 230504 (2005); X.-B. Wang, PRL 94, 230503 (2005).

QKD WITH DECOY STATES

Intuition:

In principle Eve can guess the intensity setting *l* selected by Alice:

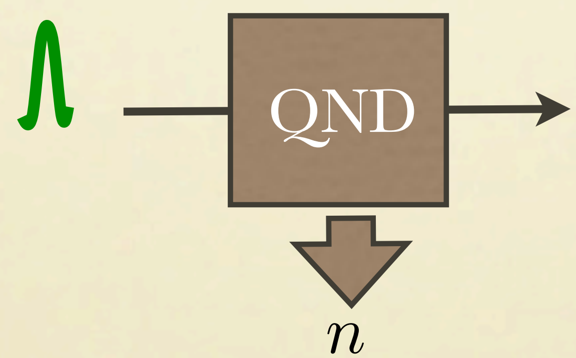
$$\rho_l = e^{-\mu_l} \sum_{n=0}^{\infty} \frac{\mu_l^n}{n!} |n\rangle\langle n|$$



$$p(l|n) = p(n|l)\frac{p(l)}{p(n)}$$

$$= e^{\mu_l}\frac{\mu_l^n}{n!}\frac{p(l)}{\sum_l p(l)e^{\mu_l}\mu_l^n/n!}$$

Key idea: The yields Y_n and the error rates e_n are equal for the different intensity settings



Eve has to decide Y_n and e_n

W.-Y. Hwang, PRL 91, 057901 (2003); H.-K. Lo, X. Ma and K. Chen, PRL 94, 230504 (2005); X.-B. Wang, PRL 94, 230503 (2005).

QKD with decoy states

How to estimate the parameters Y_1, e_1? We have a set of linear equations...

W.-Y. Hwang, PRL 91, 057901 (2003); H.-K. Lo, X. Ma and K. Chen, PRL 94, 230504 (2005); X.-B. Wang, PRL 94, 230503 (2005).

QKD WITH DECOY STATES

How to estimate the parameters Y_1, e_1? We have a set of linear equations...

$$Q_{\mathrm{s}} = e^{-\mu_{\mathrm{s}}} \sum_{n=0}^{\infty} \frac{\mu_{\mathrm{s}}^n}{n!} Y_n \qquad E_{\mathrm{s}} Q_{\mathrm{s}} = e^{-\mu_{\mathrm{s}}} \sum_{n=0}^{\infty} \frac{\mu_{\mathrm{s}}^n}{n!} Y_n e_n$$

$$Q_{\mathrm{d}_1} = e^{-\mu_{\mathrm{d}_1}} \sum_{n=0}^{\infty} \frac{\mu_{\mathrm{d}_1}^n}{n!} Y_n \qquad E_{\mathrm{d}_1} Q_{\mathrm{d}_1} = e^{-\mu_{\mathrm{d}_1}} \sum_{n=0}^{\infty} \frac{\mu_{\mathrm{d}_1}^n}{n!} Y_n e_n$$

$$\vdots \qquad\qquad\qquad \vdots$$

$$\underbrace{Q_{\mathrm{d}_\mathrm{N}}}_{\textbf{observed}} = \underbrace{e^{-\mu_{\mathrm{d}_\mathrm{N}}} \sum_{n=0}^{\infty} \frac{\mu_{\mathrm{d}_\mathrm{N}}^n}{n!}}_{\textbf{known}} \underbrace{Y_n}_{\textbf{unknown}} \qquad \underbrace{E_{\mathrm{d}_\mathrm{N}} Q_{\mathrm{d}_\mathrm{N}}}_{\textbf{observed}} = \underbrace{e^{-\mu_{\mathrm{d}_\mathrm{N}}} \sum_{n=0}^{\infty} \frac{\mu_{\mathrm{d}_\mathrm{N}}^n}{n!}}_{\textbf{known}} \underbrace{Y_n e_n}_{\textbf{unknown}}$$

W.-Y. Hwang, PRL 91, 057901 (2003); H.-K. Lo, X. Ma and K. Chen, PRL 94, 230504 (2005); X.-B. Wang, PRL 94, 230503 (2005).

QKD WITH DECOY STATES

For certain cases, as the Poisson distribution, one can obtain analytical bounds for Y_1, e_1

X. Ma, B. Qi, Y. Zhao, H.-K. Lo, Phys. Rev. A 72, 012326 (2005).

QKD with decoy states

For certain cases, as the Poisson distribution, one can obtain analytical bounds for Y_1, e_1

X. Ma, B. Qi, Y. Zhao, H.-K. Lo, Phys. Rev. A 72, 012326 (2005).

In general, one can solve the estimation problem using **linear programming**,

$$\begin{aligned} &\max c^T \mathbf{x} \\ &\text{s.t.} \quad A\mathbf{x} \leq b \\ &\qquad \mathbf{x} \geq 0 \end{aligned}$$

where **x** is a vector of unknown variables, *c* and *b* are vectors whose coefficients are known, and *A* is a known matrix.

QKD WITH DECOY STATES

For certain cases, as the Poisson distribution, one can obtain analytical bounds for Y_1, e_1

X. Ma, B. Qi, Y. Zhao, H.-K. Lo, Phys. Rev. A 72, 012326 (2005).

In general, one can solve the estimation problem using **linear programming**,

$$
\begin{aligned}
&\max c^T \mathbf{x} \\
&\text{s.t.} \quad A\mathbf{x} \leq b \\
&\qquad\quad \mathbf{x} \geq 0
\end{aligned}
$$

where $\mathbf{x}$ is a vector of unknown variables, c and b are vectors whose coefficients are known, and A is a known matrix.

We need a finite number of known/unknown parameters $Q_l = e^{-\mu_l} \sum_{n=0}^{\infty} \frac{\mu_l^n}{n!} Y_n$

QKD with decoy states

For certain cases, as the Poisson distribution, one can obtain analytical bounds for Y_1, e_1

X. Ma, B. Qi, Y. Zhao, H.-K. Lo, Phys. Rev. A 72, 012326 (2005).

In general, one can solve the estimation problem using **linear programming**,

$$\begin{aligned} &\max c^T \mathbf{x} \\ &\text{s.t.} \quad A\mathbf{x} \leq b \\ &\qquad\quad \mathbf{x} \geq 0 \end{aligned}$$

where **x** is a vector of unknown variables, c and b are vectors whose coefficients are known, and A is a known matrix.

We need a finite number of known/unknown parameters $Q_l = e^{-\mu_l} \sum_{n=0}^{\infty} \frac{\mu_l^n}{n!} Y_n$

$$Q_l \geq e^{-\mu_l} \sum_{n=0}^{M_{\text{cut}}} \frac{\mu_l^n}{n!} Y_n$$

$$Q_l \leq e^{-\mu_l} \sum_{n=0}^{M_{\text{cut}}} \frac{\mu_l^n}{n!} Y_n + e^{-\mu_l} \sum_{n=M_{\text{cut}}+1}^{\infty} \frac{\mu_l^n}{n!} = e^{-\mu_l} \sum_{n=0}^{M_{\text{cut}}} \frac{\mu_l^n}{n!} Y_n + \left(1 - e^{-\mu_l} \sum_{n=0}^{M_{\text{cut}}} \frac{\mu_l^n}{n!}\right)$$

QKD WITH DECOY STATES

$$\min \; Y_1$$

$$\text{s.t.} \quad Q_l \geq e^{-\mu_l} \sum_{n=0}^{M_{\text{cut}}} \frac{\mu_l^n}{n!} Y_n \quad \forall l$$

$$Q_l \leq e^{-\mu_l} \sum_{n=0}^{M_{\text{cut}}} \frac{\mu_l^n}{n!} Y_n + \left(1 - e^{-\mu_l} \sum_{n=0}^{M_{\text{cut}}} \frac{\mu_l^n}{n!}\right) \quad \forall l$$

$$1 \geq Y_n \geq 0$$

⇨ Lower bound for Y_1

This is done for both BB84 basis.

QKD with decoy states

$$\begin{aligned}
&\min \quad Y_1 \\
&\text{s.t.} \quad Q_l \geq e^{-\mu_l} \sum_{n=0}^{M_{\text{cut}}} \frac{\mu_l^n}{n!} Y_n \quad \forall l \\
&\qquad Q_l \leq e^{-\mu_l} \sum_{n=0}^{M_{\text{cut}}} \frac{\mu_l^n}{n!} Y_n + \left(1 - e^{-\mu_l} \sum_{n=0}^{M_{\text{cut}}} \frac{\mu_l^n}{n!}\right) \quad \forall l \\
&\qquad 1 \geq Y_n \geq 0
\end{aligned}$$

$\Rightarrow$ Lower bound for Y_1

This is done for both BB84 basis.

Similarly, if we define $\gamma_n = Y_n e_n$

$$\begin{aligned}
&\max \quad \gamma_1 \\
&\text{s.t.} \quad E_l Q_l \geq e^{-\mu_l} \sum_{n=0}^{M_{\text{cut}}} \frac{\mu_l^n}{n!} \gamma_n \quad \forall l \\
&\qquad E_l Q_l \leq e^{-\mu_l} \sum_{n=0}^{M_{\text{cut}}} \frac{\mu_l^n}{n!} \gamma_n + \left(1 - e^{-\mu_l} \sum_{n=0}^{M_{\text{cut}}} \frac{\mu_l^n}{n!}\right) \quad \forall l \\
&\qquad 1 \geq \gamma_n \geq 0
\end{aligned}$$

$\Rightarrow$ Upper bound for e_1 :

$$e_1 \leq \frac{\gamma_1}{Y_1}$$

QKD WITH DECOY STATES

$$R \geq q\left\{p_{1|\mathrm{s}} Y_1 [1 - h(e_1)] - Q_\mathrm{s} h(E_\mathrm{s})\right\}$$

$p_{1,\mathrm{s}} = \mu_\mathrm{s} e^{-\mu_\mathrm{s}}$	is the conditional probability that Alice emits a single-photon state when she uses the signal intensity setting (***known***)
Q_s	is the overall gain of the signal states (***observed***)
E_s	is the overall error rate of the signal states (***observed***)

D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, Quantum Inf. Comput. 4, 325 (2004).

QKD WITH DECOY STATES

$$R \geq q\left\{p_{1|\mathrm{s}} Y_1[1-h(e_1)] - Q_\mathrm{s} h(E_\mathrm{s})\right\}$$

$p_{1,\mathrm{s}} = \mu_\mathrm{s} e^{-\mu_\mathrm{s}}$ is the conditional probability that Alice emits a single-photon state when she uses the signal intensity setting (***known***)

Q_s is the overall gain of the signal states (***observed***)

E_s is the overall error rate of the signal states (***observed***)

If we use the channel model described before:

<u>Example:</u>

$p_\mathrm{dark} = 10^{-6}$

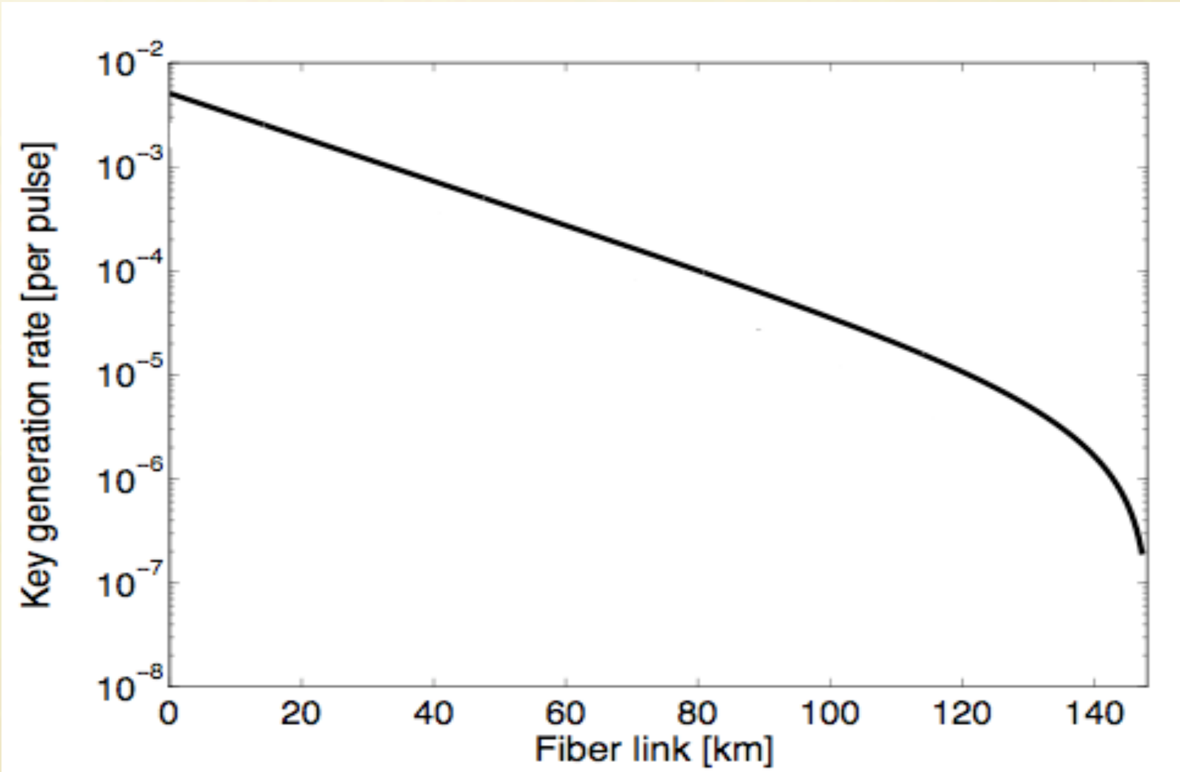
$e_d = \sin^2\theta = 0.015$

$\eta_\mathrm{B} = 0.045$

$\alpha = 0.2$ dB/km

$q \approx 1$

μ optimised



D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, Quantum Inf. Comput. 4, 325 (2004).

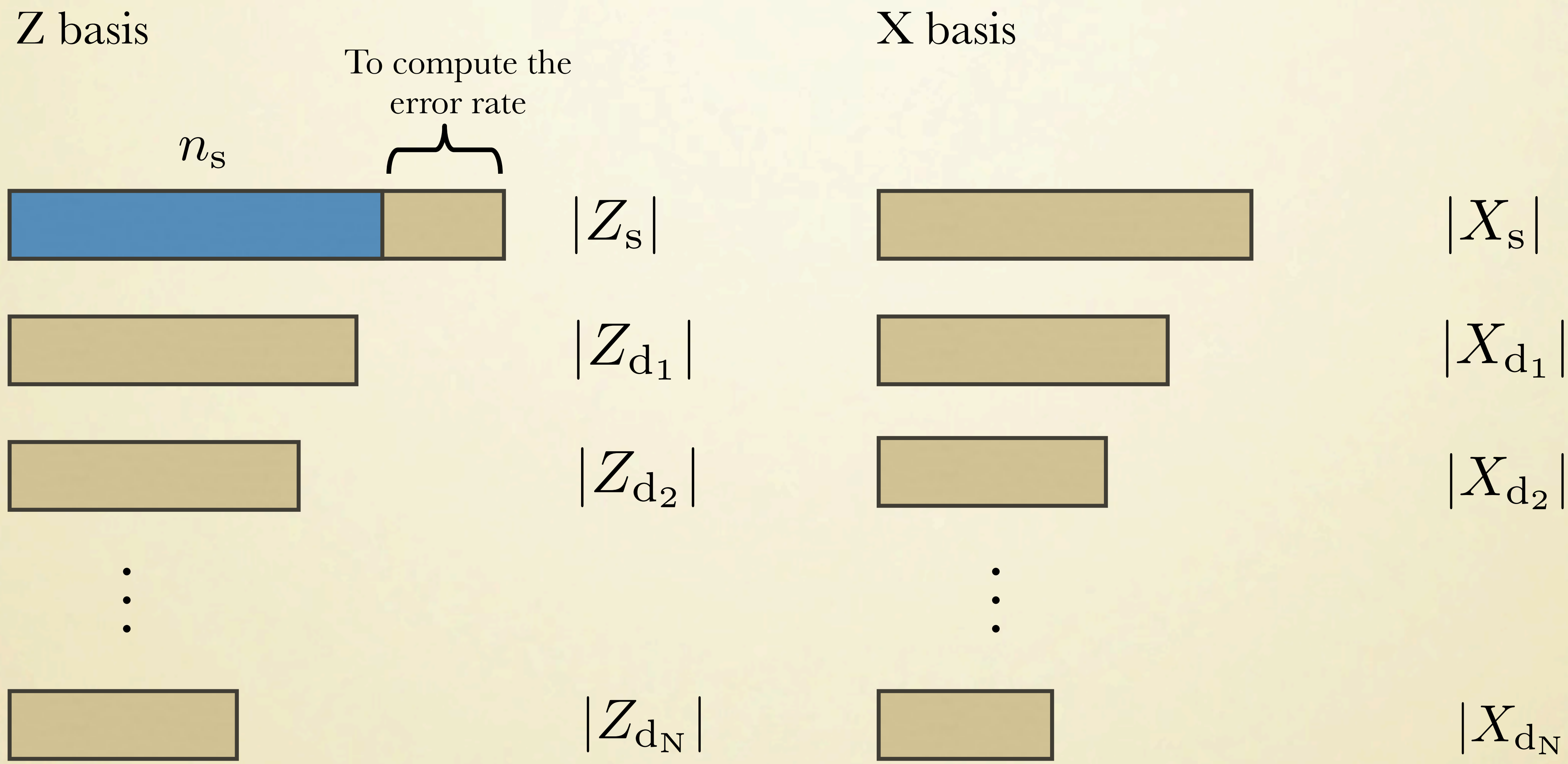
Parameter estimation (finite case)

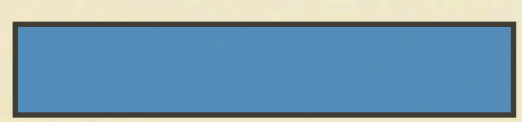
Parameter estimation (finite case)

In any experiment Alice only sends a finite number of signals. When the sifting conditions are met we have that

Parameter estimation (finite case)

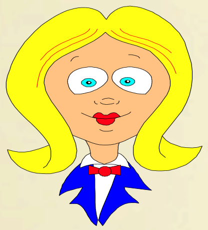
In any experiment Alice only sends a finite number of signals. When the sifting conditions are met we have that



We need to compute a lower bound for the number of single photons and an upper bound for their phase error rate in the set 

Parameter estimation (finite case)

Actual protocol (let us focus, for instance, in the Z basis):

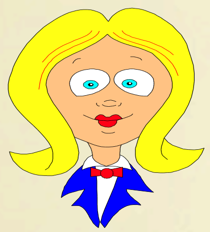


Alice

Alice chooses an intensity setting l with probability $p(l|\mathrm{Z})$ $\Rightarrow$ $\rho_l = e^{-\mu_l} \sum_{n=0}^{\infty} \frac{\mu_l^n}{n!} |n\rangle\langle n|$

Parameter estimation (finite case)

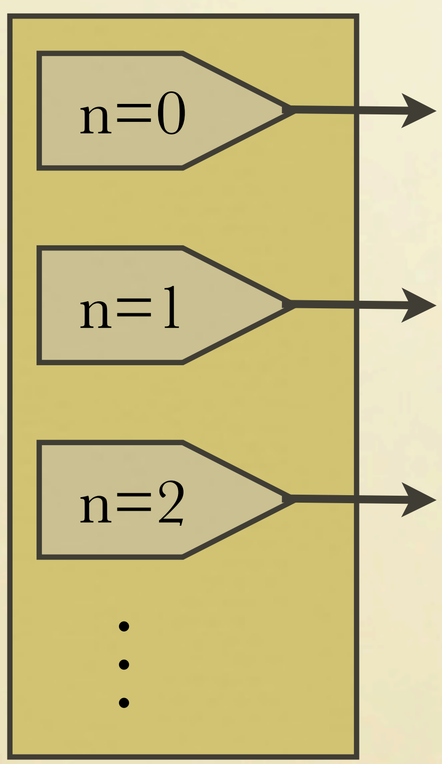
Actual protocol (let us focus, for instance, in the Z basis):


Alice

Alice chooses an intensity setting l with probability $p(l|\mathrm{Z})$

$$\rho_l = e^{-\mu_l} \sum_{n=0}^{\infty} \frac{\mu_l^n}{n!} |n\rangle\langle n|$$

Equivalent protocol:



For each signal, Alice first chooses a photon number n with probability

$$p(n|\mathrm{Z}) = \sum_l p(l|\mathrm{Z}) p(n|l, \mathrm{Z})$$

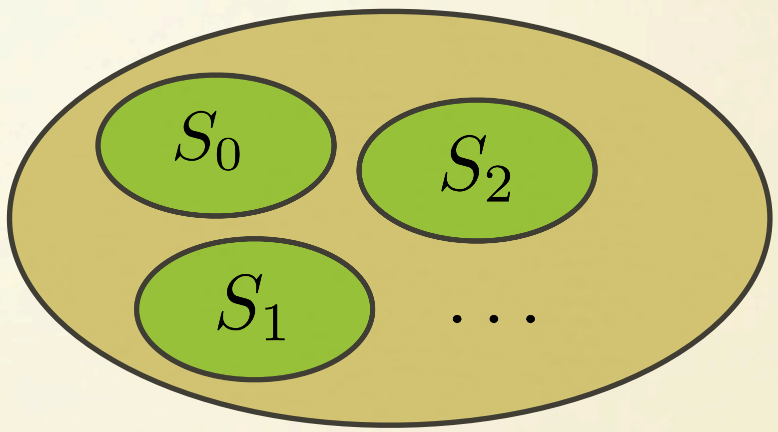
After Bob declares the detected events, Alice decides the intensity setting l with probability

$$p(l|n, \mathrm{Z}) = p(n|l, \mathrm{Z}) \frac{p(l|\mathrm{Z})}{p(n|\mathrm{Z})}$$

Parameter estimation (finite case)

Let S_n denote the number of signals sent by Alice with n photons, when both Alice and Bob select the basis Z, and Bob obtains a click in his measurement apparatus.

$$\sum_l |Z_l| = \sum_n S_n$$

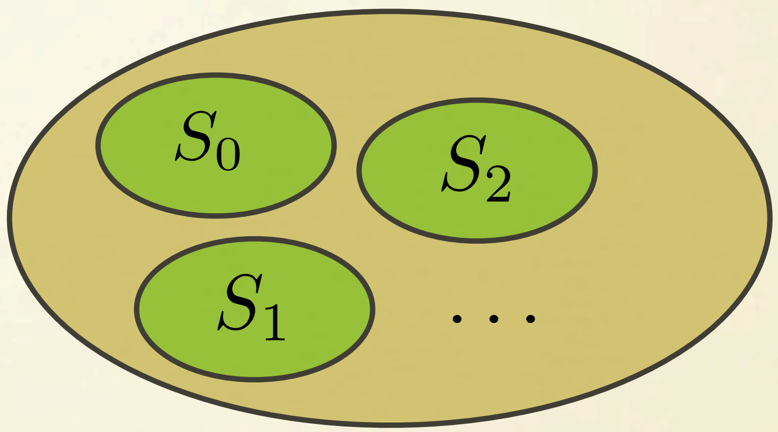


Set of detected events

Parameter estimation (finite case)

Let S_n denote the number of signals sent by Alice with *n* photons, when both Alice and Bob select the basis Z, and Bob obtains a click in his measurement apparatus.

$$\sum_l |Z_l| = \sum_n S_n$$



Set of detected events

Using the equivalent protocol we expect to be able to write:

$$\underbrace{|Z_l|}_{\textit{observed}} = \sum_n \underbrace{p(l|n,\mathrm{Z})}_{\textit{known}} \underbrace{S_n}_{\textit{unknown}} + \underbrace{\delta_l}_{\textit{can be bounded}}$$

We will be able to obtain the parameters S_n , in particular S_1

Parameter estimation (finite case)

How to bound the fluctuation term δ_l $\longrightarrow$ Example: Chernoff bound

Parameter estimation (finite case)

How to bound the fluctuation term $\delta_l \quad \longrightarrow \quad$ Example: Chernoff bound

Claim 1. *Let $X_1, X_2, \ldots, X_n$, be a set of independent Bernoulli trials that satisfy* $\Pr(X_i = 1) = p_i$. *And, let $X = \sum_{i=1}^{n} X_i$ and $\mu = E[X] = \sum_{i}^{n} p_i$, where $E[\cdot]$ is the mean value. Then, we have that*

$$X = \mu + \delta, \tag{B1}$$

except with error probability $\gamma = \varepsilon + \hat{\varepsilon}$, where the parameter $\delta \in [-\Delta, \hat{\Delta}]$, with $\Delta = g(X, \varepsilon^{2(4+\sqrt{7})^2/9})$ and $\hat{\Delta} = g(X, \hat{\varepsilon}^3)$, and the function $g(x, y) = \sqrt{x \ln(y^{-1})}$, given that $\max\{\hat{\varepsilon}^{-1/X}, \varepsilon^{-1/X}\} \leq$ $\exp(1/3)$.

Parameter estimation (finite case)

How to bound the fluctuation term δ_l $\longrightarrow$ Example: Chernoff bound

Claim 1. *Let $X_1, X_2, \ldots, X_n$, be a set of independent Bernoulli trials that satisfy* $\Pr(X_i = 1) = p_i$. *And, let $X = \sum_{i=1}^n X_i$ and $\mu = E[X] = \sum_i^n p_i$, where $E[\cdot]$ is the mean value. Then, we have that*

$$X = \mu + \delta, \tag{B1}$$

except with error probability $\gamma = \varepsilon + \hat{\varepsilon}$, where the parameter $\delta \in [-\Delta, \hat{\Delta}]$, with $\Delta = g(X, \varepsilon^{2(4+\sqrt{7})^2/9})$ and $\hat{\Delta} = g(X, \hat{\varepsilon}^3)$, and the function $g(x,y) = \sqrt{x \ln (y^{-1})}$, given that $\max\{\hat{\varepsilon}^{-1/X}, \varepsilon^{-1/X}\} \leq$ $\exp(1/3)$.

This implies that

$$|Z_l| = \sum_n p(l|n, \mathrm{Z}) S_n + \delta_l$$

except with error probability $\gamma_l = \epsilon_l + \hat{\epsilon}_l$, where $\delta_l \in [-\Delta_l, \hat{\Delta}_l]$, with

$$\Delta_l = g\left(|Z_l|, \epsilon_l^{2(4+\sqrt{7})^2/9}\right)$$
$$\hat{\Delta}_l = g\left(|Z_l|, \hat{\epsilon}_l^3\right)$$

Importantly, the fluctuation term is bounded by observed quantities and the tolerated failure probability

Parameter estimation (finite case)

We have **more conditions**: $N_n \geq S_n \geq 0$

N_n : Number of signals sent by Alice with n photons, when she and Bob select the Z basis.

Parameter estimation (finite case)

We have **more conditions**: $N_n \geq S_n \geq 0$

N_n : Number of signals sent by Alice with n photons, when she and Bob select the Z basis.

Using Chernoff inequality, we have that

$$p\left(N_n \geq N[p(n|\mathrm{Z}) + \xi_n]\right) \leq e^{-N\xi_n^2/[2(p(n|\mathrm{Z})+\xi_n)]}$$

$$p\left(N_n \leq N[p(n|\mathrm{Z}) - \xi_n]\right) \leq e^{-N\xi_n^2/[2p(n|\mathrm{Z})]}$$

where $N = \sum_n N_n$ is the number of signals sent by Alice and measured by Bob in the Z basis

Parameter estimation (finite case)

We have **more conditions**: $N_n \geq S_n \geq 0$

N_n : Number of signals sent by Alice with n photons, when she and Bob select the Z basis.

Using Chernoff inequality, we have that

$$p\left(N_n \geq N[p(n|\mathrm{Z}) + \xi_n]\right) \leq e^{-N\xi_n^2/[2(p(n|\mathrm{Z})+\xi_n)]}$$

$$p\left(N_n \leq N[p(n|\mathrm{Z}) - \xi_n]\right) \leq e^{-N\xi_n^2/[2p(n|\mathrm{Z})]}$$

where $N = \sum_n N_n$ is the number of signals sent by Alice and measured by Bob in the Z basis

Equivalently, we can say that $N_n = N[p(n|\mathrm{Z}) + \delta_n]$

except with error probability $\gamma_n = \epsilon_n + \hat{\epsilon}_n$, where $\delta_n \in [-\Delta_n, \hat{\Delta}_n]$, with

$$\Delta_n = \min\left\{g[p(n|\mathrm{Z})/N, \epsilon_n^2], p(n|\mathrm{Z})\right\}$$
$$\hat{\Delta}_n = \min\left\{f[N, p(n|\mathrm{Z}), \hat{\epsilon}_n], 1 - p(n|\mathrm{Z})\right\}$$

We also use $N \geq N_n \geq 0$

where $g(x,y) = \sqrt{x \ln(y^{-1})}$ and $f(x,y,z) = \ln(z^{-1})[1 + \sqrt{1 + 2xy/\ln(z^{-1})}]/x$

Parameter estimation (finite case)

Based on the foregoing:

$$\begin{aligned}
&\min \;\; S_1 \\
&\text{s.t.} \;\; |Z_l| = \sum_{n=0}^{\infty} p(l|n,\mathrm{Z})S_n + \delta_l, \quad \forall l \\
&\qquad \hat{\Delta}_l \geq \delta_l \geq -\Delta_l, \quad \forall l \\
&\qquad \sum_l \delta_l = 0, \quad \forall l \quad \text{(from the condition } \sum_l |Z_l| = \sum_n S_n\text{)} \\
&\qquad N[p(n|\mathrm{Z}) + \delta_n] \geq S_n \geq 0, \quad \forall n \\
&\qquad \hat{\Delta}_n \geq \delta_n \geq -\Delta_n, \quad \forall n
\end{aligned}$$

except with error probability ϵ_1 given by $\epsilon_1 \leq \sum_l \gamma_l + \sum_n \gamma_n$

Unknown parameters: S_n, δ_l, δ_n

Parameter estimation (finite case)

Based on the foregoing:

$$
\begin{aligned}
&\min \;\; S_1 \\
&\text{s.t.} \quad |Z_l| = \sum_{n=0}^{\infty} p(l|n, \mathrm{Z}) S_n + \delta_l, \quad \forall l \\
&\qquad\quad \hat{\Delta}_l \geq \delta_l \geq -\Delta_l, \quad \forall l \\
&\qquad\quad \sum_l \delta_l = 0, \quad \forall l \quad \text{(from the condition } \sum_l |Z_l| = \sum_n S_n) \\
&\qquad\quad N[p(n|\mathrm{Z}) + \delta_n] \geq S_n \geq 0, \quad \forall n \\
&\qquad\quad \hat{\Delta}_n \geq \delta_n \geq -\Delta_n, \quad \forall n
\end{aligned}
$$

except with error probability ϵ_1 given by $\epsilon_1 \leq \sum_l \gamma_l + \sum_n \gamma_n$

Unknown parameters: S_n, δ_l, δ_n

→ This linear optimisation problem can be solved analytically or numerically using linear programming

Parameter estimation (finite case)

Example: Solution using **linear programming**. We reduce the number of unknown parameters to a finite set:

Parameter estimation (finite case)

Example: Solution using **linear programming**. We reduce the number of unknown parameters to a finite set:

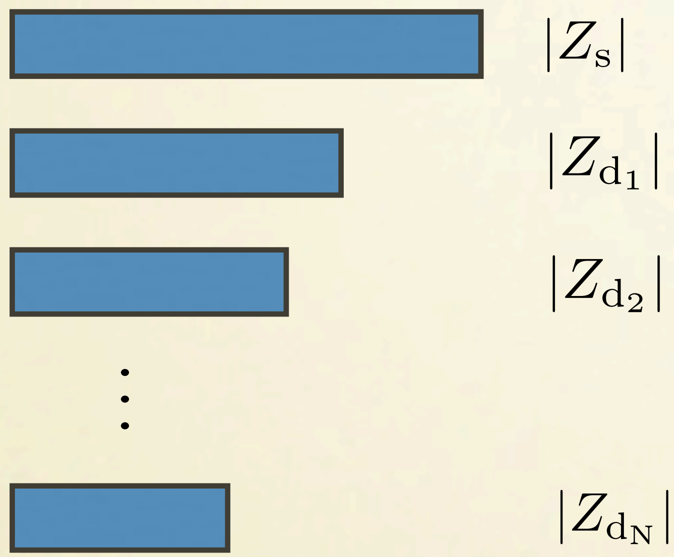
$$
\begin{aligned}
\min\ & S_1 \\
\text{s.t.}\ & |Z_l| \geq \sum_{n\in\mathcal{S}_{\rm cut}} p(l|n,Z)S_n + \delta_l, \quad \forall l \\
& |Z_l| \leq \sum_{n\in\mathcal{S}_{\rm cut}} p(l|n,Z)S_n + \delta_l + \max_{j\notin\mathcal{S}_{\rm cut}} p(l|j,Z)N\left[1 - \sum_{n\in\mathcal{S}_{\rm cut}} (p(n|Z)+\delta_n)\right], \quad \forall l \\
& \hat{\Delta}_l \geq \delta_l \geq -\Delta_l, \quad \forall l \\
& \sum_l \delta_l = 0, \quad \forall l \\
& N[p(n|\mathrm{Z}) + \delta_n] \geq S_n \geq 0, \quad \forall n \in \mathcal{S}_{\rm cut} \\
& \hat{\Delta}_n \geq \delta_n \geq -\Delta_n, \quad \forall n \in \mathcal{S}_{\rm cut}
\end{aligned}
$$

except with error probability ϵ_1 given by $\epsilon_1 \leq \sum_l \gamma_l + \sum_{n\,\in\,\mathcal{S}_{\rm cut}} \gamma_n$

Here: $\mathcal{S}_{\rm cut} = \{n:\ 0 \leq n \leq M_{\rm cut}\}$

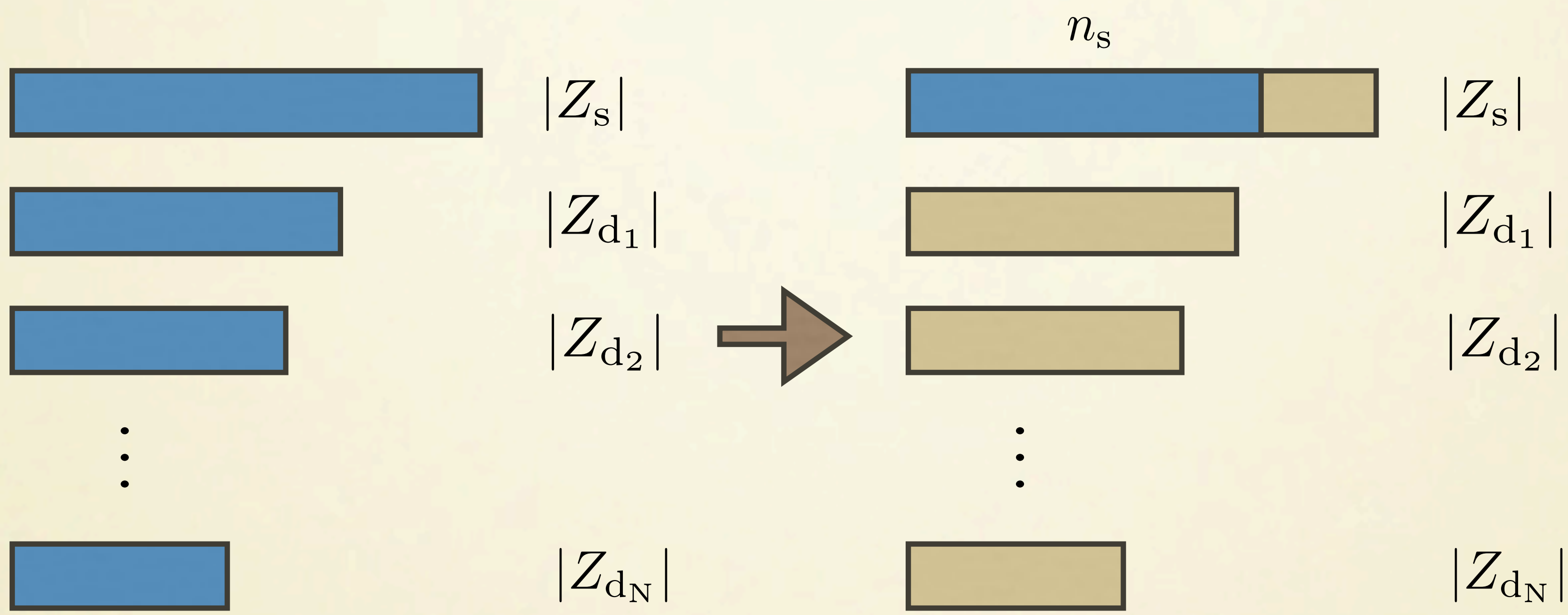
Parameter estimation (finite case)

S_1 is a lower bound for the number of single photon in the Z basis:



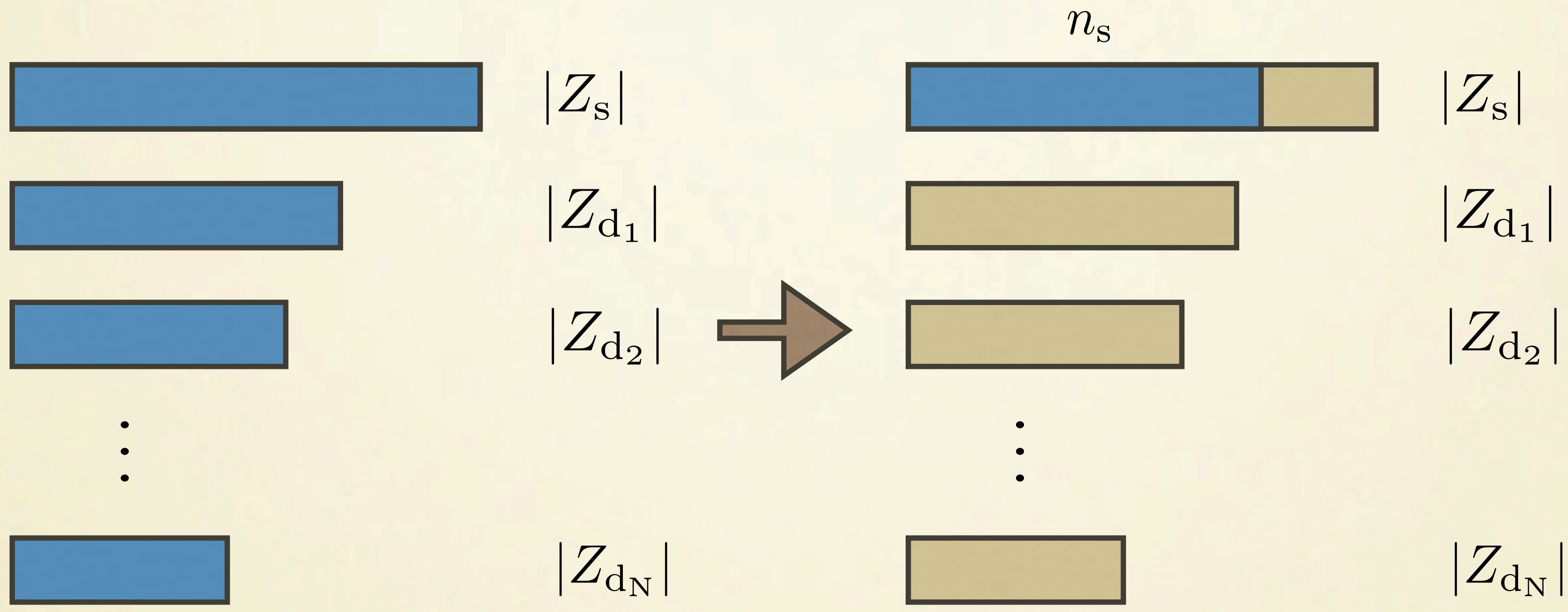
Parameter estimation (finite case)

S_1 is a lower bound for the number of single photon in the Z basis:



Parameter estimation (finite case)

S_1 is a lower bound for the number of single photon in the Z basis:



Using again Chernoff bound: $n_1 \geq p(\mathrm{s}|1,\mathrm{Z})\dfrac{n_{\rm s}}{|Z_{\rm s}|}S_1 - \Delta_1$

except with error probability ϵ_1' , where:

$$\Delta_1 = g\left(p(\mathrm{s}|1,\mathrm{Z})\frac{n_{\rm s}}{|Z_{\rm s}|}S_1, \epsilon_1'^2\right)$$

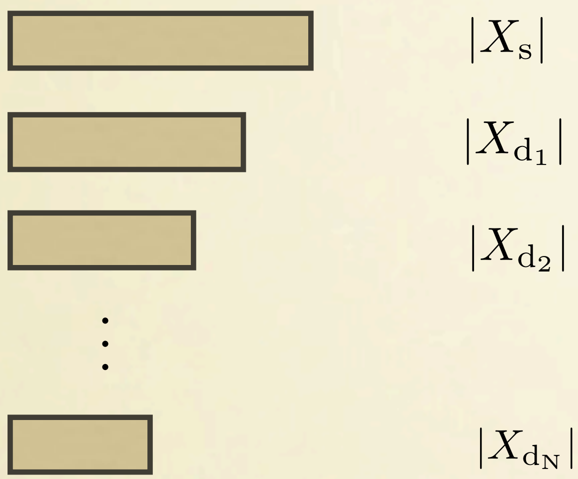
Total error probability in the estimation of n_1 : $\varepsilon_1 \leq \epsilon_1' + \sum_l \gamma_l + \sum_{n\in\mathcal{S}_{\rm cut}} \gamma_n$

Parameter estimation (finite case)

Let us know calculate the phase error of the single photons:

Parameter estimation (finite case)

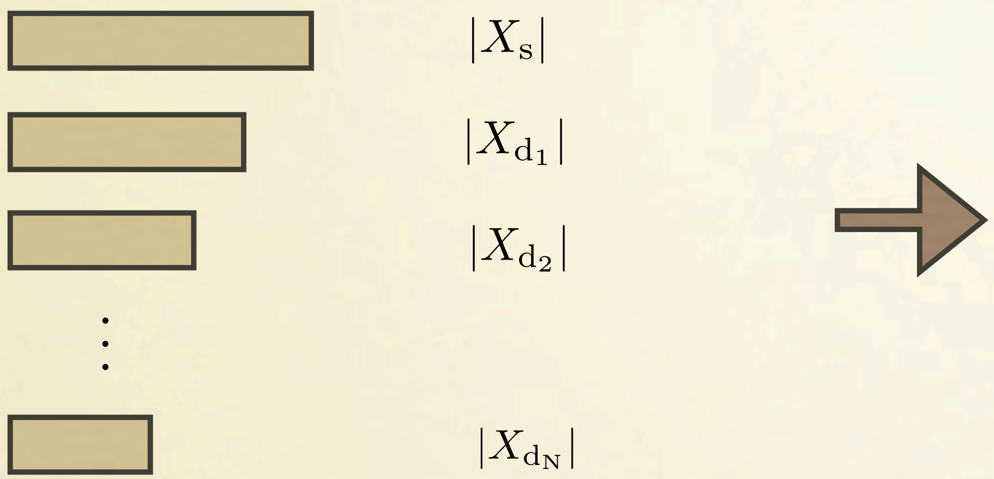
Let us know calculate the phase error of the single photons:



Using the same techniques as before we can obtain a lower bound for S_1 (in the X basis) and an upper bound for the number of errors $\bar{e}_1$ associated to single-photon events in the X basis

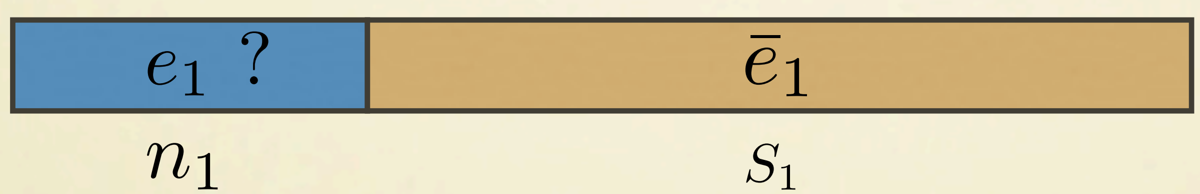
Parameter estimation (finite case)

Let us know calculate the phase error of the single photons:



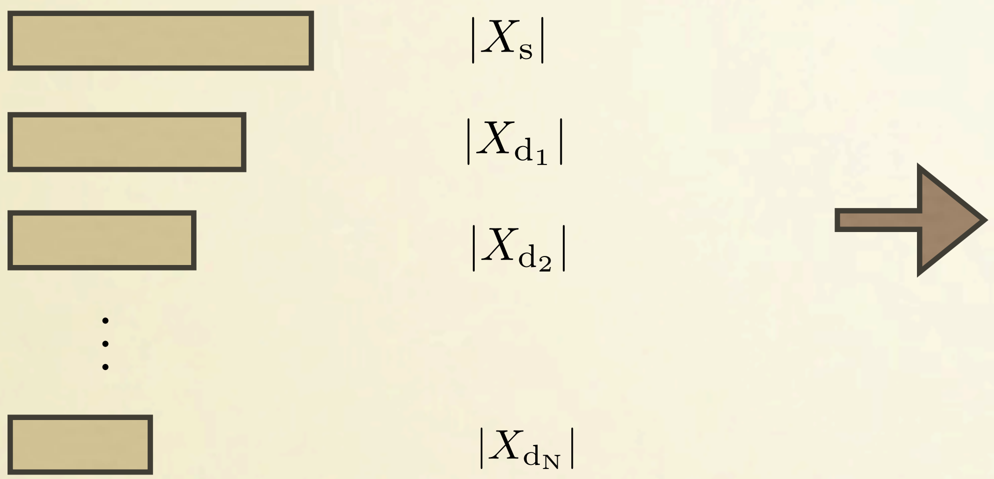
Using the same techniques as before we can obtain a lower bound for S_1 (in the X basis) and an upper bound for the number of errors $\bar{e}_1$ associated to single-photon events in the X basis

Now we can use a result from random sampling without replacement:



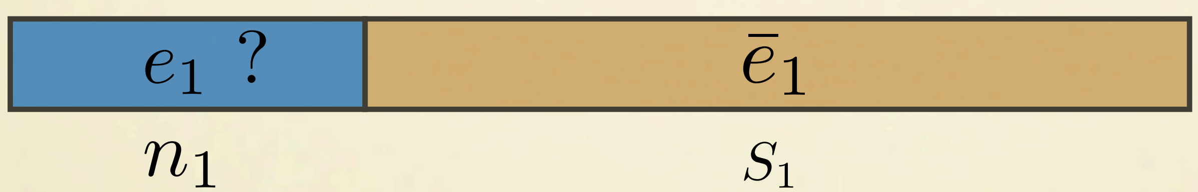
Parameter estimation (finite case)

Let us know calculate the phase error of the single photons:



Using the same techniques as before we can obtain a lower bound for S_1 (in the X basis) and an upper bound for the number of errors $\bar{e}_1$ associated to single-photon events in the X basis

Now we can use a result from random sampling without replacement:



$$e_1 \leq \min\left\{\left\lceil n_1\left(\frac{\bar{e}_1}{S_1}\right) + (n_1+S_1)\Omega(n_1, S_1, \epsilon_e)\right\rceil, n_1/2\right\} \text{ with } \Omega(x,y,z) = \sqrt{(x+1)\ln(z^{-1})/(2y(x+y))}$$

except with error probability $\epsilon_{e_1} \leq \epsilon_e + \sum_l (\gamma_l + \gamma_{l,e}) + \sum_{n\in\mathcal{S}_{\mathrm{cut}}} \gamma_n$

R. J. Serfling, Ann. Statist. 2 (1), 39-48 (1974).

Side-channels

Side-channels

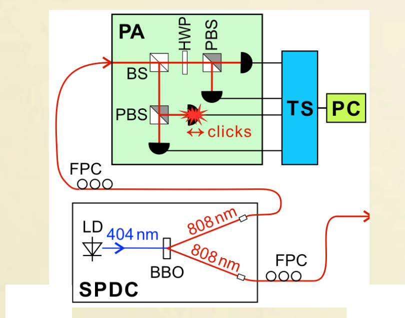
Are experimental implementations of QKD really secure?

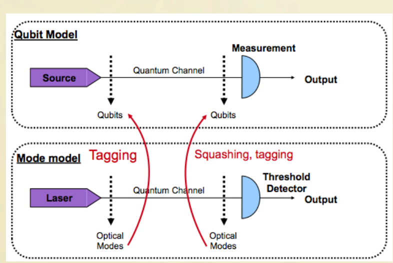
Side-channels

Are experimental implementations of QKD really secure?

Side-channels

The security proof of a QKD system typically includes several steps





$$\frac{1}{2}||\rho_{\mathrm{AE}} - U_{\mathrm{A}} \otimes \rho_{\mathrm{E}}|| \leq \epsilon$$

$$\rho_{\mathrm{AE}} = \sum_s |s\rangle\langle s| \otimes \rho_{\mathrm{E}}^s$$

$$U_{\mathrm{A}} = \frac{1}{|\mathcal{S}|}\sum_s |s\rangle\langle s|$$

Actual physical devices

↓ Modelling

Quantum optical model e.g. mode based

e.g. realistic laser sources
beamsplitters model
threshold detectors model

↓ Reduction to essentials
e.g. tagging, squashing

Security model e.g. qubit based

↓ Entanglement distillation
Information theoretic

Security proof

From a mathematical model for employed devices we can provide a scientific (mathematical and physical) universally composable security proof for QKD: perfect key except with probability ε

Side-channels

Modelling of real devices: What can go wrong?

Side-channels

Modelling of real devices: What can go wrong?

State preparation:

- Does the source emit coherent states?
- Are the states truly phase-randomised?
- Are we preparing perfect BB84 states?
- Are the states single-mode?
- Consider intensity fluctuations in the source...

$\vdots$

Side-channels

Modelling of real devices: What can go wrong?

State preparation:

- Does the source emit coherent states?
- Are the states truly phase-randomised?
- Are we preparing perfect BB84 states?
- Are the states single-mode?
- Consider intensity fluctuations in the source...

⋮

If we know the imperfections we can include them in the security proof

Side-channels

Modelling of real devices: What can go wrong?

State preparation:

- Does the source emit coherent states?
- Are the states truly phase-randomised?
- Are we preparing perfect BB84 states?
- Are the states single-mode?
- Consider intensity fluctuations in the source...

⋮

If we know the imperfections we can include them in the security proof

Measurement device:

- Problem with efficiency mismatch
- Take into account the dead-time of the detectors
- Guarantee that the BS (passive receiver) cannot be controlled by Eve (e.g. wavelength dependence)

⋮

- **Do the detectors behave as we expect?**

Side-channels

Modelling of real devices: What can go wrong?

State preparation:

- Does the source emit coherent states?
- Are the states truly phase-randomised?
- Are we preparing perfect BB84 states?
- Are the states single-mode?
- Consider intensity fluctuations in the source...

⋮

If we know the imperfections we can include them in the security proof

Measurement device:

- Problem with efficiency mismatch
- Take into account the dead-time of the detectors
- Guarantee that the BS (passive receiver) cannot be controlled by Eve (e.g. wavelength dependence)

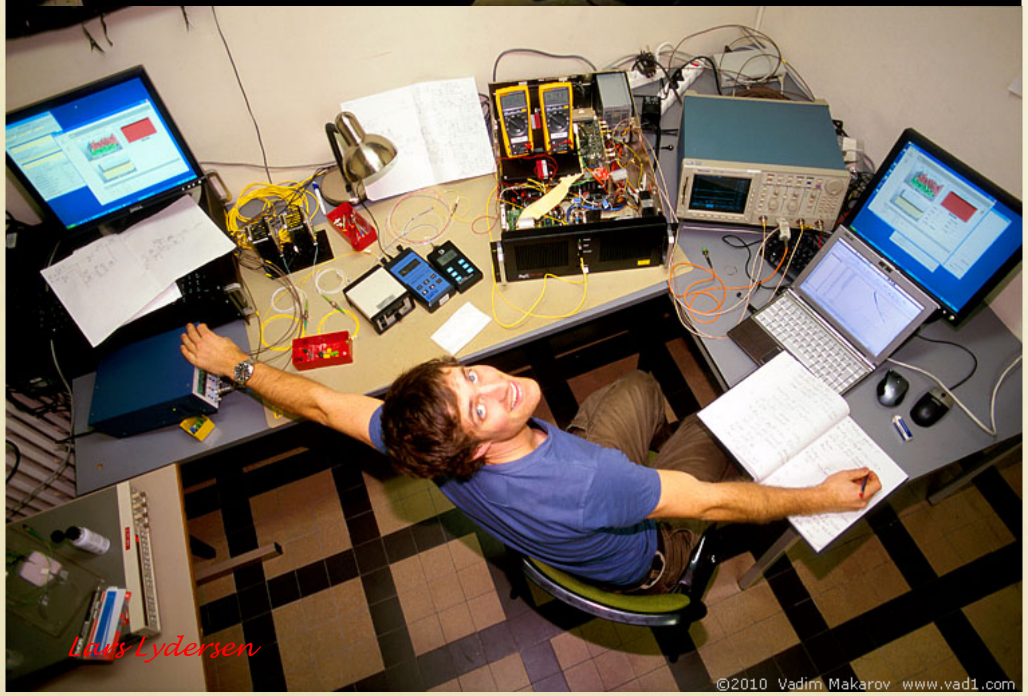
⋮

- **Do the detectors behave as we expect?**

The **weakest link** in a QKD system is the measurement device

Side-channels

Quantum hacking: Blinding attack



NTNU
Norwegian University of
Science and Technology

nature photonics

nature.com ▸ journal home ▸ archive ▸ issue ▸ letter ▸ abstract

ARTICLE PREVIEW
view full access options ▸

NATURE PHOTONICS | LETTER

Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar & Vadim Makarov

Affiliations | Contributions | Corresponding author

Nature Photonics **4**, 686–689 (2010) | doi:10.1038/nphoton.2010.214
Received 02 April 2010 | Accepted 11 July 2010 | Published online 29 August 2010

Abstract

Abstract • Author information • Supplementary information

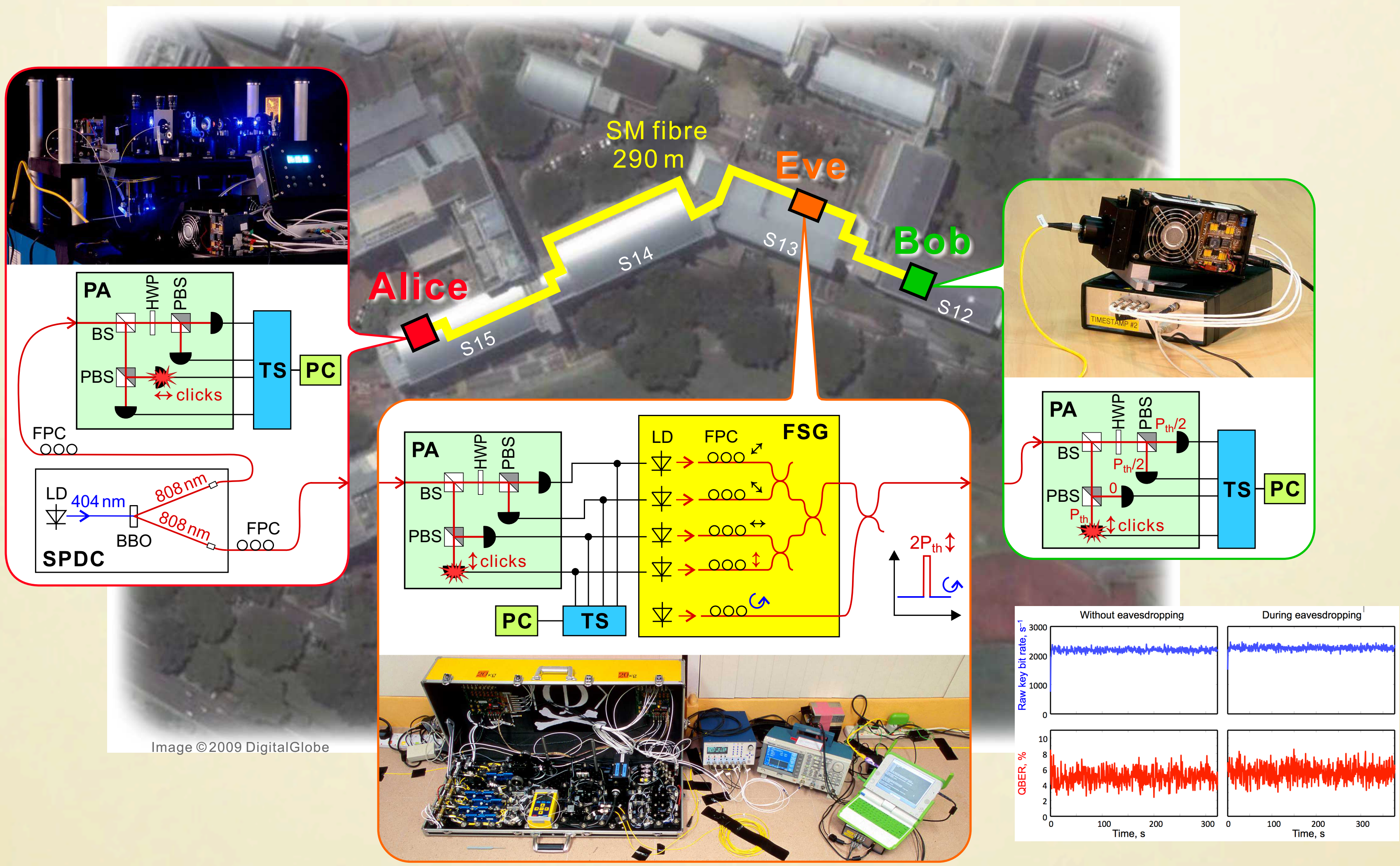
The peculiar properties of quantum mechanics allow two remote parties to communicate a private, secret key, which is protected from eavesdropping by the laws of physics[1, 2, 3, 4]. So-called quantum key distribution (QKD) implementations always rely on detectors to measure the relevant quantum property of single photons[5]. Here we demonstrate experimentally that the detectors in two commercially available QKD systems can be fully remote-controlled using specially tailored bright illumination. This makes it possible to tracelessly acquire the full secret key; we propose an eavesdropping apparatus built from off-the-shelf components. The loophole is likely to be present in most QKD systems using avalanche photodiodes to detect single photons. We believe that our findings are crucial for strengthening the security of practical QKD, by identifying and patching technological deficiencies.

print
email
download citation
order reprints
rights and permissions
share/bookmark

Subject terms: Quantum optics

SIDE-CHANNELS

Eavesdropping 100% of the key on installed QKD line.



I. Gerhardt et al., Nature Comm. 2, 349 (2011).

See also:

Y. Zhao et al., Phys. Rev. A 78, 042333 (2008).
N. Jain et al., Phys. Rev. Lett. 107, 110501 (2011).
H. Weier et al., New J. Phys. 13, 073024 (2011)

Side-channels

Bridging the gap between theory and practice...

SIDE-CHANNELS

Bridging the gap between theory and practice...

Option 1: "Patches"

- *Abandon the provable security model of QKD*
- *Can often be defeated by hacking advances*

Side-channels

Bridging the gap between theory and practice...

Option 1: “Patches”

- *Abandon the provable security model of QKD*
- *Can often be defeated by hacking advances*

Option 2: Integrate imperfections into the security proof

- *Typically, it may need deep modification of the protocol, hardware and security proof*
- ***Device-independent quantum key distribution** (avoids the hard-verifiable requirement of completely characterizing real devices)*

Side-channels

Device independent QKD (diQKD)/Self-testing QKD

D. Mayers and A. C.-C. Yao, in Proc. 39th Annual Symposium on Foundations of Computer Science (FOCS98), p. 503 (1998); A. Acín et al., Phys. Rev. Lett. 98, 230501 (2007); A. Acín, N. Gisin and Ll. Masanes, Phys. Rev. Lett. 97, 120405 (2006).

SIDE-CHANNELS

Device independent QKD (diQKD)/Self-testing QKD

We still need some assumptions: validity of QM, true RNG, Alice and Bob shielded from Eve, no memory, ... Removes the problem of full characterising real devices!

D. Mayers and A. C.-C. Yao, in Proc. 39th Annual Symposium on Foundations of Computer Science (FOCS98), p. 503 (1998); A. Acín et al., Phys. Rev. Lett. 98, 230501 (2007); A. Acín, N. Gisin and Ll. Masanes, Phys. Rev. Lett. 97, 120405 (2006).

SIDE-CHANNELS

Device independent QKD (diQKD)/Self-testing QKD

We still need some assumptions: validity of QM, true RNG, Alice and Bob shielded from Eve, no memory, ... Removes the problem of full characterising real devices!

BASIC idea: The existence of entanglement => possibility of secure key generation

Bell inequalities test => Entanglement verification

Alice and Bob can perform Bell inequality test with untrusted devices

If p(a,b|x,y) violates some Bell inequality, then p(a,b|x,y) contains secrecy irrespectively of the implementation!

Advantage: diQKD eliminates ALL potential side-channels

D. Mayers and A. C.-C. Yao, in Proc. 39th Annual Symposium on Foundations of Computer Science (FOCS98), p. 503 (1998); A. Acín et al., Phys. Rev. Lett. 98, 230501 (2007); A. Acín, N. Gisin and Ll. Masanes, Phys. Rev. Lett. 97, 120405 (2006).

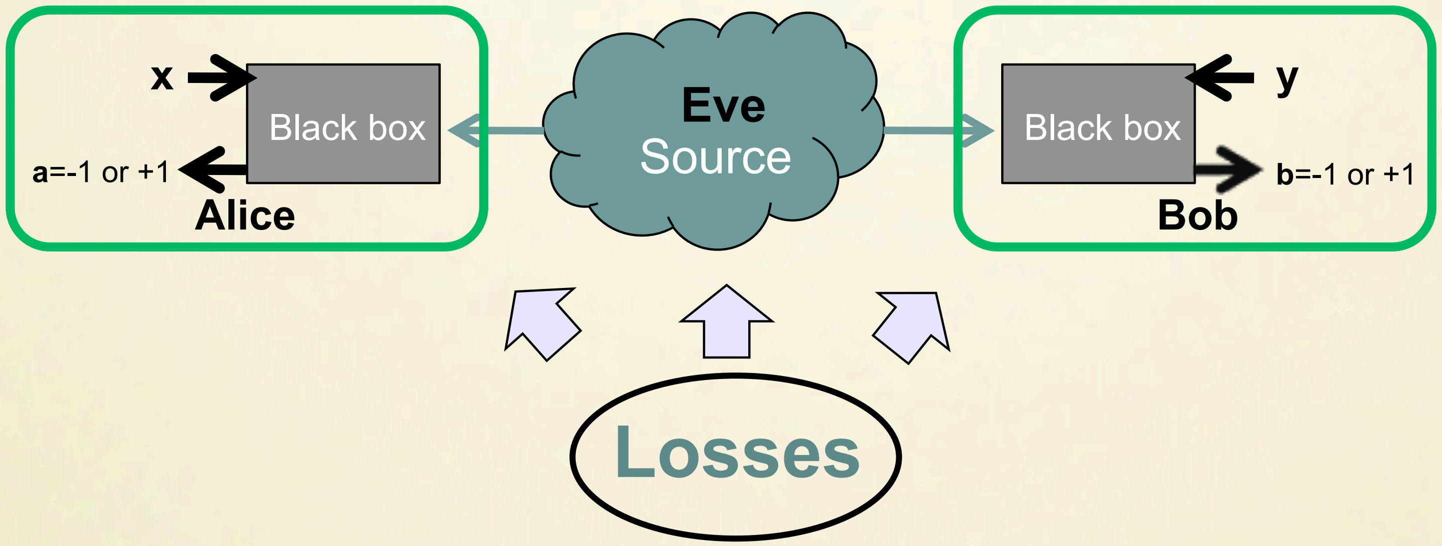
Side-channels

Now... let's go to the lab

Side-channels

Now… let's go to the lab

We need to violate a Bell inequality loophole-free $\longrightarrow$ Very hard!

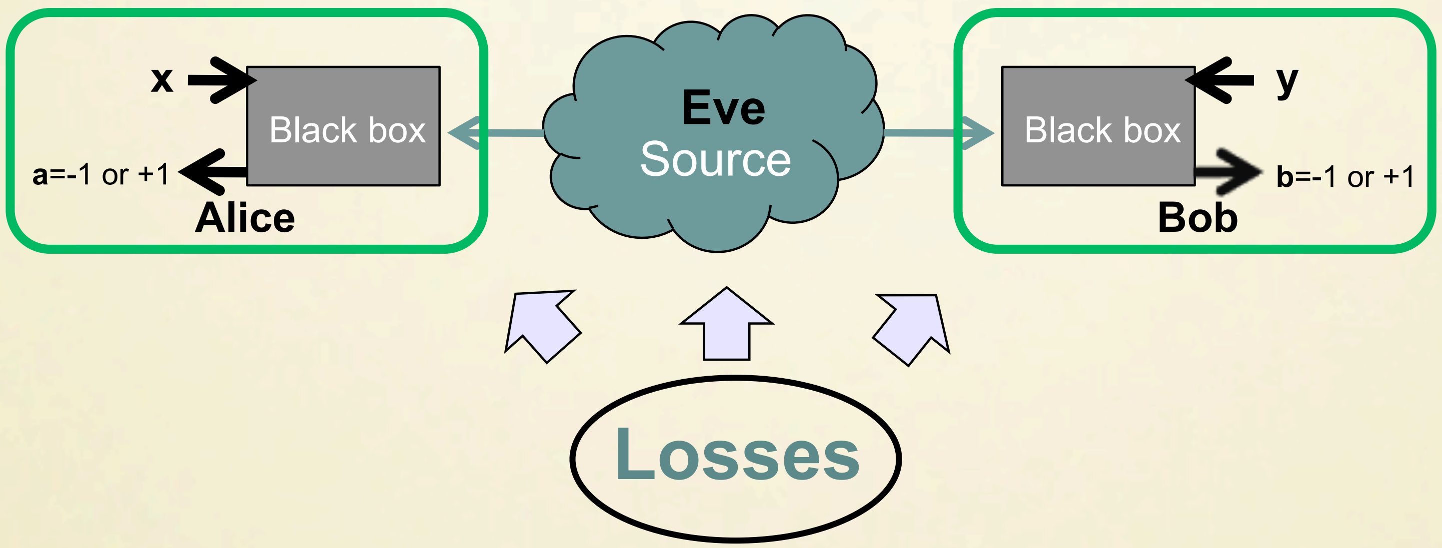


Patch: random/deterministic assignment for lost signals $\longrightarrow$ increase error rate $\longrightarrow$ loss of violation

Side-channels

Now... let's go to the lab

We need to violate a Bell inequality loophole-free $\longrightarrow$ Very hard!



Patch: random/deterministic assignment for lost signals $\longrightarrow$ increase error rate $\longrightarrow$ loss of violation

Detection loophole

Required detection efficiency > 82.8%

But the transmission efficiency of 5 km of telecom fiber is roughly 80%; typical detection efficiencies are 10-15%

Side-channels

Fair-sampling device

N. Gisin, S. Pironio and N. Sangouard, *Phys. Rev. Lett.* 105, 070501 (2010); N. Sangouard et al., *Phys. Rev. Lett.* 106, 120403 (2011); M. Curty and T. Moroder, *Phys. Rev. A* 84, 010304(R) (2011).

SIDE-CHANNELS

Fair-sampling device

In Bell tests $\longrightarrow$ assume that the set of detected photon pairs is a fair set (fair-sampling assumption). It is reasonable to assume that Nature is not malicious.
In diQKD, however, we fight against a possible active adversary.

Reduce channel loss via a "fair-sampling device" (leaves only problem of detection efficiency)

N. Gisin, S. Pironio and N. Sangouard, Phys. Rev. Lett. 105, 070501 (2010); N. Sangouard et al., Phys. Rev. Lett. 106, 120403 (2011); M. Curty and T. Moroder, Phys. Rev. A 84, 010304(R) (2011).

SIDE-CHANNELS

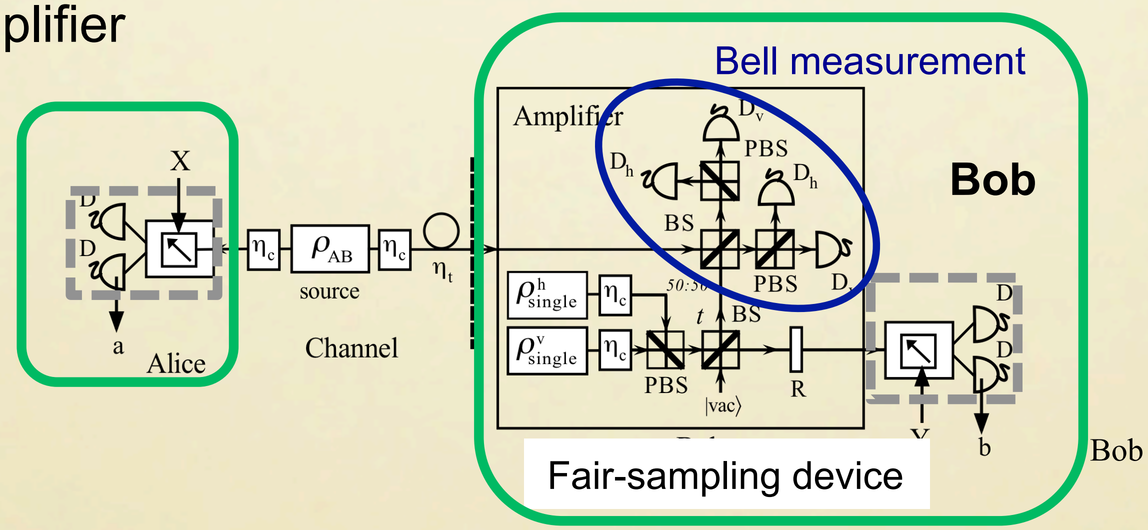
Fair-sampling device

In Bell tests $\longrightarrow$ assume that the set of detected photon pairs is a fair set (fair-sampling assumption). It is reasonable to assume that Nature is not malicious.
In diQKD, however, we fight against a possible active adversary.

Reduce channel loss via a "fair-sampling device" (leaves only problem of detection efficiency)

Heralded qubit amplifier

For simplicity, qubit amplifier only on Bob's side



A simpler quantum relay works as well even with SPDC sources!

N. Gisin, S. Pironio and N. Sangouard, Phys. Rev. Lett. 105, 070501 (2010); N. Sangouard et al., Phys. Rev. Lett. 106, 120403 (2011); M. Curty and T. Moroder, Phys. Rev. A 84, 010304(R) (2011).

Side-channels

What performance can we expect in practice?

SIDE-CHANNELS

What performance can we expect in practice?

Simulation with

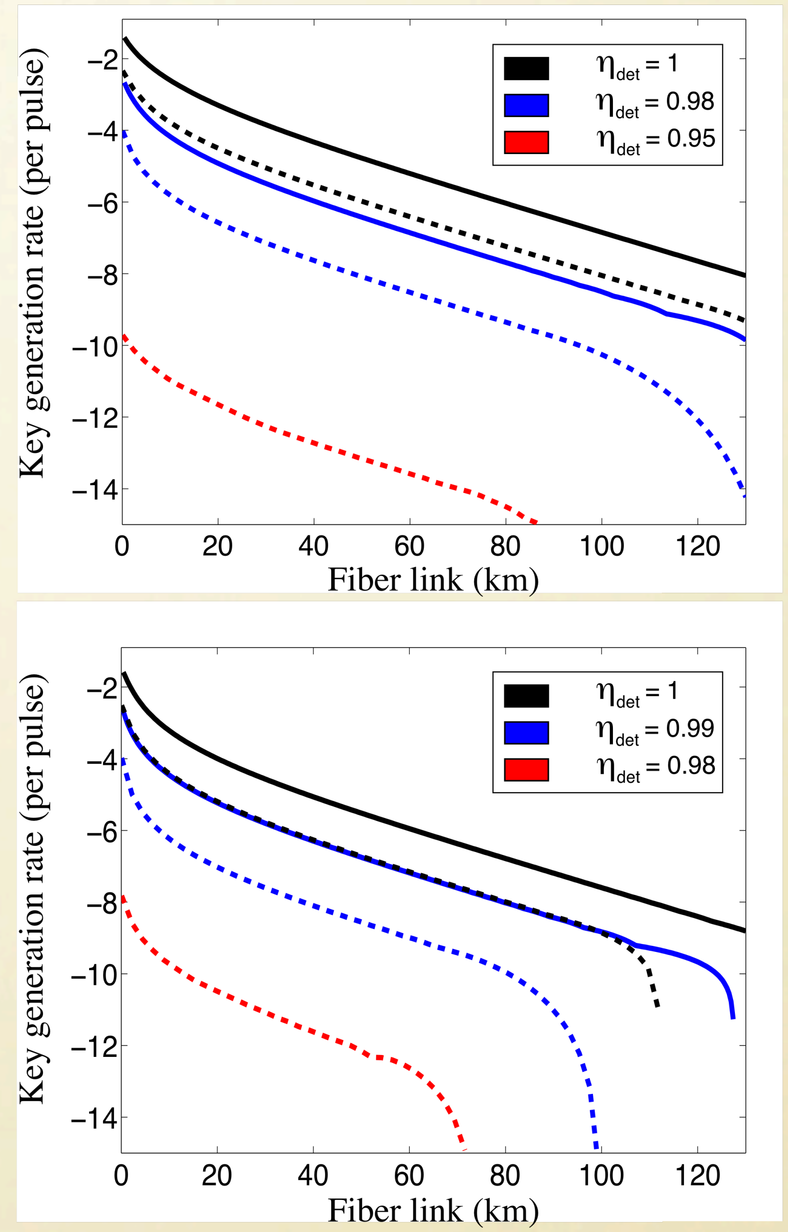
- Full-mode analysis [in contrast to perturbation approach]
- Detector, coupling efficiencies
- Optimization over variable parameters

Equipment:

* Standard PDC as entangled & heralded PDC as single photon sources

* Photon number resolving detectors

M. Curty and T. Moroder, Phys. Rev. A 84, 010304(R) (2011).
See also: D. Pitkänen et al., Phys. Rev. A 84, 022325 (2011).



"Original" qubit amplifier (dashed line) quantum relay (solid line). Upper figure shows a security analysis from Gisin et al. [PRL **105,** 070501 (2010)]. Lower figure shows the conservative situation of assigning inconclusive to conclusive results deterministically.

Limitations:

Requires near unity detection efficiency

An extremely low key rate (of order 10^{-8}-10^{-10} per pulse) at practical distances

di-QKD is a very beautiful idea but **impractical** with current technology => Need to improve entanglement sources, couplers and detectors!

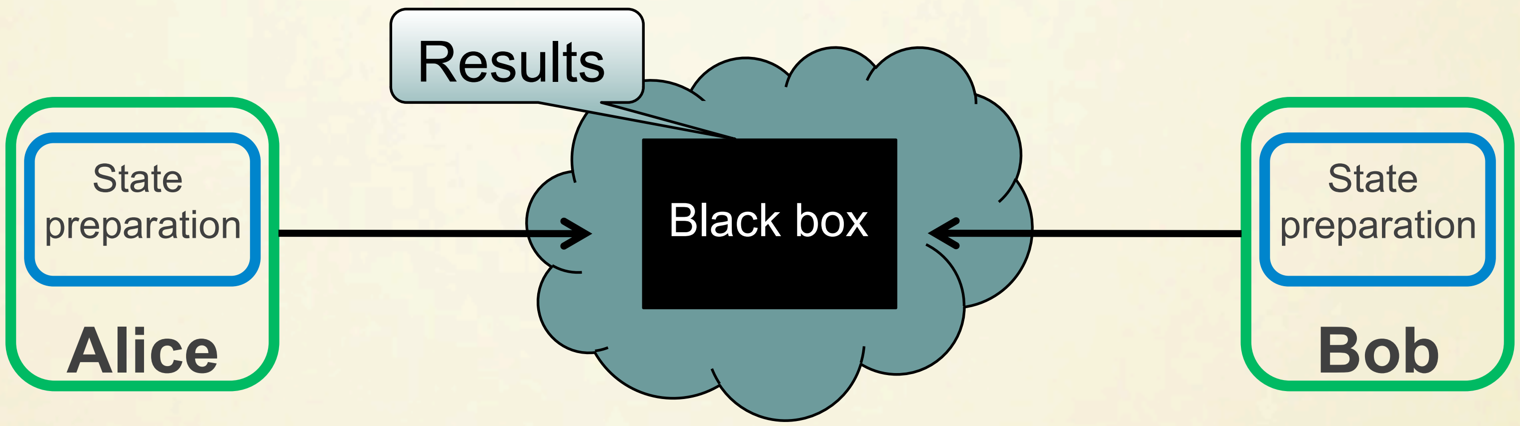
Side-channels

Rethink the problem: Most side channel attacks occur in the detectors

Side-channels

Rethink the problem: Most side channel attacks occur in the detectors

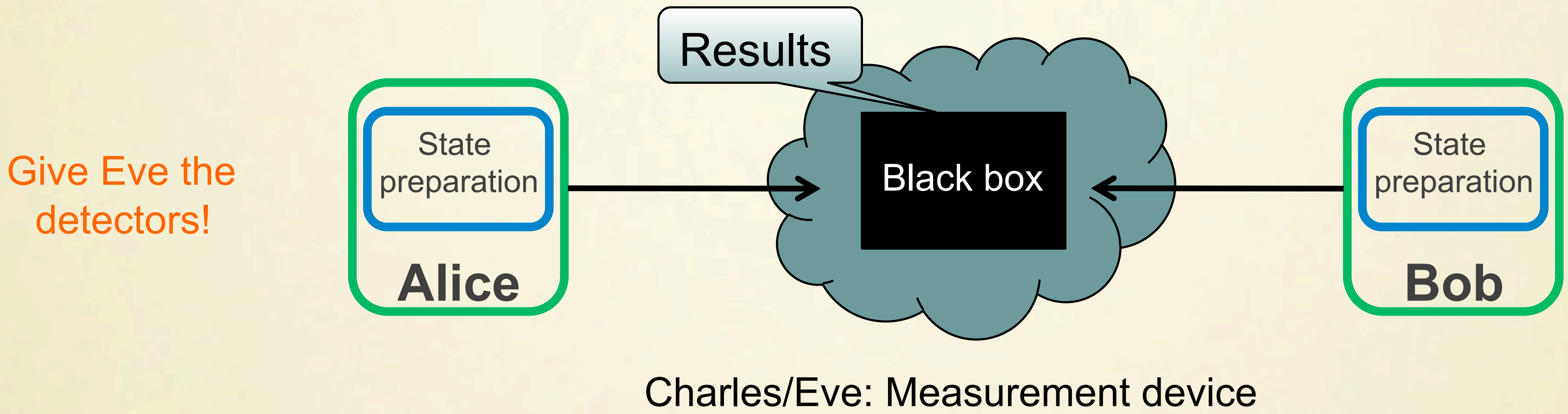
Give Eve the detectors!



Charles/Eve: Measurement device

Side-channels

Rethink the problem: Most side channel attacks occur in the detectors



Measurement-device independent QKD

A practical way to do QKD with "untrusted detectors"

Automatically immune to all detector side-channel attacks (existing and yet to be discovered)

No need to certify the measurement device (it can be even manufactured by a malicious eavesdropper, Eve). This is good news for QKD stardardisation and certification by European Telecommunications Standards Institute (ETSI)

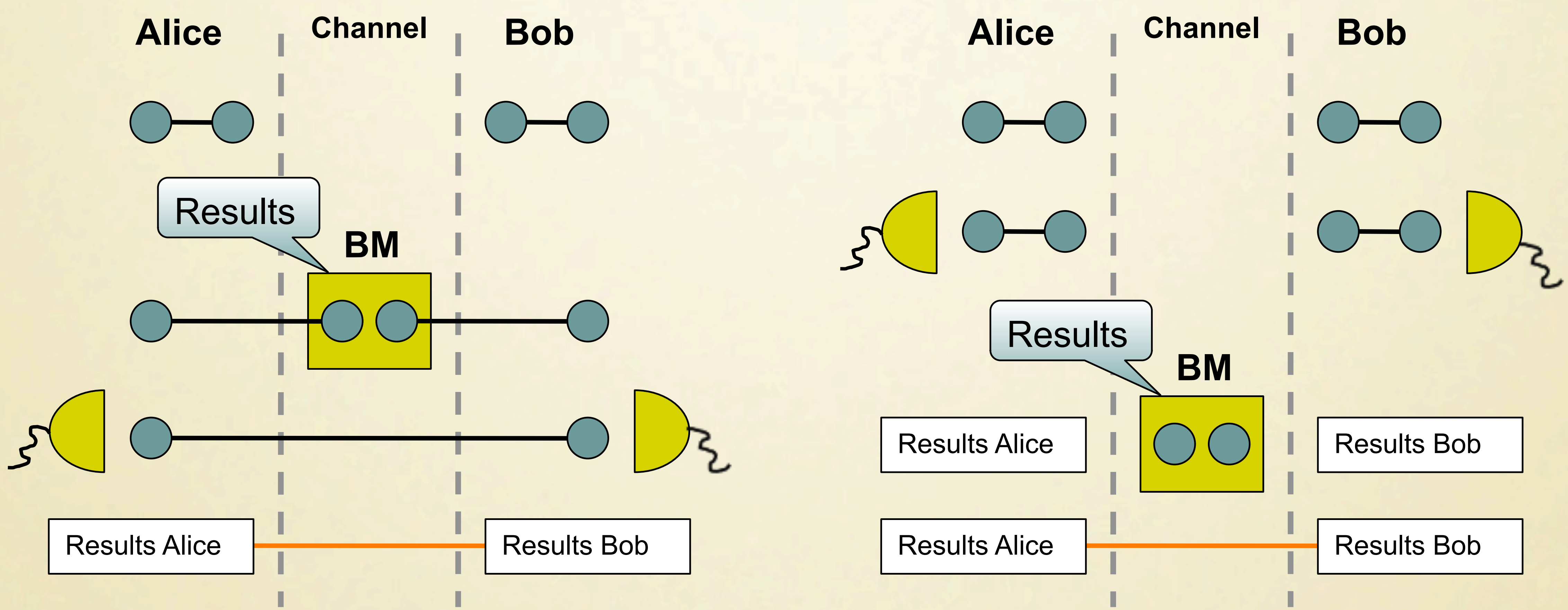
H.-K. Lo, M. Curty and B. Qi, Phys. Rev. Lett. 108, 130503 (2012); E. Biham, B. Huttner and T. Mor, Phys. Rev. A 54, 2651-2658 (1996); H. Inamori, Algorithmica 34, 340-365 (2002).

Side-channels

Intuition why it can be secure:

SIDE-CHANNELS

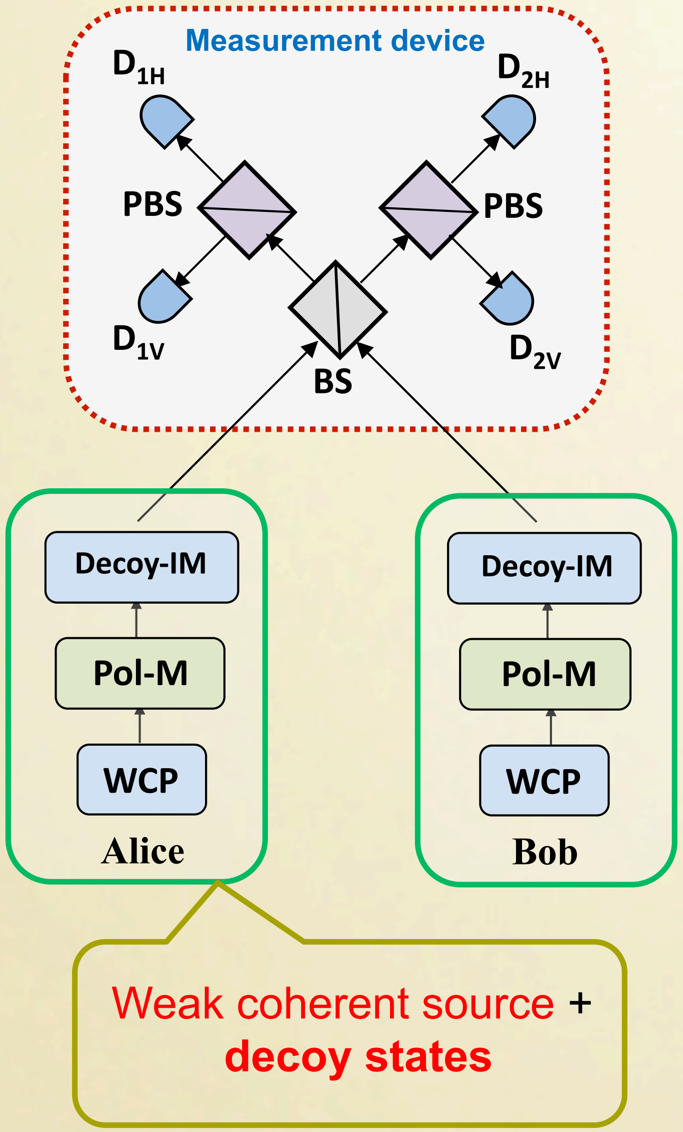
Intuition why it can be secure:



The result of the Bell measurement reveals correlations between Alice and Bob's bits but not the value of the individual bits

Side-channels

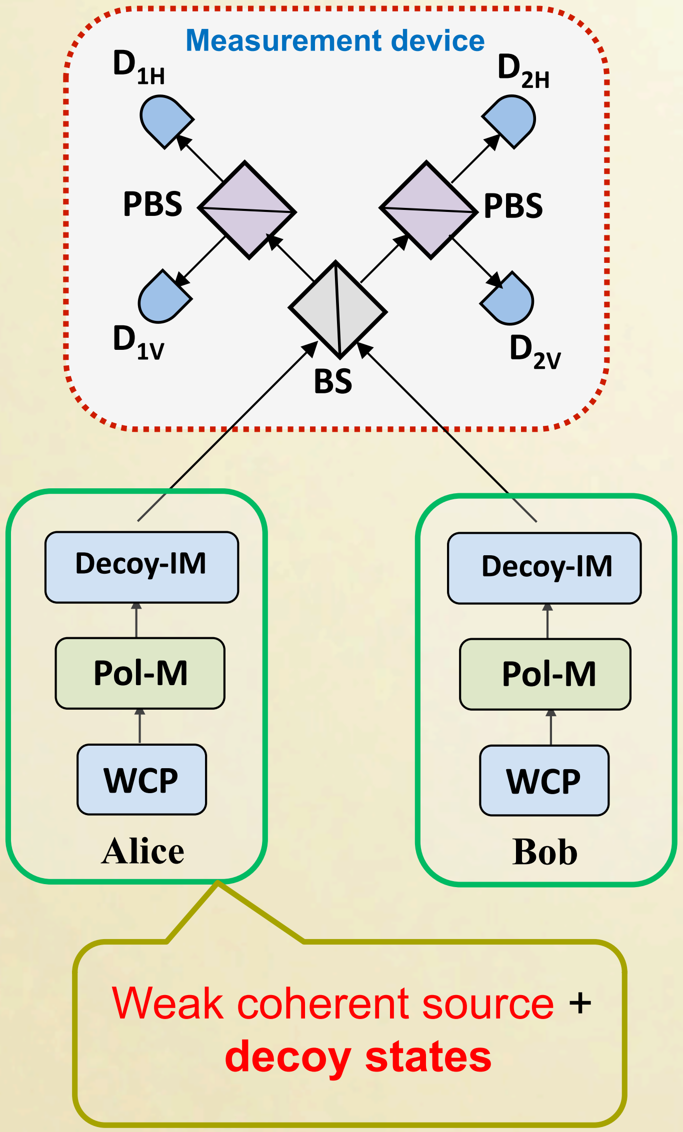
Measurement-device independent QKD



H.-K. Lo, M. Curty and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).

Side-channels

Measurement-device independent QKD



$$R \geq p_{1,1,\mathrm{Z}} Y_{1,1,\mathrm{Z}}[1 - h(e_{1,1,\mathrm{X}})] - Q_{\mathrm{Z}} h(E_{\mathrm{Z}})$$

Z basis for key generation
X basis for testing only

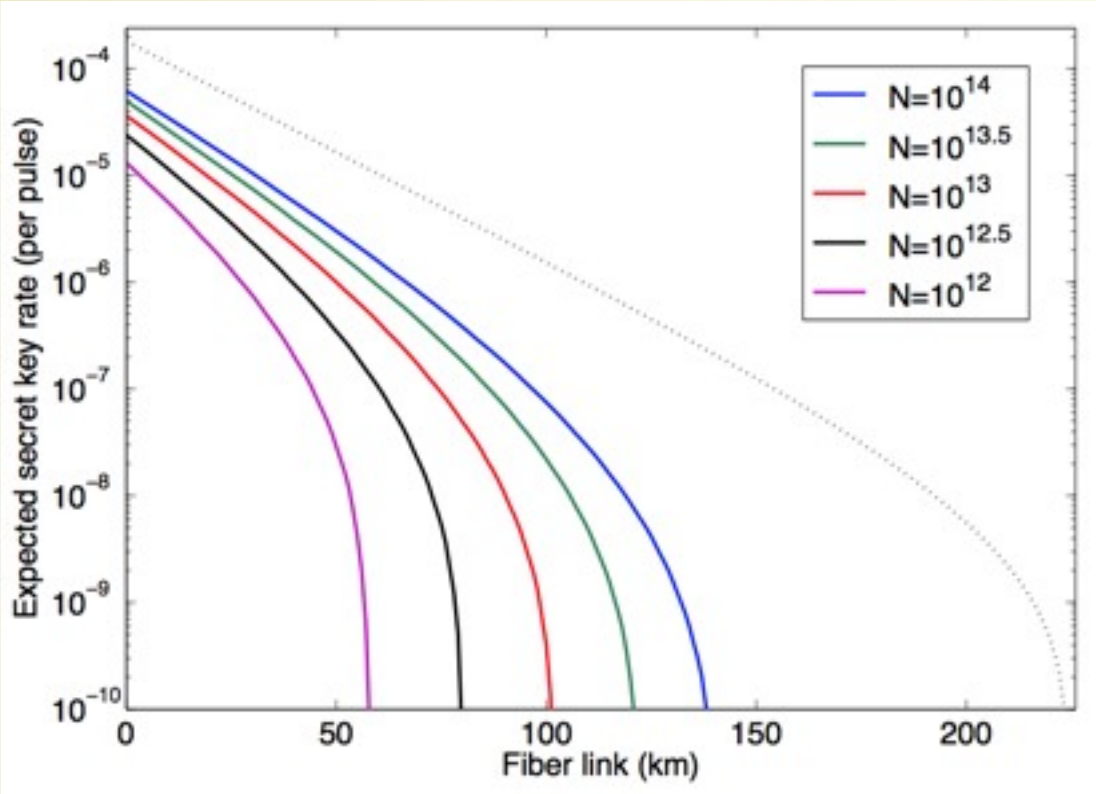
Q_{Z} and E_{Z} can be measured directly from the experiment.

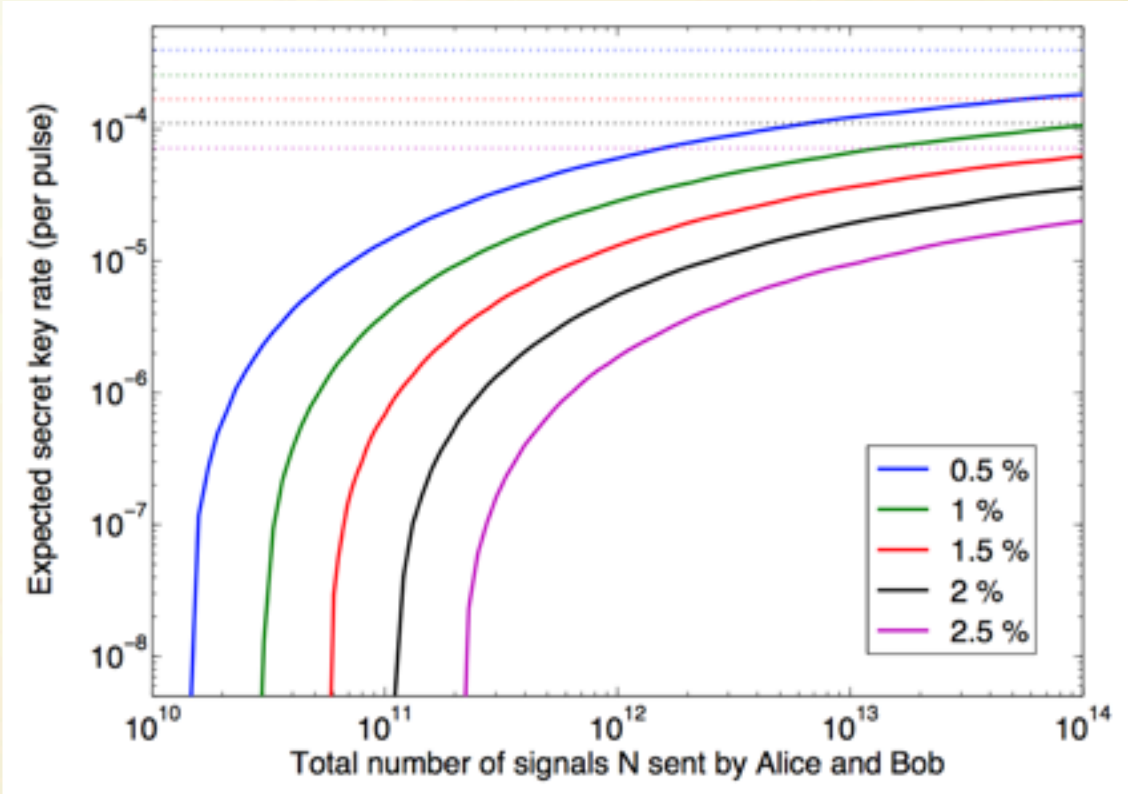
$Y_{1,1,\mathrm{Z}}$ and $e_{1,1,\mathrm{X}}$ are estimated using decoy states

H.-K. Lo, M. Curty and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).

SIDE-CHANNELS

Simulation results (finite-key case):





The experimental parameters are: $\alpha = 0.2$ dB/km, $\eta_{\mathrm{B}} = 14.5\%, Y_0 = 6.02 \times 10^{-6}$ and the security bound $\epsilon = 10^{-10}$. The misalignment in the first figure is 1.5%

If Alice and Bob use laser diodes at 1 GHz repetition rate, and each of them sends $N = 10^{13}$ signals, we find, for instance, that they can distribute a 1 Mb secret key over a 75 km fiber link in less than 3 hours.

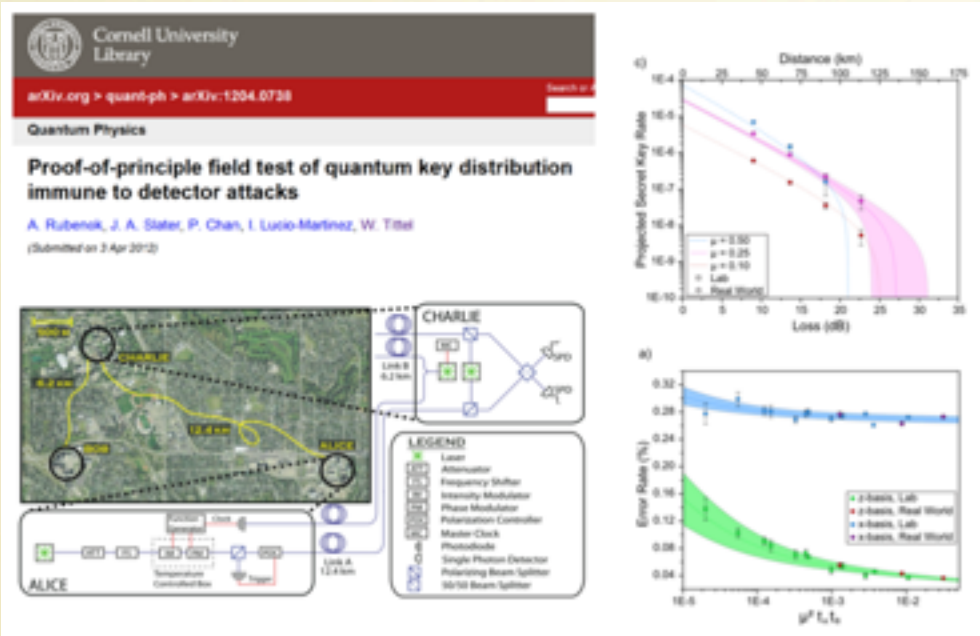
M. Curty at al., preprint arXiv:1307:1081.

Side-channels

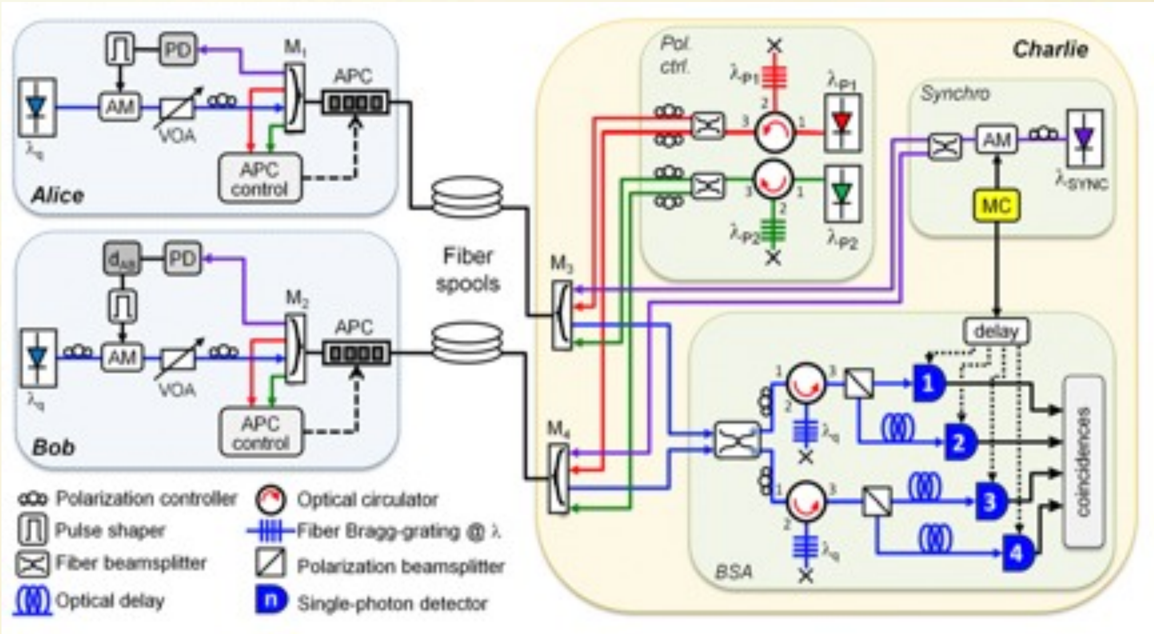
Let's return to the lab…

Side-channels

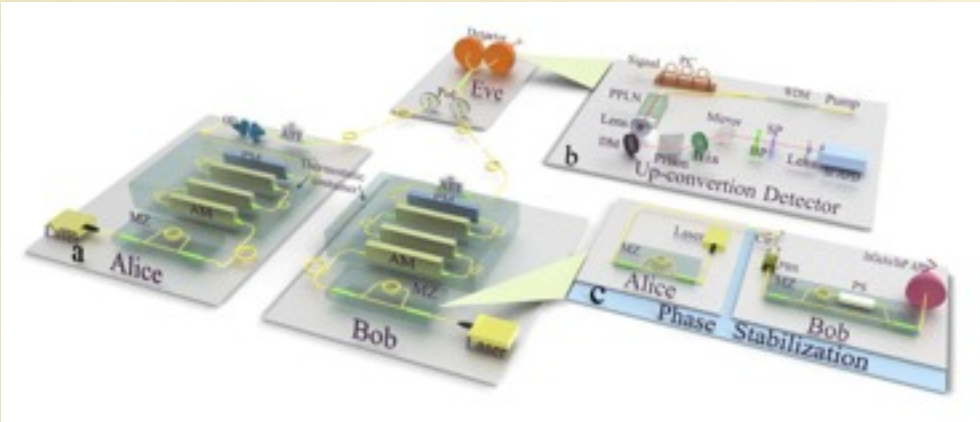
Let's return to the lab...



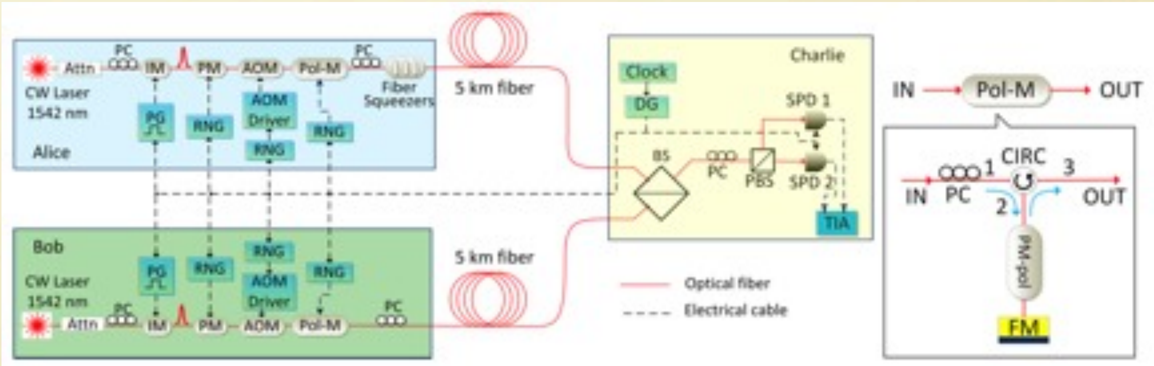
A. Rubenok et al., preprint arXiv:1204.0738



T. Ferreira da Silva et al., preprint arXiv:1207.6345



Y. Liu et al., preprint arXiv:1209.6178



Z. Tang et al., preprint arXiv:1306.6134

Thank you for your attention