Continuous-variables QKD with Preparation noise

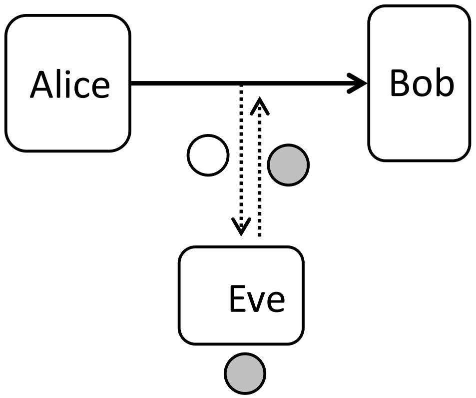
IN A WIRELESS SETTING

20 June 2024

Newcastle

Dr. Panagiotis Papanastasiou
School of Physics, Engineering, and Technology

No-cloning theorem in a copy-resend scenario



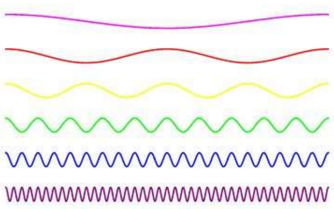
- Heisenberg's principle manifestation.
- Alice sends quantum states out of an non-orthogonal set to Bob (Quantum Superposition)
- Eve "duplicates" Alice's states and resends one of the perturbed copies.
- Quantum state copies cannot be created without perturbing the original state.
- Eve's presence can be discovered (with statistics)

W. K. Wootters and W. H. Zurek, Nature **299**, 802-803 (1982)
N. Gisin et al., Rev. Mod. Phys.**74**, 145 (2002)

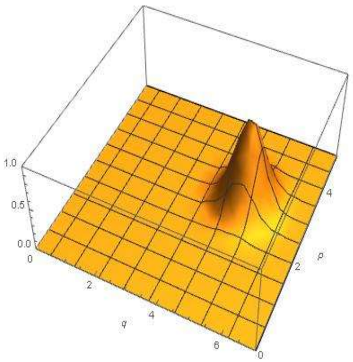
Quantum states of light

Bosonic system

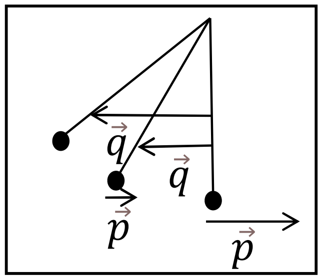
Mode of radiation field associated with a phase space, spanned by variables similar to position and momentum



Wigner function $W(q,p)$ of a mode in phase space



pendulum



Candidates for signal states:

- produced and transmitted efficiently with current technology (e.g. optical fibres).
- form non-orthogonal sets (e.g. coherent states)
- encode messages in the energy of the light field, as in an original (classical) setting for telecommunications
- described by continuous degrees of freedom (i.e. continuous variables, quadratures), in the phase space representation by a quasi-probability distribution (Wigner function).

S. L. Braunstein and P. V. Loock, Rev. Mod. Phys. **77**, 513 (2005)

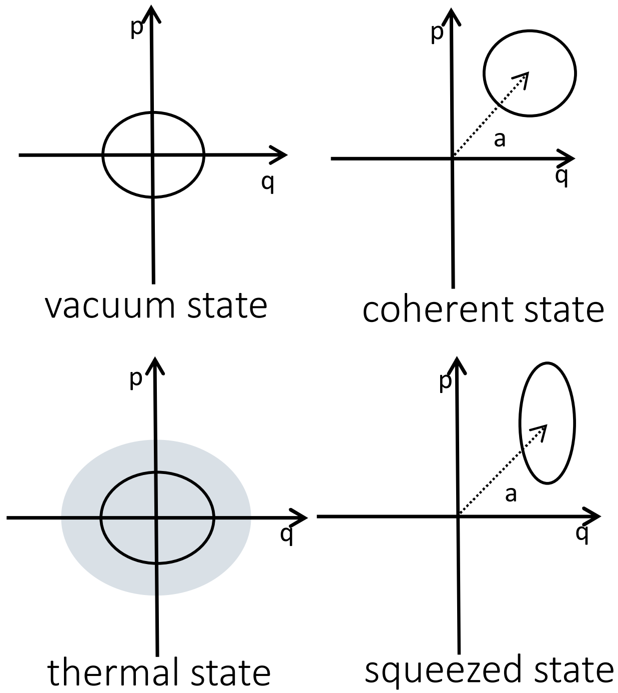
Gaussian states

- characterized by Gaussian Wigner $W(q,p)$ function
- described completely only by the first $\bar{x}$ and second moments $\boldsymbol{V}$ (covariance matrix)
- $\boldsymbol{V}$ is reduced to a diagonal form $\boldsymbol{V}^{\oplus}$ up to symplectic transformation $\boldsymbol{S}$ (Williamson's theorem).

$$\boldsymbol{V} = \mathbf{S}.\boldsymbol{V}^{\oplus}.\boldsymbol{S}^{T}$$

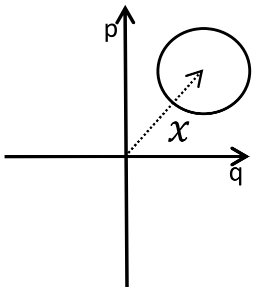
- simple calculation of von Neumann entropy via symplectic spectrum v_k of $\boldsymbol{V}$ for an M-mode state $\hat{\rho}$.

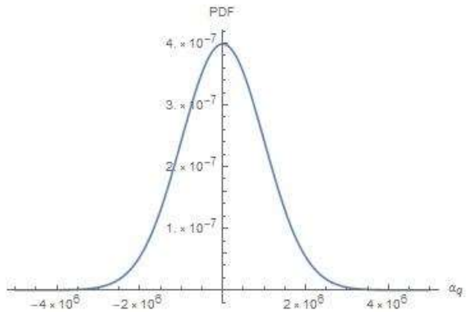
$$S(\hat{\rho}) = \sum_{i=1}^{M} h({v_k}^{\oplus})$$



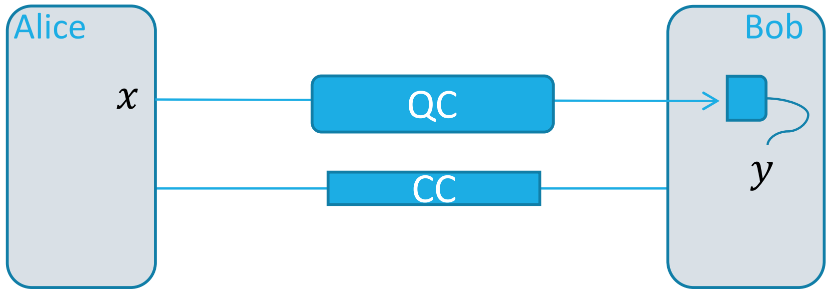
C. Weedbrook *et al.*, Rev. Mod. Phys. **84**, 621 (2012)

Gaussian modulation of coherent states





$\sigma_x^2 = \mu - 1$



- Alice modulates coherent states with a Gaussian distribution, i.e., adds random displacements
- Sends them to Bob through a quantum channel
- Bob is measuring with either a homodyne detection (plus shifting, q or p) or a heterodyne detection $(q$ and $p)$
- Error correction and Privacy amplification is taking place with respect to x or y with the use of the authenticated classical channel

F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002)
F. Grosshans, G. van Assche *et al.*, Nature (London) **421**, 238 (2003)
C. Weedbrook, A. M. Lance, W. P. Bowen *et al.*, Phys. Rev. Lett. **101**, 200504 (2008)

Secret key distribution

<u>One-time Pad key:</u>

- *random* string
- *shared* by the parties
- kept completely *secret*
- length of the message, never be reused (*performance constrains*, e.g., achievable distance)

<u>Quantum key distribution:</u>

Quant. comm.

- Alice: a random variable encoded into quantum states.
- Eavesdropper: controls quantum channel to Bob
- Bob: quantum measurements decoding
- Alice and Bob: error correction between encoding decoding outputs (classical communication)
- Alice and Bob: compare instances of encoded-decoded outputs (classical communication, channel parameter estimation)
- Alice and Bob: privacy amplification, compression to a smaller but secret random data sting. (classical post-processing)

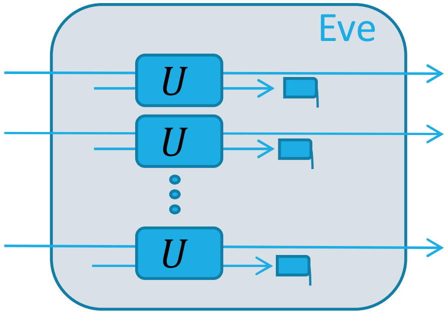
randomness

sharing

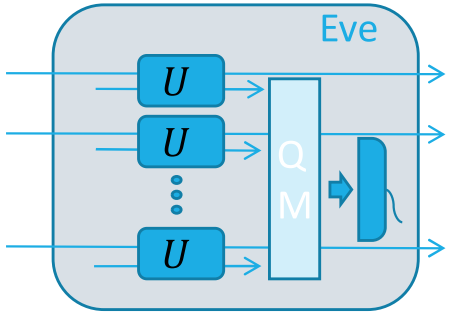
secrecy

Quantum Channel and Attacks

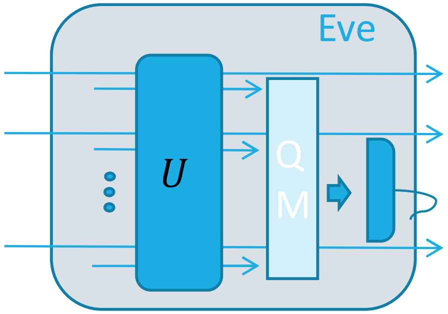
Individual Attack



Collective Attack



Coherent Attack

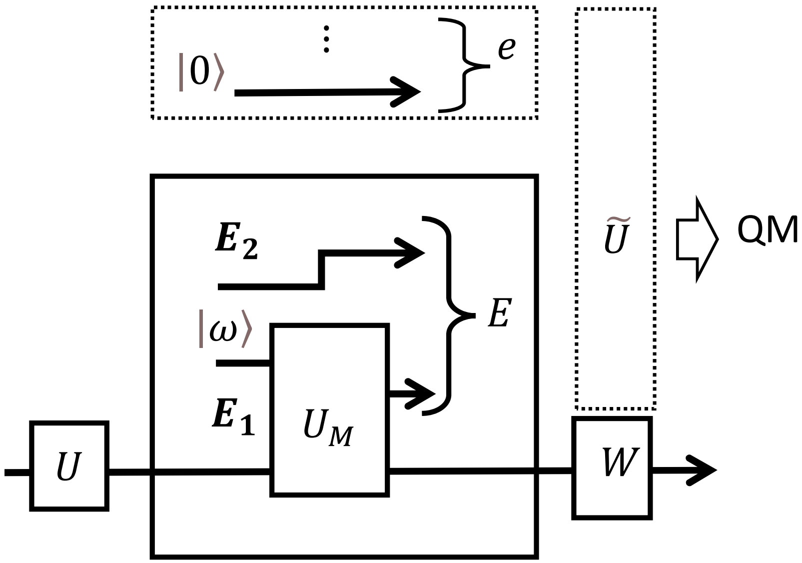


de Finetti like reduction

i.i.d. variables: $F_{X_1,\ldots,X_n}(x_1,\ldots,x_n) = F_{X_1}(x_1)\cdot\ldots\cdot F_{X_n}(x_n)$

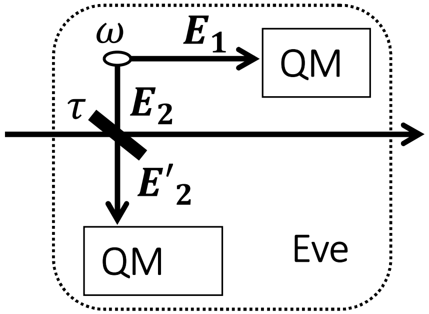
Dilation of Gaussian Attacks

Canonical Form C



Entangling Cloner

Attenuation $0 < \tau < 1$



Symplectic transformation

$$M[\tau] = \begin{pmatrix} \sqrt{\tau}\, I & \sqrt{1-\tau}\, I \\ -\sqrt{1-\tau} I & \sqrt{\tau}\, I \end{pmatrix}$$

- Realistic Attack: Simulates thermal loss channels (optical fibres)

$|\omega\rangle \equiv \text{TMSV} \quad \omega = 2\bar{n} + 1$

$$\boldsymbol{V} = \begin{pmatrix} \omega\, \boldsymbol{I} & \sqrt{\omega^2 - 1}\boldsymbol{Z} \\ \sqrt{\omega^2 - 1}\boldsymbol{Z} & \omega\, \boldsymbol{I} \end{pmatrix}$$

$$\boldsymbol{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \boldsymbol{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. 97, 190503(2006).
M. Navascues et al, Phys. Rev. Lett. 97, 190502 (2006)
S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. 101, 200504 (2008)

Asymptotic Secret key Rate

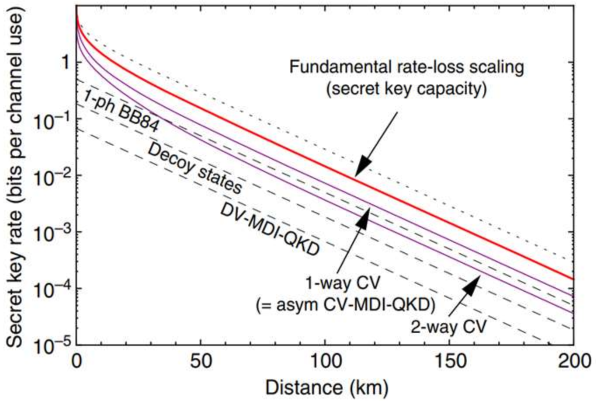
$$R_{\infty}(\mu, \tau, \omega) = \beta I(x: y) - \chi(E: \{x, y\})$$

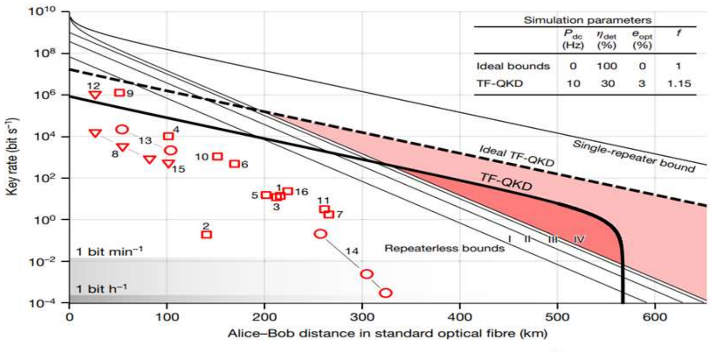
- Infinite uses of the channel
- $I(x: y) = H(x) - H(x|y)$ is the mutual information between the variables of the parties.
- $H(.)$ is the Shannon entropy
- β is the reconciliation parameter accounting for the efficiency of the error correction
- $\chi(E: \{x, y\}) = S(\hat{\rho}_E) - S\left(\hat{\rho}_{E|\{x,y\}}\right)$ is the Holevo information between Eve's system E and the variable $\{x, y\}$
- No-dependence on unitary transformations, Gaussian attacks minimize R

I. Devetak and A. Winter, Proc. R. Soc. A 461, 207 (2005).

F. Furrer, Ph.D., Leibnitz University, Hannover, 2012.

PLOB bound





- (Quantum) telecommunications bound
- Rates can be comparable to DV-QKD also in terms of achievable distance
- We can have end-to-end settings that can lead to QKD networks

❑ New protocols for aproaching the bound: Refine the strategy for communication and post-processing steps

❑ Detailed description including practical steps: decrease the performance to realistic levels

S. Pirandola, R. Laurenza, C. Ottaviani, L. Banchi, Nat. Commun **8**,15043 (2017)
M. Lucamarini, Z.L. Yuan, J.F. Dynes, *et al*., *Nature* **557**, 400–403 (2018).
Y. Zhang et al., Phys. Rev. Lett. **125**, 010502 (2020)
S. Pirandola et al., Nat. Photon. **9**, 397-402 (2015).
M. Ghalaii, P. Papanastasiou, and S. Pirandola, *npj Quantum Inf* **8**, 105 (2022)

Composable Framework Security

Secret key length:

$$s_n \leq n[H(l) - \chi(l:E)_\rho] - \text{leak}_{\text{ec}} - \sqrt{n}\Delta_{\text{aep}} + \theta.$$

$$\theta := \log_2(2\varepsilon_{\text{h}}^2 \varepsilon_{\text{cor}})$$

Finite size penalty:

$$\Delta_{\text{aep}} \simeq 4\log_2\left(\sqrt{|\mathcal{L}|}+2\right)\sqrt{\log_2(2/\varepsilon_{\text{s}}^2)}$$

Overall security:

$$\varepsilon = \varepsilon_{\text{cor}} + \varepsilon_{\text{s}} + \varepsilon_{\text{h}} + p_{\text{ec}} n_{\text{pm}} \varepsilon_{\text{pe}}$$

Reconciliation efficiency:

$$H(l) - n^{-1}\text{leak}_{\text{ec}} = \beta I(k:l)$$

Composable framework:

- Cryptographic primitives associated with parameter ε
- ϵ probability of failure of the primitive
- protocol consist of n primitives: $\varepsilon = \varepsilon_1 + \cdots + \varepsilon_n$
- Security proof: guaranties that $\varepsilon_i \ll 1$, i.e., $\varepsilon \ll 1$
- Required when the number of exchanged signals is limmited

S. Pirandola , P. Papanastasiou, arXiv:2301.10270v3

Smooth min-entropy

Classical Guessing probability: $$\sum_y \rho(y) \max_x \rho(x|y) = \exp\left(-H_{\min}(X|Y)_\rho\right)$$

Generalization to Quantum regime: $$H_{\min}(A|B)_\rho = \sup_{\sigma_B \in \mathcal{S}_\bullet(B)} \sup\left\{\lambda \in \mathbb{R} : \rho_{AB} \leq \exp(-\lambda) I_A \otimes \sigma_B\right\}$$

Smoothing (Uncertainty about the probability distribution): $$H_{\min}^{\varepsilon}(A|B)_\rho := \max_{\tilde{\rho}_{AB} \in \mathscr{B}^{\varepsilon}(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}}$$

M. Tomamichel, arXiv:1504.00233

Uniform Randomness Extraction

PA function

Leftover Hash Lemma: $$D(\bar{\rho}^n_{BEF}, \omega^n_B \otimes \rho_{E^n F}) \leq \varepsilon_{\mathrm{s}} + \frac{1}{2}\sqrt{2^{s_n - H^{\varepsilon_{\mathrm{s}}}_{\min}(B^n|E^n)_{\bar{\rho}^{\otimes n}}}}$$

State after PA

State before PA

Ideal state: uniform randomness, Bob is decoupled from Eve

- Skipped the EC step (analysis too complicated for this talk)
- Discretized variables
- Variables are n-length strings (finite-size)

S. Pirandola and P. Papanastasiou, arXiv:2301.10270

Uniform Randomness Extraction

Secrecy bound:

$$\varepsilon_{\mathrm{s}} + \frac{1}{2}\sqrt{2^{s_n - H_{\min}^{\varepsilon_{\mathrm{s}}}(B^n|E^n)_{\tilde{\rho}^{\otimes n}}}} \leq \varepsilon_{\mathrm{sec}}$$

Secret key length:

$$\begin{aligned} s_n &\leq H_{\min}^{\varepsilon_{\mathrm{s}}}(B^n|E^n)_{\tilde{\rho}^{\otimes n}} + 2\log_2(2\varepsilon_{\mathrm{h}}) \\ &\quad - \mathrm{leak}_{\mathrm{ec}} - \log_2(2/\varepsilon_{\mathrm{cor}}) \\ &= H_{\min}^{\varepsilon_{\mathrm{s}}}(B^n|E^n)_{\tilde{\rho}^{\otimes n}} + \log_2(2\varepsilon_{\mathrm{h}}^2\varepsilon_{\mathrm{cor}}) - \mathrm{leak}_{\mathrm{ec}} \end{aligned}$$

Leakage terms from EC and verification steps

Asymptotic Equipartition property

$$H_{\min}^{\varepsilon_s}(B^n|E^n)_{\tilde{\rho}^{\otimes n}} \geq nH(B|E)_{\tilde{\rho}} - \sqrt{n}\Delta_{\text{aep}}$$

Smooth Entropy

von Neumann Entropy

$$\Delta_{\text{aep}} \simeq 4\log_2\left(\sqrt{\aleph}+2\right)\sqrt{\log_2(2/\varepsilon_s^2)},$$

Discretisation: connection with the EC

Asymptotic rate with composable terms

$$s_n \leq nH(B|E)_\rho - \mathrm{leak}_{\mathrm{ec}} - \sqrt{n}\Delta_{\mathrm{aep}} + \log_2(2\varepsilon_{\mathrm{h}}^2\varepsilon_{\mathrm{cor}})$$

$$s_n \leq n[H(l) - \chi(l:E)_\rho] - \mathrm{leak}_{\mathrm{ec}} - \sqrt{n}\Delta_{\mathrm{aep}} + \log_2(2\varepsilon_{\mathrm{h}}^2\varepsilon_{\mathrm{cor}}).$$

- $\chi(l:E)_\rho \leq \chi(y:E)_\rho$
- $H(l) - n^{-1}\mathrm{leak}_{\mathrm{ec}} = \beta I(x:y)$

Strongly dependent on the reconciliation process: may differ for each run of the protocol

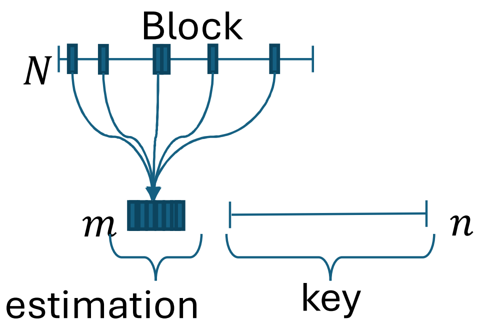
$$\boxed{s_n \leq nR_\infty - \sqrt{n}\Delta_{\mathrm{aep}} + \log_2(2\varepsilon_{\mathrm{h}}^2\varepsilon_{\mathrm{cor}}),}$$

Secret key rate: $R = \frac{p_{\mathrm{ec}} s_n}{N}$

Probability of successful EC (p_{ec})

Total number of signals (N)

Channel Parameter Estimation



output, signal and noise:

$$y = \sqrt{\eta T} x + z$$

Estimators:

$$\hat{C}_{xy} := \frac{1}{V_0 m} \sum_{i=1}^{V_0 m} [x]_i [y]_i$$

$$\widehat{T} = \frac{1}{\eta (\sigma_x^2)^2} \hat{C}_{xy}^2 = \frac{V_{\mathrm{Cov}}}{\eta (\sigma_x^2)^2} \left(\frac{\hat{C}_{xy}}{\sqrt{V_{\mathrm{Cov}}}} \right)^2$$

$$\widehat{\sigma}_z^2 = \frac{1}{V_0 m} \sum_{i=1}^{V_0 m} \left(y - \sqrt{\eta \widehat{T}} x \right)^2$$

Variances:

$$V_{\mathrm{Cov}} = \frac{1}{V_0 m} \sigma_x^2 \sigma_z^2$$

$$\frac{4T^2}{V_0 m} \left[c_{\mathrm{pe}} + \frac{\sigma_z^2}{\eta T \sigma_x^2} \right] := \sigma_T^2$$

$$V_z = \frac{2(\sigma_z^2)^2}{V_0 m}$$

Worst-case values:

$$T_{\mathrm{wc}} \simeq T - w \sigma_T$$

$$[\sigma_z^2]_{\mathrm{wc}} \simeq \sigma_z^2 + w \sqrt{V_z}$$

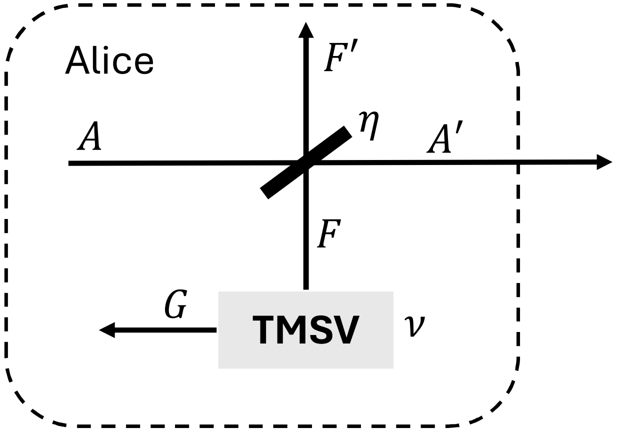
$$w = \sqrt{2} \mathrm{erf}^{-1} (1 - 2\varepsilon_{\mathrm{pe}})$$

Error in PE

PE Rate:

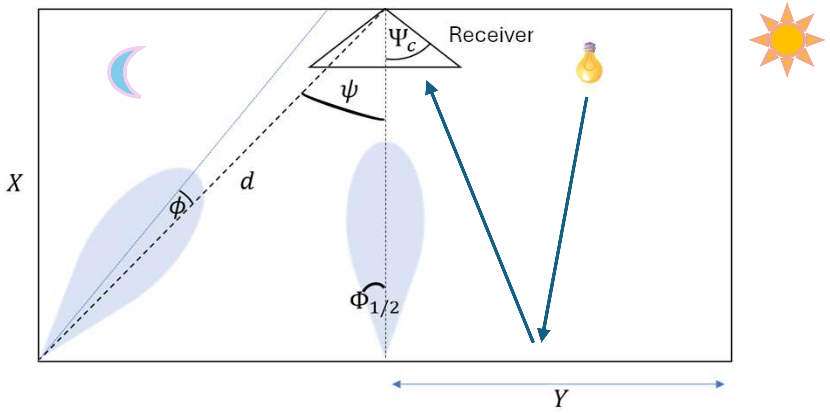
$$R_\infty^{\mathrm{pe}} = \beta [I]_{\hat{\mathbf{p}}} - [\chi_\rho]_{\mathbf{p}_{\mathrm{wc}}}$$

Preparation Noise Scheme



- Modelling imperfections due to cheap light sources
- ν preparation noise
- η preparation losses
- Noise and losses are trusted
- We assume a calibrated system (no PE for η and ν)

Indoors environment



- ϕ irradiance angle (receiver's normal)
- $\Phi_{1/2}$ beam's half-power semi-angle
- ψ incidence angle
- Ψ_c receiver's FOV
- d distance between receiver-transmitter
- X hight of the room
- Y room's dimension

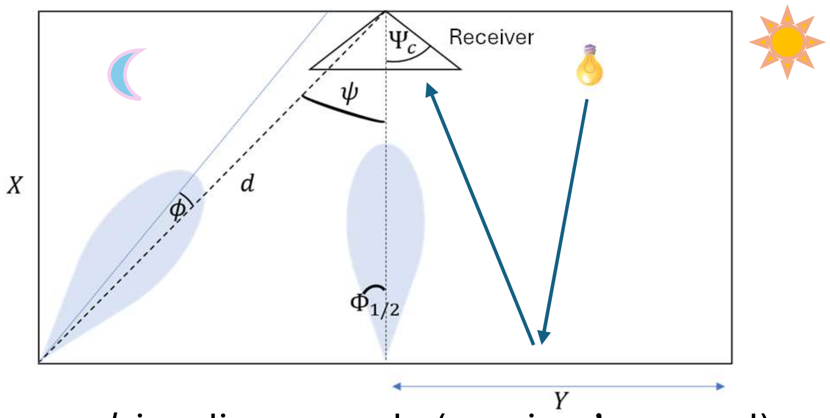
Ambient light:
- not dependent on FOV
- Isotropic
- Noise $\sim p_n$ (spectral irradiance)

Light from windows:
- Modelled in free-space studies
- windowless room assumption

Light from artificial sources:
- dependent on receiver's parameters
- noise from reflections

O. Elmabrok and M. Razavi, J. Opt. Soc. Am. B 35, 197-207 (2018)
O. Elmabrok, M. Ghalaii, and M. Razavi, J. Opt. Soc. Am. B 35, 487-499 (2018)

Indoors environment



- ϕ irradiance angle (receiver's normal)
- $\Phi_{1/2}$ beam's half-power semi-angle
- ψ incidence angle
- Ψ_c receiver's FOV
- d distance between receiver-transmitter
- X hight of the room
- Y room's dimension
- A receiver's area

$$H_{\mathrm{DC}} = \begin{cases} \frac{A(m+1)}{2\pi d^2} \cos(\phi)^m T_s(\psi) \times g(\psi) \cos(\psi) & 0 \le \psi \le \Psi_c \\ 0 & \text{elsewhere} \end{cases},$$

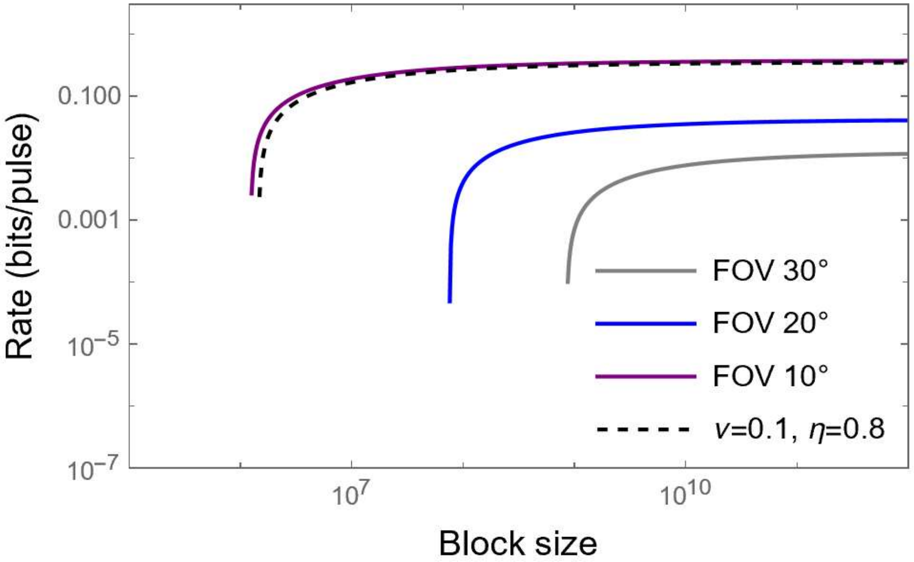
Directivity number: $$m = \frac{-\ln 2}{\ln(\cos(\Phi_{1/2}))}$$

Concentrator function: $$g(\psi) = \begin{cases} \frac{n^2}{\sin^2(\Psi_c)} & 0 \le \psi \le \Psi_c \\ 0 & \psi > \Psi_c \end{cases}.$$

O. Elmabrok and M. Razavi, J. Opt. Soc. Am. B 35, 197-207 (2018)
O. Elmabrok, M. Ghalaii, and M. Razavi, J. Opt. Soc. Am. B 35, 487-499 (2018)

Results:

Reverse reconciliation-Heterodyne detection



Parameters	Values
$\Phi_{1/2}$	1^o
d	$3\ m$
n	1.5
A	$0.1\ cm^2$
p_{ec}	0.95
β	0.98
u_{el}	$0.015\ SNU$
η_d	0.6
ε	$\sim 10^{-10}$
p_n	$10^{-9}\frac{w}{nm}/m^2$
λ	$880\ nm$
ξ_q^{rec}	0.002

Conclusion and Outlook

- Trade-off: higher repetition rates vs access to the receiver from any angle
- Trade-off: higher repetition rates vs quality-focus of the beam

Future work:

- Receiver's Area and repetition rate connection
- FOV and artificial light noise connection (geometry of the room)
- Mitigate the negative phenomena through post-selection techniques

Thank You !