$$\Sigma_{\mathrm{AB}} = \begin{pmatrix} (V+1)\mathbb{I} & \sqrt{T((V+1)^2-1)}\sigma_Z \\ \sqrt{T((V+1)^2-1)}\sigma_Z & (TV+1+\xi)\mathbb{I} \end{pmatrix} \equiv \begin{pmatrix} a\mathbb{I} & c\sigma_Z \\ c\sigma_Z & b\mathbb{I} \end{pmatrix} \tag{1}$$

Modeling noise of the homodyne measurement as (*independent, i.e. no off-diagonal terms)*:

$$b\mathbb{I} \mapsto (b+\sigma_N)\mathbb{I} = V_{\mathrm{B}}\mathbb{I}, \tag{2}$$

we obtain

$$\Sigma^{\mathrm{HOM}} = \begin{pmatrix} a\mathbb{I} & c\sigma_Z \\ c\sigma_Z & V_{\mathrm{B}}\mathbb{I} \end{pmatrix} \tag{3}$$

which ***does not destroy*** *the equivalency between prepare-and-measure and entanglement-based protocols, as it is just added noise.*

1 Homodyne detection

Consider the distributions on Alice's side:

$$\hat{q}_A = \hat{p}_A \sim G(0, V). \tag{4}$$

Bob's side:

$$\hat{q}_B \sim \sqrt{T}\hat{q}_A + \sqrt{1-T}\hat{q}_{\mathrm{vac}} + G(0, \sigma_N). \tag{5}$$

$$\mathrm{cov}(\hat{q}_A, \hat{q}_B) = \langle \hat{q}_A \hat{q}_B \rangle - \underbrace{\langle \hat{q}_A \rangle \langle \hat{q}_B \rangle}_{0} = \sqrt{T}\langle \hat{q}_A^2 \rangle + \sqrt{1-T}\underbrace{\langle \hat{q}_A \hat{q}_{\mathrm{vac}} \rangle}_{\langle \hat{q}_A \rangle \langle \hat{q}_{\mathrm{vac}} \rangle = 0} + \underbrace{\langle \hat{q}_A G(0, \sigma_N) \rangle}_{\langle \hat{q}_A \rangle \langle G(0,\sigma_N) \rangle = 0} = \sqrt{T}V, \tag{6}$$

so the covariance matrices *for measured quadrature* read

$$\Sigma^{\mathrm{HOM}}_{\hat{q},\hat{p}} = \begin{pmatrix} V & \sqrt{T}V \\ \sqrt{T}V & V_{\mathrm{B}} \end{pmatrix}, \tag{7}$$

and for both quadratures

$$\Sigma^{\mathrm{HOM}}_{\mathrm{AB}} = \begin{pmatrix} V\mathbb{I} & \sqrt{T}V\mathbb{I} \\ \sqrt{T}V\mathbb{I} & V_{\mathrm{B}}\mathbb{I} \end{pmatrix}, \tag{8}$$

which is the covariance matrix of a prepare and-measure protocol.

Using formulae for mutual information in the form [1] (*reduced to the case* $n = m = 1$) yields

$$I^{\mathrm{HOM}}_{\mathrm{AB}} = \frac{1}{2}\log\frac{VV_{\mathrm{B}}}{\det \Sigma_{\hat{q},\hat{p}}} = \frac{1}{2}\log\frac{TV+\sigma_x+\xi}{\sigma_x+\xi}. \tag{9}$$

1.1 Equivalence between prepare-and-measure and entanglement-based protocols

It seems that the equivalence between PM and EB is somewhat lost when calculating mutual information. Consider using elements of Σ_{AB}:

$$I^{\mathrm{EB}} = \frac{1}{2}\log\frac{TV + \xi + \sigma_x}{TV - \frac{TV}{V+1} + \xi + \sigma_x} \neq I. \tag{10}$$

Covariance matrices of PM and EB are connected by a scaling factor $\kappa = \pm\sqrt{2\frac{V}{V+2}}$ (see Eq.(46) in Ref. [2]), *as the form of the elements is not important, they are replaced by first* 3 *letters of greek alphabet*:

$$\Sigma^{\mathrm{PM}} \mapsto \Sigma^{\mathrm{EB}} = \begin{pmatrix} \frac{1}{\kappa^2}\alpha\mathbb{I} & \frac{1}{\kappa}\gamma\sigma_Z \\ \frac{1}{\kappa}\gamma\sigma_Z & \beta\mathbb{I} \end{pmatrix}, \tag{11}$$

$$I^{\mathrm{EB}} = \frac{1}{2}\log\frac{\frac{1}{\kappa^2}\alpha\beta}{\frac{1}{\kappa^2}\left(\alpha\beta - \gamma\right)} = \frac{1}{2}\log\frac{\alpha\beta}{\left(\alpha\beta - \gamma\right)} = I, \tag{12}$$

where I is the same as in Eq. (9). However, $\Sigma^{\mathrm{EB}} \neq \Sigma_{\mathrm{AB}}$ (Eq.(39) and (41)). Σ^{EB} is the covariance matrix that describes the substate between Alice and Bob *after the beamsplitter* that splits her EPR pair to send one half to Bob.

The symplectic eigenvalues of Σ^{EB} are obviously different from those of Σ_{AB}, as they are related as follows

$$a \mapsto \frac{a+1}{2} \tag{13}$$

$$c \mapsto \frac{c}{\sqrt{2}} \tag{14}$$

However, security analysis (purification attack) assumes that Eve holds a purification to the TMSVS shared by Alice and Bob. Experimentally, they would need to rescale their results. Theoretically, Holevo information is estimated from TMSVS's covariance matrix:

$$\Sigma_{\mathrm{AB}}^{\mathrm{TVMS}} = \begin{pmatrix} (V+1)\mathbb{I} & \sqrt{T((V+1)^2-1)}\sigma_Z \\ \sqrt{T((V+1)^2-1)}\sigma_Z & (TV + \xi + \sigma_x)\mathbb{I} \end{pmatrix} \tag{15}$$

As in, current Holevo information in the article is correct.

2 Double homodyne

Measurement noise must be modeled last, as it is not splitted by signal BS. Consider

$$\Sigma_{\mathrm{AB}} = \begin{pmatrix} V\mathbb{I} & \sqrt{T}V\mathbb{I} \\ \sqrt{T}V\mathbb{I} & \left(TV + 1 + \xi\right)\mathbb{I} \end{pmatrix} \equiv \begin{pmatrix} V\mathbb{I} & c\mathbb{I} \\ c\mathbb{I} & b\mathbb{I} \end{pmatrix}, \tag{16}$$

Bob's mode is splitted on BS_S, i.e.

$$\tilde{\Sigma}_{\mathrm{AB}}^{\mathrm{DHOM}} = \mathrm{BS}\left[\Sigma_{\mathrm{AB}} \oplus \Sigma_{\mathrm{vac}}\right]\mathrm{BS}^{\mathrm{T}} = \begin{pmatrix} V\mathbb{I} & C_S c\mathbb{I} & -S_S c\mathbb{I} \\ C_S c\mathbb{I} & (C_S^2 b + S_S^2)\mathbb{I} & C_S S_S(1-b)\mathbb{I} \\ -S_S c\mathbb{I} & C_S S_S(1-b)\mathbb{I} & (C_S^2 + S_S^2 b)\mathbb{I} \end{pmatrix}, \tag{17}$$

where $\Sigma_{\mathrm{vac}} = \mathbb{I}$ and $\mathrm{BS} = \mathbb{I} \oplus \begin{pmatrix} C_S\mathbb{I} & S_S\mathbb{I} \\ -S_S\mathbb{I} & C_S\mathbb{I} \end{pmatrix}$. Finally, we will model the measurement noise as

$$\Sigma_{\mathrm{AB}}^{\mathrm{DHOM}} = \tilde{\Sigma}_{\mathrm{AB}}^{\mathrm{DHOM}} + N, \tag{18}$$

where

$$N = 0\mathbb{I} \oplus \begin{pmatrix} \sigma_N^{(1)} I & 0\mathbb{I} \\ 0\mathbb{I} & \sigma_N^{(2)}\mathbb{I} \end{pmatrix} = 0\mathbb{I} \oplus \begin{pmatrix} \left[\frac{\sigma_1}{2} - \frac{1}{2}\right]\mathbb{I} & 0\mathbb{I} \\ 0\mathbb{I} & \left[\frac{\sigma_2}{2} - \frac{1}{2}\right]\mathbb{I} \end{pmatrix} \tag{19}$$

which is evident from Eq. (20):

$$\mathsf{P}_G(x_1, x_2) = \frac{1}{2\pi\sqrt{\sigma_G^{(1)}\sigma_G^{(2)}}} \exp\left\{-\frac{(x_1 - \mathrm{Re}\,\alpha e^{-i\varphi})^2}{\sigma_1} - \frac{(x_2 - \mathrm{Im}\,\alpha e^{-i\varphi})^2}{\sigma_2}\right\}. \tag{20}$$

$$\Sigma + N = \begin{pmatrix} V\mathbb{I} & C_S c\mathbb{I} & -S_S c\mathbb{I} \\ C_S c\mathbb{I} & (C_S^2 b + S_S^2 + \frac{\sigma_1 - 1}{2})\mathbb{I} & C_S S_S(1-b)\mathbb{I} \\ -S_S c\mathbb{I} & C_S S_S(1-b)\mathbb{I} & (C_S^2 + S_S^2 b + \frac{\sigma_2 - 1}{2})\mathbb{I} \end{pmatrix} \tag{21}$$

Analogously to Eq. (9), to calculate mutual information, we will consider the covariance matrix of one quadrature:

$$\Sigma_{\hat{q},\hat{p}}^{\mathrm{DH}} = \begin{pmatrix} V & C_S c & -S_S c \\ C_S c & C_S^2 b + S_S^2 + \frac{\sigma_1 - 1}{2} & C_S S_S(1-b) \\ -S_S c & C_S S_S(1-b) & (C_S^2 + S_S^2 b + \frac{\sigma_2 - 1}{2}) \end{pmatrix} = \tag{22}$$

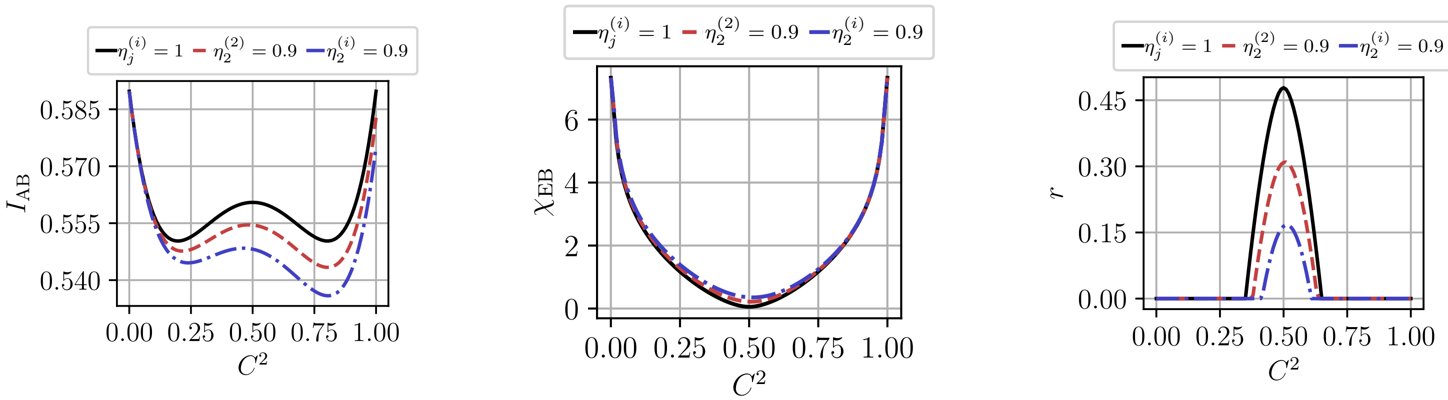
$$\equiv \begin{pmatrix} V & \gamma_1 & \gamma_2 \\ \gamma_1 & \beta_1 & \gamma_{12} \\ \gamma_2 & \gamma_{12} & \beta_2 \end{pmatrix}, \tag{23}$$

so mutual information between Alice and Bob reads

$$I = \frac{1}{2}\sum_i \log\frac{V\beta_i}{\det\Sigma_i}, \qquad \Sigma_i = \begin{pmatrix} V & \gamma_i \\ \gamma_i & \beta_i \end{pmatrix}, \tag{24}$$

simplifying det for article-worthy formulae:

$$I = \frac{1}{2}\sum_i \log\frac{V\beta_i}{V\beta_i - \gamma_i^2} \tag{25}$$



(a) I_{AB}

(b) χ_{EB}

(c) R

Figure 1: (a) Mutual information (b) Holevo information and (c) asymptotic secret fraction using double homodyne measurement as functions of signal beam splitter transmission with all other beamsplitter taken to be balanced for various detector efficiencies (unspecified in legend efficiencies are taken to be unity) at $V = 1, T = 0.95, \xi = 10^{-3}, \beta = 0.95$.

$$\frac{V\beta_1}{\det \Sigma_1} = \frac{C_S^2 b + S_S^2 + \frac{\sigma_1 - 1}{2}}{C_S^2 \xi + 1 + \frac{\sigma_1 - 1}{2}}, \tag{26}$$

$$\frac{V\beta_2}{\det \Sigma_2} = \frac{S_S^2 b + C_S^2 + \frac{\sigma_2 - 1}{2}}{S_S^2 \xi + 1 + \frac{\sigma_2 - 1}{2}}, \tag{27}$$

further prettifying:

$$I = \frac{1}{2} \sum_i \log \frac{TV_i + \xi_i + \sigma_i + 1}{\xi_i + \sigma_i + 1}, \tag{28}$$

$$V_1 = 2C_S^2 V, \quad \xi_1 = 2C_S^2 \xi \tag{29}$$

$$V_2 = 2S_S^2 V, \quad \xi_2 = 2S_S^2 \xi \tag{30}$$

Calculating @ symmetrical case yields:

$$I = \log \frac{TV + \xi + 2}{\xi + 2} = \log \frac{\frac{TV}{2} + \frac{\xi}{2} + 1}{1 + \frac{\xi}{2}} \tag{31}$$

which coincides with known results (Eq.(50) in Ref. [2]). Consideration of N (19) with squeezed states is still required.

3 SNR

In the GG02 protocol, Alice prepares an ensemble of coherent states whose amplitudes α are drawn from a zero-mean Gaussian distribution, denoted by $G_\alpha(0; V_{\mathrm{mod}})$, where V_{mod} is

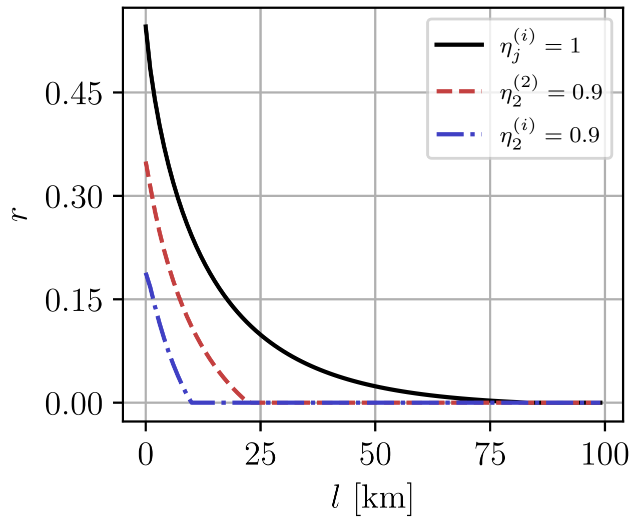


Figure 2: The asymptotic secret fraction as a function channel length computed for double homodyne detection for various detector efficiencies at $V = 1, T = 0.95, \xi = 10^{-3}, \beta = 0.95$, losses are taken as 20 dB @ 100 km.

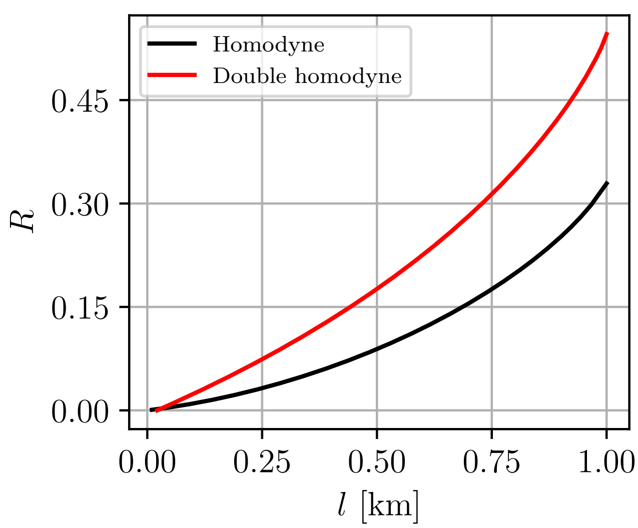


Figure 3: Comparison between performances of ideal homodyne and double homodyne at $V = 1, \xi = 10^{-3}, \beta = 0.95$, losses are taken as 20 dB @ 100 km. The advantage of using double homodyne rather that homodyne is not that big.

the modulation variance. The density matrix reads

$$\rho = \int \mathrm{d}^2\alpha \, G_\alpha(0; V_{\mathrm{mod}}) \, |\alpha\rangle \langle\alpha| \, . \tag{32}$$

After transmission through a Gaussian channel, which attenuates the coherent amplitude by a factor of $\sqrt{T}$, where T is the channel transmission, the state transforms as $|\alpha\rangle \mapsto \left|\sqrt{T}\alpha\right\rangle \equiv |\tilde{\alpha}\rangle$. The quadratures are then measured by Bob. The resulting quadrature distribution is:

$$\begin{aligned} p_{\mathrm{B}} = \mathrm{Tr}\, \rho \hat{\Pi} = \int \mathrm{d}^2\alpha \, G_\alpha(0; V_{\mathrm{mod}}) \, \langle\tilde{\alpha}| \, \hat{\Pi} \, |\tilde{\alpha}\rangle = \\ \frac{1}{T} \int \mathrm{d}^2\tilde{\alpha} \, G_{\tilde{\alpha}}(0; T V_{\mathrm{mod}}) Q_\Pi(\tilde{\alpha}), \end{aligned} \tag{33}$$

where $\hat{\Pi}$ is the POVM describing the measurements, and $Q_\Pi(\alpha)$ is its' corresponding Q-function. Note that the variance $G_{\tilde{\alpha}}$ is TV_{mod}.

Assuming that Bob performs homodyne detection, the variance of the distribution p_{B} in Eq. (33) is given by

$$V_{\mathrm{B}}^{\mathrm{HOM}} = TV + 1 + \sigma_N = TV + \sigma_x, \tag{34}$$

where we used the relation $2\hat{a} = \hat{q} + i\hat{p}$, which implies $4V(\hat{a}) \equiv 4V_{\mathrm{mod}} = V(\hat{q}) = V(\hat{p}) \equiv V$, and integrated Eq. (33) by $\mathrm{d}^2\alpha = \frac{1}{2}\mathrm{d}q \; \mathrm{d}p$. Analogously, adding any stochastic noise (e.g., channel excess noise) with variance ξ modifies the total variance $V_{\mathrm{B}}^{\mathrm{HOM}}$ as

$$V_{\mathrm{B}}^{\mathrm{HOM}} = TV_{\mathrm{mod}} + \sigma_x + \xi. \tag{35}$$

From this, the signal-to-noise ratio (SNR) and the mutual information between Alice and Bob are given by

$$\mathrm{SNR}^{\mathrm{HOM}} = \frac{TV_{\mathrm{mod}}}{\sigma_x + \xi}, \tag{36}$$

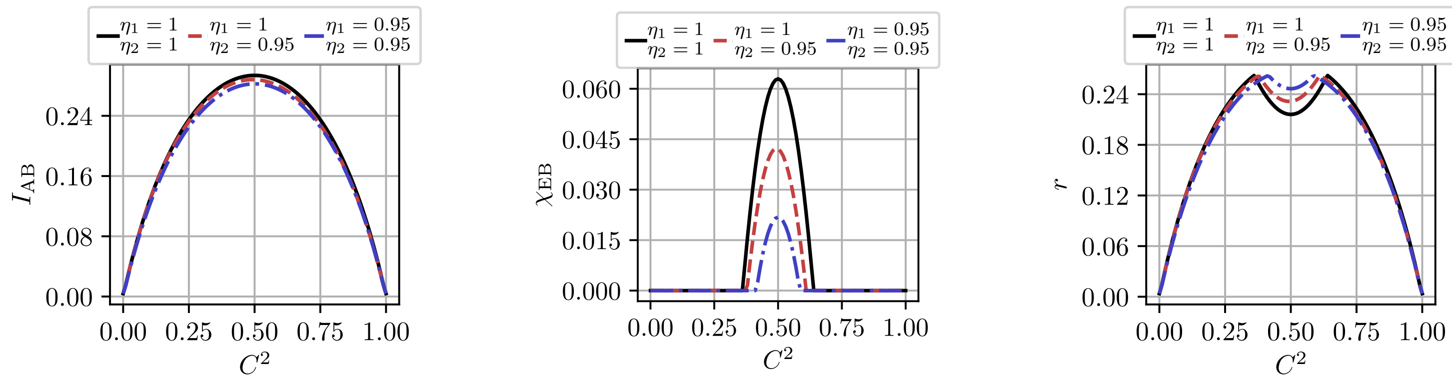
$$I_{\mathrm{AB}}^{\mathrm{HOM}} = \frac{1}{2} \log \left[1 + \mathrm{SNR}^{\mathrm{HOM}}\right] \tag{37}$$

This method, however, won't hold for calculating mutual information if Bob is using double homodyne detection.

4 Trusted noise

Holevo information for homodyne is calculated from

$$\begin{aligned} \nu_{1,2} &= \frac{1}{2} \left(z \pm [V_{\mathrm{B}} - \sigma_N - a] \right), \\ z &= \sqrt{\left(a + (b - \sigma_N)\right)^2 - 4c^2}, \end{aligned} \tag{38}$$



(a) I_{AB} (b) χ_{EB} (c) R

Figure 4: (a) Mutual information, (b) Holevo information, and (c) asymptotic secret fraction using homodyne measurements (**trusted noise**) as functions of the beam splitter transmission, for various detector efficiencies at $V = 1, T = 0.8, \xi = 10^{-3}, \beta = 0.95$

and in case of homodyne detection:

$$\nu_3 = \sqrt{a\left(a - \frac{c^2}{V_{\mathrm{B}}^{\mathrm{HOM}}}\right)} = \sqrt{V\left(V - \frac{T(V^2-1)}{V_{\mathrm{B}}^{\mathrm{HOM}}}\right)}, \tag{39}$$

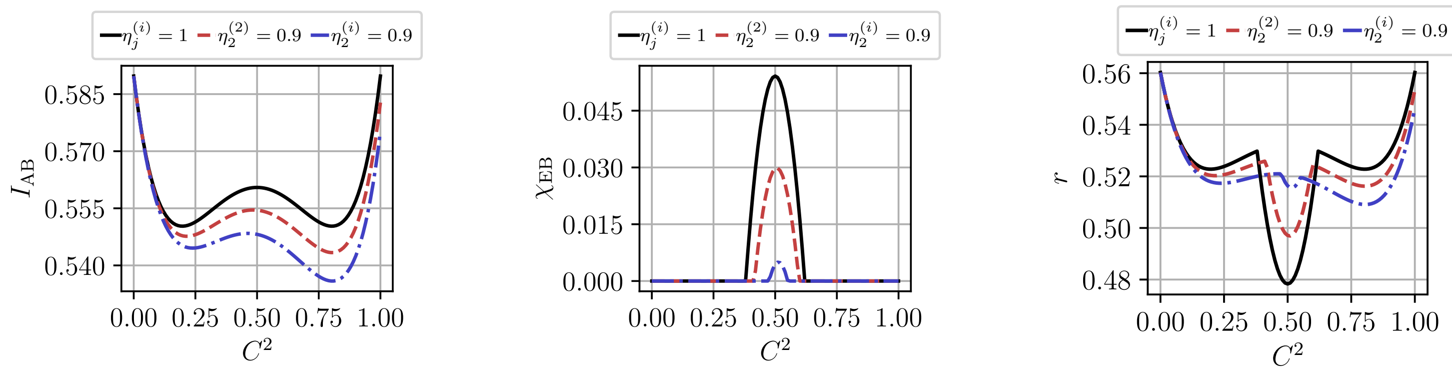
and double homodyne:

$$\nu_3 = a - \frac{c^2}{V_{\mathrm{B}} + 1 + \sigma_N}. \tag{40}$$

References

[1] Joram Soch et al. *StatProofBook/StatProofBook.github.io: The Book of Statistical Proofs (Version 2023)*. `https://doi.org/10.5281/zenodo.4305949`. Accessed: 2025-07-15. 2024.

[2] Fabian Laudenbach et al. "Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations". In: *Advanced Quantum Technologies* 1.1 (2018), p. 1800011.



(a) I_{AB} (b) χ_{EB} (c) R

Figure 5: (a) Mutual information, (b) Holevo information, and (c) asymptotic secret fraction using double homodyne detection as functions of the signal beam splitter transmission **(trusted noise)**. All other beam splitters are assumed to be balanced. Results are shown for various detector efficiencies; efficiencies not specified in the legend are taken to be unity. Parameters: $V_{\mathrm{mod}} = 1, T = 0.8, \xi = 10^{-3}, \beta = 0.95$.

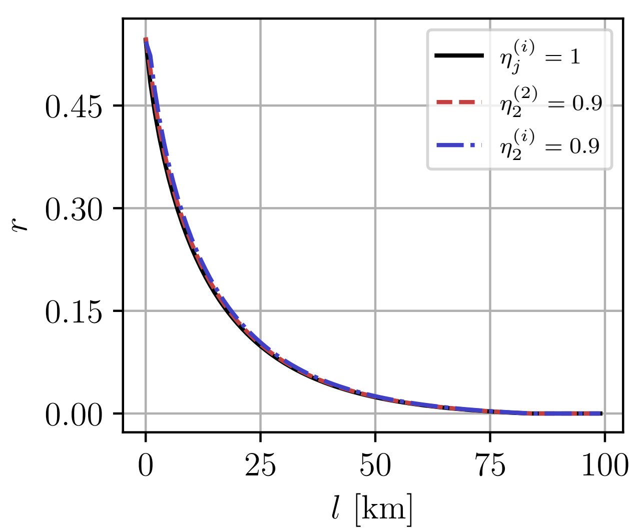


Figure 6: The asymptotic secret fraction as a function channel length computed for double homodyne detection **(trusted noise)** for various detector efficiencies. Parameters: $V = 1, T = 0.8, \xi = 10^{-3}, \beta = 0.95$.