Supplementary Information

Quantum utility routing in continuous-variable QKD networks with trusted and untrusted relays

Farsad Ahmad Aeysha Khalique

This document collects the established theoretical and methodological background used in the main manuscript. The numerical settings and the QUR routing and weight selection procedures are specified in the main Methods.

Supplementary Note 1. Composable finite-size SKR transition model

We evaluate all physical and relay transitions using the composable finite-size security framework for Gaussian quantum networks with untrusted relays under collective Gaussian attacks[1]. A transition contains $L_\ell = 1, \ldots, 4$ physical links, where $L_\ell = 1$ denotes a direct P2P connection and $L_\ell > 1$ contains $L_\ell - 1$ untrusted CV Bell-measurement relays.

For squeezing r_{dB}, the TMSV variance is

$$\mu = \cosh(2r), \qquad \text{for} \qquad r = \frac{r_{\mathrm{dB}} \ln 10}{20} \tag{S1}$$

and each physical link ℓ is represented in standard form by

$$\Gamma_\ell = \Gamma(a_\ell, b_\ell, c_\ell), \qquad a_\ell = \mu, \quad b_\ell = T_\ell \mu + 1 - T_\ell + \xi, \quad c_\ell = \sqrt{T_\ell(\mu^2 - 1)}, \tag{S2}$$

where ξ is the output referenced excess noise and transmissivity of the link is

$$T_\ell = 10^{-\alpha d_\ell / 10}, \qquad \alpha = 0.2 \text{ dB/km}. \tag{S3}$$

where d_ℓ is the link distance. For P2P transitions, the SKR is optimized over $r_{\mathrm{dB}} \in [1, 30]$ dB. Relay transitions are reduced recursively using the Gaussian swapping map. For a link $\ell = 1$ and $\ell = 2$, the swapped covariance matrix is

$$\Gamma(a', b', c') = \mathcal{S}[\Gamma(a_1, b_1, c_1), \Gamma(a_2, b_2, c_2)], \tag{S4}$$

where

$$\begin{aligned} &a' = a_1 - \frac{\eta_{\mathrm{B}} c_1^2}{D}, \qquad b' = b_2 - \frac{\eta_{\mathrm{B}} c_2^2}{D}, \qquad c' = \frac{\eta_{\mathrm{B}} c_1 c_2}{D}, \\ &D = \eta_{\mathrm{B}}(b_1 + a_2) + 1 - \eta_{\mathrm{B}}, \end{aligned} \tag{S5}$$

where η_B is the efficiency of the Bell measurement device.

For a block of $\mathcal{N}$ signals,

$$m = \lfloor f_{\mathrm{PE}} \mathcal{N} \rfloor, \qquad n = \mathcal{N} - m, \qquad p_{\mathrm{EC}} = 1 - \mathrm{FER}, \tag{S6}$$

where FER is the frame error rate which gives us p_{EC} as the probability that error correction succeeds, and f_{PE} is the fraction of signals used for parameter estimation. The parameter estimation uncertainty is

$$\delta_{\mathrm{PE}} = \sqrt{\frac{4 \ln(8/\epsilon_{\mathrm{PE}})}{m}}. \tag{S7}$$

The worst case covariance parameters are taken as

$$a_{\mathrm{wc}} = a + \delta_{\mathrm{PE}}(a + 1), \qquad b_{\mathrm{wc}} = b + \delta_{\mathrm{PE}}(b + 1), \qquad c_{\mathrm{wc}} = c - \frac{\delta_{\mathrm{PE}}}{2}(a + b + 2), \tag{S8}$$

The corresponding worst case covariance matrix is

$$\Gamma_{\rm wc} = \Gamma(a_{\rm wc}, b_{\rm wc}, c_{\rm wc}). \tag{S9}$$

These worst case covariance matrix parameters give us the symplectic eigenvalues

$$\nu_{1,2} = \sqrt{\frac{\Delta_{\rm wc} \mp \sqrt{\Delta_{\rm wc}^2 - 4\det\Gamma_{\rm wc}}}{2}}, \tag{S10}$$

where det is the determinant and

$$\Delta_{\rm wc} = a_{\rm wc}^2 + b_{\rm wc}^2 - 2c_{\rm wc}^2. \tag{S11}$$

For heterodyne detection, the conditional symplectic eigenvalue is

$$\nu_{\rm cond} = a_{\rm wc} - \frac{c_{\rm wc}^2}{b_{\rm wc}+1}. \tag{S12}$$

The corresponding worst case mutual and Holevo information, respectively, are

$$\begin{aligned} I_{AB}^{\rm wc} &= \log_2\left(\frac{a_{\rm wc}+1}{\nu_{\rm cond}+1}\right), \\ \chi_{BE}^{\rm wc} &= g(\nu_1) + g(\nu_2) - g(\nu_{\rm cond}), \end{aligned} \tag{S13}$$

where the bosonic entropy function is

$$g(\nu) = \frac{\nu+1}{2}\log_2\left(\frac{\nu+1}{2}\right) - \frac{\nu-1}{2}\log_2\left(\frac{\nu-1}{2}\right). \tag{S14}$$

The key rate after incorporating parameter estimation uncertainty is

$$K_{\rm PE} = \beta I_{AB}^{\rm wc} - \chi_{BE}^{\rm wc}. \tag{S15}$$

The composable finite size SKR assigned to the transition ℓ is

$$K_\ell = \frac{n p_{\rm EC}}{\mathcal{N}}\left[K_{\rm PE} - \frac{\Delta_{\rm AEP}}{\sqrt{n}} + \frac{\Theta}{n}\right], \tag{S16}$$

where the finite sized correction terms are

$$\begin{aligned} \Delta_{\rm AEP} &= 4\log_2(\sqrt{|\mathcal{X}|}+2)\sqrt{\log_2(18 p_{\rm EC}^{-2}\epsilon_s^{-4})}, \\ \Theta &= \log_2\left[p_{\rm EC}\left(1-\frac{\epsilon_s^2}{3}\right)\right] + 2\log_2(\sqrt{2}\epsilon_h), \end{aligned} \tag{S17}$$

where ϵ_c, ϵ_s, ϵ_h and $\epsilon_{\rm PE}$ are the security failure probabilities associated with correctness, smoothing, hashing and parameter estimation respectively and $|\mathcal{X}|$ is the size of the discretized measurement alphabet. The corresponding security parameter for the transition is

$$\epsilon_{\rm tr} = \epsilon_c + \epsilon_s + \epsilon_h + p_{\rm EC}\epsilon_{\rm PE}. \tag{S18}$$

The numerical parameter used in this study are specified in the main Methods.

Supplementary Note 2. Waxman graph generation

The standard Waxman construction used in the simulations is summarized below [2].

The physical network is modeled as an undirected Waxman graph $G = (V, E)$ with V vertices and E edges, and N_V nodes are uniformly distributed within a disk of radius R. For each node i, the radial and angular coordinates are generated as

$$\rho_i = R\sqrt{U_i}, \qquad \theta_i = 2\pi V_i, \qquad \boldsymbol{x}_i = \rho_i(\cos\theta_i, \sin\theta_i), \tag{S19}$$

where $U_i, V_i \sim \mathcal{U}(0,1)$ and $\boldsymbol{x}_i$ is the resulting position of node i. Edges are generated according to

$$P[(u,v)\in E] = \beta_W \exp\left(-\frac{d_{uv}}{r_0}\right), \qquad d_{uv} = \|\boldsymbol{x}_u - \boldsymbol{x}_v\|_2, \tag{S20}$$

where u and v are any two nodes in the network, d_{uv} is their Euclidean distance, and $\|\cdot\|_2$ denotes the Euclidean norm. The parameter $r_0 = 0.07R$ is the characteristic connection distance and controls how rapidly the probability of an edge decreases with node separation, while β_W controls the overall connection probability of the Waxman graph. Each edge represents an optical fiber link with attenuation coefficient $\alpha = 0.2\,\mathrm{dB/km}$.

Supplementary Note 3. A* routing

The geometric benchmark uses A* search[3]. Route notation follows from the main Methods.

A* is the geometric shortest route benchmark. The cost of a transition ℓ is the total length d_ℓ of the fiber links contained within that transition. For a partial route $\mathcal{R}_{S\to v}$ ending at trusted node v,

$$C_{A^*}(v) = \sum_{\ell\in\mathcal{R}_{S\to u}} d_\ell + d_\ell(u,v). \tag{S21}$$

The search priority is

$$f_{A^*}(v) = C_{A^*}(v) + \|\boldsymbol{x}_v - \boldsymbol{x}_T\|_2, \tag{S22}$$

where the second term is the Euclidean distance from current trusted node v to the destination T. The next trusted node is selected according to the lowest value of f_{A^*}.

Supplementary Note 4. Max–Min routing

The bottleneck rate benchmark uses Max–Min routing[4]. Here, $K(\mathcal{R}) = \min_{\ell\in\mathcal{R}} K_\ell$, with route notation as in the main Methods.

Max–Min selects the route with the largest bottleneck SKR,

$$\mathcal{R}^*_{\mathrm{MM}} = \arg\max_{\mathcal{R}\in\mathcal{R}_{ST}} K(\mathcal{R}), \tag{S23}$$

where $\mathcal{R}_{ST}$ is the set of available routes between the source and destination. If the current node is u and v is a reachable node, extending a partial route $\mathcal{R}_{S\to u}$ through the transition $\ell = (u,v)$ gives

$$K(\mathcal{R}_{S\to v}) = \min[K(\mathcal{R}_{S\to u}), K_\ell]\,. \tag{S24}$$

For each reachable node v, the partial route with the largest bottleneck SKR is retained. The Max–Min search priority is therefore

$$f_{\mathrm{MM}}(v) = \max_{\mathcal{R}\in\mathcal{R}_{S\to v}} K(\mathcal{R}), \tag{S25}$$

and the reachable node with the largest $f_{\mathrm{MM}}(v)$ is explored next.

Supplementary Note 5. Gradient boosting score model

Here, $\boldsymbol{z}$ combines graph properties and a QUR weight vector, and S' denotes the transformed optimization score defined in the main Methods.

We use histogram based gradient boosting[5;6]. The model is formed from a sequence of regression trees. Each new tree provides a correction to the prediction obtained from the preceding trees. Since the model is trained using the transformed score S', its final prediction is written as

$$S'^{,\mathrm{ML}}(\boldsymbol{z}) = F_0 + \lambda_{\mathrm{ML}} \sum_{t=1}^{T_{\mathrm{ML}}} f_t(\boldsymbol{z}), \tag{S26}$$

where F_0 is the initial prediction, $f_t(\boldsymbol{z})$ is the correction provided by regression tree t, $T_{\mathrm{ML}} = 300$ is the maximum number of trees, and $\lambda_{\mathrm{ML}} = 0.06$ controls the contribution of each new tree. The model parameters are chosen to limit the complexity of the regression trees and reduce overfitting, with a maximum of 31 leaf nodes, at least 20 training samples per leaf, and an ℓ_2 regularization value of 1.

Supplementary References

[1] Masoud Ghalaii, Panagiotis Papanastasiou, and Stefano Pirandola. Composable end-to-end security of gaussian quantum networks with untrusted relays. *npj Quantum Information*, 8:105, 2022. doi: 10.1038/s41534-022-00620-5.

[2] Cillian Harney and Stefano Pirandola. Practical routing and criticality in large-scale quantum communication networks. *Phys. Rev. Res.*, 7:043168, Nov 2025. doi: 10.1103/vy37-28jc. URL https://link.aps.org/doi/10.1103/vy37-28jc.

[3] Peter E. Hart, Nils J. Nilsson, and Bertram Raphael. A formal basis for the heuristic determination of minimum cost paths. *IEEE Transactions on Systems Science and Cybernetics*, 4(2):100–107, 1968. doi: 10.1109/TSSC.1968.300136.

[4] Maurice Pollack. Letter to the editor—the maximum capacity through a network. *Operations Research*, 8 (5):733–736, October 1960. ISSN 1526-5463. doi: 10.1287/opre.8.5.733. URL http://dx.doi.org/10.1287/opre.8.5.733.

[5] Duo Ma, Yue Li, Haoyang Wang, Kaiyi Shi, Chang Liu, Yujia Zhang, Fangze Ma, and Haiqiang Ma. Parameter optimization for mode-pairing quantum key distribution based on lightgbm. *Optics Continuum*, 5:611–620, 02 2026. doi: 10.1364/OPTCON.581743.

[6] Qin Dong, Guoqi Huang, Wei Cui, and Rongzhen Jiao. Optimization parameter prediction-based xgboost of tf-qkd. *Quantum Information Processing*, 21(7), 2022. ISSN 1573-1332. doi: 10.1007/s11128-022-03579-6. URL http://dx.doi.org/10.1007/s11128-022-03579-6.