

Article

Performance Improvement of Continuous-Variable Quantum Secret Sharing via Heralded Hybrid Linear Amplifier

Kunlin Zhou ¹ , Yang Yu ¹, Lining Zeng ¹, Shijie Deng ¹ and Ying Guo ^{2,*} 

¹ College of Business Administration, Hunan University of Finance and Economics, Changsha 410205, China; zhokunlin@hufe.edu.cn (K.Z.); yuyang@hufe.edu.cn (Y.Y.); zenglining@hufe.edu.cn (L.Z.); 202305690104@mails.hufe.edu.cn (S.D.)

² School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

* Correspondence: guoying@bupt.edu.cn

Abstract

Continuous-variable quantum secret sharing (CVQSS) distributes a secret key among multiple players while requiring their cooperation for reconstruction. Its performance deteriorates rapidly in sequential multiparty links because optical loss, excess noise, and receiver noise accumulate with the number of players. We investigate a dealer-side heralded hybrid linear amplifier (HHLA), formed by measurement-based noiseless linear amplification and trusted deterministic preamplification, for mitigating the relative receiver-noise penalty. The accepted data are described by an equivalent Gaussian channel and evaluated with an asymptotic reverse-reconciliation key-rate model against collective Gaussian attacks. We explicitly condition parameter estimation and Eve's Holevo information on successful heralding, include a cutoff-dependent Gaussian-input estimate of the heralding probability in the rate per transmitted pulse, apply a single calibrated output-quadrature rescaling, and provide parallel heterodyne and homodyne calculations. The homodyne simulation includes detector noise consistently in the mutual information and Holevo bound and enforces the Gaussian-equivalent NLA feasibility constraint. For an excess-noise variance of 0.001 shot-noise units per player, the constrained homodyne optimization gives maximum reported distances of approximately 108, 42, and 25.5 km for 5, 50, and 100 players, respectively, at a reporting floor of 10^{-6} bit/pulse. Composable finite-size security, finite-cutoff non-Gaussian corrections, and active-insider verifiability are left for future work.

Keywords: continuous-variable quantum secret sharing; heralded hybrid linear amplifier; quantum communication; performance improvement; quantum cryptography



Academic Editor: Michel Planat

Received: 24 June 2026

Revised: 14 July 2026

Accepted: 16 July 2026

Published: 18 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Secret sharing distributes a secret among several participants according to an access structure, so that only an authorized subset can reconstruct it. Classical threshold secret sharing was introduced independently by Shamir and Blakley [1,2]. Quantum secret sharing (QSS) subsequently used quantum states and measurements to protect the distribution and reconstruction processes. The seminal protocol of Hillery, Bužek, and Berthiaume used a Greenberger–Horne–Zeilinger state to establish a shared secret among multiple parties [3]. Unlike point-to-point quantum key distribution (QKD), QSS is intrinsically multiparty: in the (n, n) access structure considered here, all n players must cooperate with the dealer, and neither an individual player nor an unauthorized coalition should recover the secret.

QSS has developed along several complementary lines. Sequential single-qubit schemes reduce the need to distribute multipartite entanglement, although direct operations on a traveling system can create multiphoton and Trojan-horse vulnerabilities [4,5]. Dynamic QSS permits participants to join or leave while preserving the shares held by the remaining authorized users [6]. Semi-quantum QSS reduces endpoint requirements by restricting some users to a limited set of quantum operations; recent protocols add explicit verification against man-in-the-middle interference [7]. Mediated QSS delegates demanding quantum operations to a possibly untrusted mediator and thereby enables restricted users to participate under a different trust model [8]. These families improve flexibility, accessibility, or implementation efficiency, but practical QSS must still balance four coupled requirements: verifiability, resistance to dishonest participants, scalability with the number of users, and efficient use of quantum sources, memories, detectors, and classical communication.

Continuous-variable (CV) technology is attractive for this balance because Gaussian-modulated coherent states and homodyne or heterodyne receivers are compatible with mature optical-communication components [9,10]. Covariance matrices also provide an efficient description for parameter estimation and for bounding information leakage under Gaussian attacks. In a sequential CVQSS architecture, each player couples an independently prepared, Gaussian-modulated coherent state into a traveling mode through a highly asymmetric beam splitter. The dealer measures only the aggregate mode, so reconstruction requires the combined classical information of the authorized players. Local preparation and injection also reduce the need for each player to directly modulate a backward-propagating probe [5]. The security analysis of CVQSS is related to that of CVQKD, but the multiparty access structure adds insider and scaling issues. Security against external eavesdroppers and dishonest players has been studied in several CVQSS settings [11,12], while decentralized topologies, local-local-oscillator implementations, and discrete modulation improve practicality or reconciliation at low signal-to-noise ratio [13–15]. Nevertheless, in a sequential network the optical loss and excess noise seen by the most distant player increase with the number of intermediate nodes. At the same time, electronic noise and imperfect efficiency at the dealer become increasingly important when the received field is weak.

Receiver-side optical preamplification can reduce the relative detector-noise penalty. A noiseless linear amplifier (NLA) can probabilistically increase an optical amplitude without the deterministic noise penalty of a phase-insensitive amplifier, but its success probability decreases with gain and depends on the finite postselection cutoff and input distribution [16–20]. A heralded hybrid linear amplifier combines measurement-based NLA with deterministic linear amplification to trade gain, added noise, and acceptance probability [21,22]. A phase-insensitive amplifier is appropriate when both quadratures are measured by heterodyne detection, whereas an ideal phase-sensitive amplifier can amplify the measured quadrature without added noise in a homodyne receiver [23,24].

The research gap addressed here is therefore not merely the transfer of a CVQKD preamplifier to a new link. In sequential CVQSS, the amplifier acts on an aggregate optical mode containing all players' contributions; the dealer must then (i) estimate an accepted-event equivalent channel, (ii) remove the publicly disclosed contributions of a potentially colluding set without applying the gain twice, (iii) optimize the worst-player rate rather than a single point-to-point rate, and (iv) count failed heralding events in the throughput. We propose a dealer-side HHLA-assisted CVQSS protocol and provide a unified covariance-matrix analysis for heterodyne and homodyne receivers. The security claim is explicitly restricted to the asymptotic collective-attack model with a Gaussian-equivalent description

of the accepted data. Composable finite-size security, finite-cutoff non-Gaussian effects, and a complete active-insider verification proof are not claimed.

The remainder of this paper is organized as follows. Section 2 introduces the HHLA-assisted CVQSS protocol and derives its equivalent parameters. Section 3 derives the output-quadrature processing. Section 4 presents the key-rate model, a compact sensitivity summary, gain optimization, and numerical results. Appendix A gives the complete homodyne derivation, constrained optimization, and numerical results; Appendix B reports the complete parameter-sensitivity scans; and Appendix C makes the covariance-block notation explicit and derives the invariants used by the numerical algorithm.

2. HHLA-Assisted CVQSS Protocol

The HHLA is located inside the dealer's trusted receiver, before homodyne or heterodyne detection, as shown in Figure 1. A strong phase-reference pulse and active phase tracking may be used to establish a common quadrature frame. The present model assumes that residual phase noise is included in the experimentally estimated excess noise.

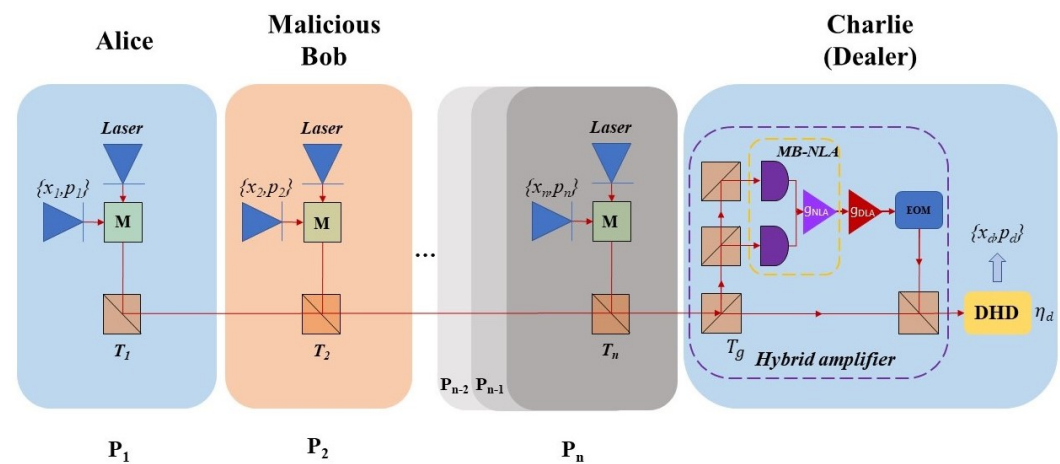


Figure 1. Sequential CVQSS assisted by an HHLA. The figure illustrates the security reduction in which player P_1 is treated as the candidate honest player and players $P_2, \dots, P_n$ are included in the adversarial coalition. The HHLA is located in the dealer's trusted receiver. DHD denotes conjugate heterodyne detection; for homodyne detection, DHD is replaced by a single-quadrature detector and an appropriate phase-sensitive deterministic amplifier.

2.1. Heralded Hybrid Linear Amplifier and Equivalent Parameters

Let $g_N \geq 1$ denote the amplitude gain of the measurement-based NLA, and let $G_D \geq 1$ denote the power gain of the deterministic amplifier, with quadrature gain $g_D = \sqrt{G_D}$. The total calibrated quadrature gain is

$$g_{\text{eff}} = g_N g_D. \quad (1)$$

The NLA is implemented as a heralded filter rather than as a deterministic operator. For a heterodyne outcome α_m and a radial cutoff α_c , a commonly used acceptance rule is

$$P_{\text{acc}}(\alpha_m) = \begin{cases} \exp\left[(1 - g_N^{-2})(|\alpha_m|^2 - \alpha_c^2)\right], & |\alpha_m| < \alpha_c, \\ 1, & |\alpha_m| \geq \alpha_c. \end{cases} \quad (2)$$

Consequently, the actual heralding probability is not fixed by the gain alone but must be evaluated from the measured input distribution,

$$P_s(g_N, \alpha_c) = \int_{\mathbb{C}} p(\alpha_m) P_{\text{acc}}(\alpha_m) d^2\alpha_m. \quad (3)$$

The frequently used expression $1/g_N^2$ is therefore only an idealized scaling rule and is not used as a substitute for the cutoff-dependent acceptance probability in the present security model.

For the equivalent entanglement-based description, the thermal coherent-state ensemble may be written as

$$\hat{\rho}_{\text{in}} = \frac{1}{\pi} \frac{1 - \lambda^2}{\lambda^2} \int d^2\alpha \exp\left[-\frac{1 - \lambda^2}{\lambda^2} |\alpha|^2\right] |\alpha\rangle\langle\alpha|, \quad (4)$$

where $V = (1 + \lambda^2)/(1 - \lambda^2)$ is the quadrature variance in shot-noise units (SNU). In the ideal NLA limit, the accepted ensemble has

$$V_g = \frac{1 + g_N^2 \lambda^2}{1 - g_N^2 \lambda^2}, \quad g_N^2 \lambda^2 < 1. \quad (5)$$

The finite-cutoff implementation approaches this transformation only within the operating region in which the accepted data are well approximated by a Gaussian distribution.

The effective parameters are obtained by matching the first and second moments of the accepted output to those of a Gaussian channel. Let T and ϵ be the pre-amplifier channel transmittance and input-referred excess noise. Solving the covariance-matrix matching equations gives [21,22]

$$\zeta = \lambda \sqrt{\frac{(g_N^2 - 1)(\epsilon - 2)T - 2}{(g_N^2 - 1)\epsilon T - 2}}, \quad (6)$$

$$T_g = \frac{g_N^2 T}{(g_N^2 - 1)T \left[\frac{1}{4}(g_N^2 - 1)(\epsilon - 2)\epsilon T - \epsilon + 1 \right] + 1}, \quad (7)$$

$$\epsilon_g = \epsilon - \frac{1}{2}(g_N^2 - 1)(\epsilon - 2)\epsilon T. \quad (8)$$

These equations are a covariance-equivalent representation of the accepted input–output statistics; they do not assert that the non-deterministic NLA physically commutes with channel loss. Their use requires (i) $g_N^2 \lambda^2 < 1$, (ii) real, positive denominators in Equations (6)–(8), (iii) a physical covariance matrix satisfying the uncertainty relation, and (iv) empirical confirmation that the accepted distribution is adequately Gaussian for the chosen cutoff.

The deterministic preamplifier is treated as a calibrated trusted receiver component. With detector efficiency η , electronic noise v_{el} , and deterministic-amplifier added noise $v_D^{(m)}$ for measurement $m \in \{\text{het}, \text{hom}\}$, the detector-added noises referred to the preamplifier input are written as

$$\chi_{\text{det}}^{\text{het}}(G_D) = \frac{2 - \eta + 2v_{\text{el}} + v_D^{\text{het}}}{\eta G_D}, \quad (9)$$

$$\chi_{\text{det}}^{\text{hom}}(G_D) = \frac{1 - \eta + v_{\text{el}} + v_D^{\text{hom}}}{\eta G_D}. \quad (10)$$

For an ideal phase-sensitive amplifier aligned with the measured homodyne quadrature, $v_D^{\text{hom}} = 0$; a phase-insensitive amplifier used before heterodyne detection necessarily

has nonzero added noise. Equations (9) and (10) also fix the notation: G_D is a power gain, whereas $g_D = \sqrt{G_D}$ is the quadrature gain used in data rescaling. The step-by-step construction of the equivalent amplified channel is summarized in Table 1.

Table 1. Step-by-step construction of the equivalent amplified channel.

Step	Quantity	Operation and Assumption
1	Pre-amplifier moments (T, ϵ, V)	Estimated from a randomly disclosed calibration subset before applying the accepted-event model.
2	NLA filter (g_N, α_c)	Apply Equation (2); record the public herald flag H and evaluate $P_s = N_{H=1} / N_{\text{sent}}$ experimentally, or use the explicitly stated Gaussian-input model when only analytical simulation data are available.
3	Accepted-event moments	Re-estimate means and covariances conditional on $H = 1$; verify the Gaussian-equivalent approximation.
4	(ζ, T_g, ϵ_g)	Match the accepted covariance matrix using Equations (6)–(8); reject unphysical parameter points.
5	$\chi_{\text{det}}^{(m)}$	Add the calibrated trusted DLA/detector contribution from Equations (9) or (10).
6	Secret throughput	Compute the conditional Devetak–Winter term and multiply by the measured P_s and other implementation efficiencies.

Because each candidate honest player has a different path to the dealer, the procedure is applied to every effective link. Figure 2 distinguishes the physical channel from its accepted-event Gaussian representation.

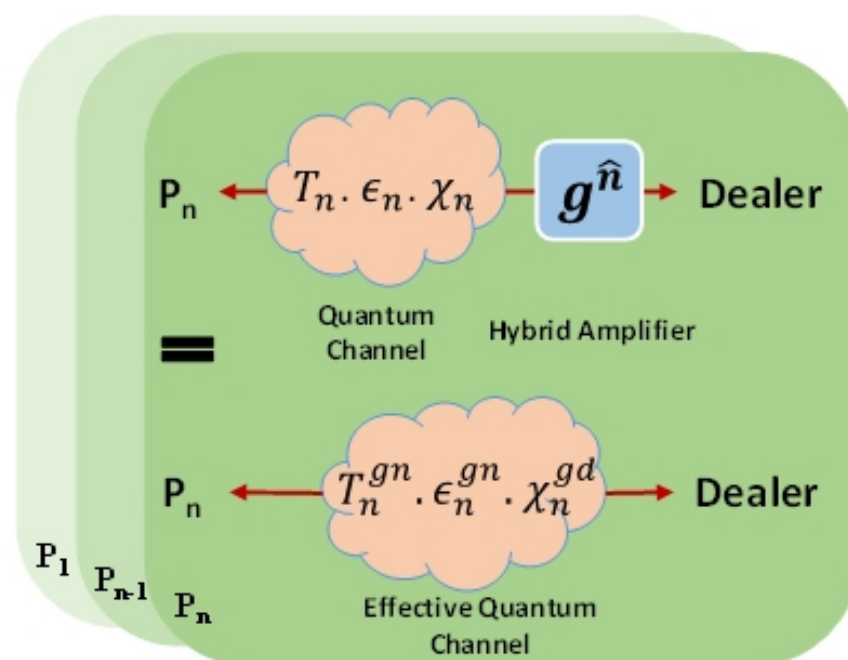


Figure 2. Equivalent-channel representation. The upper channel has transmittance T_k , excess noise ϵ_k , and trusted detector noise $\chi_{\text{det}}^{(m)}$. Conditional on a successful herald, the lower Gaussian channel has matched parameters $T_{g,k}$ and $\epsilon_{g,k}$, followed by the same calibrated trusted receiver. The equivalence concerns accepted first and second moments and is not a physical rearrangement of the probabilistic NLA and channel loss.

2.2. Sequential CVQSS Operation

In each round, player P_1 prepares a coherent state with Gaussian quadratures (x_1, p_1) and sends it to P_2 . Player P_k couples an independently prepared coherent state into the traveling mode through a highly asymmetric beam splitter of transmittance $T_{BS} \simeq 1$. After all n injections, the aggregate field arriving at the dealer before amplification is

$$\left| \sum_{k=1}^n \sqrt{T_k^{\text{path}}} x_k + i \sum_{k=1}^n \sqrt{T_k^{\text{path}}} p_k \right\rangle, \quad (11)$$

where T_k^{path} includes fiber loss and all downstream beam-splitter losses for player P_k . The dealer records the HHLA herald flag and measures the accepted round by heterodyne or homodyne detection.

A random subset of accepted and rejected rounds is used to estimate the acceptance probability and channel statistics. For the key associated with candidate honest player P_k , the other $n - 1$ players are conservatively grouped with the external eavesdropper and disclose their modulation data on the designated parameter-estimation subset. The dealer subtracts their expected accepted-event contribution and calculates a pairwise lower bound R_k . The multiparty rate is

$$R_{\text{QSS}} = \min_{k \in \{1, \dots, n\}} R_k. \quad (12)$$

This worst-player construction models collusion of the other players at the level of the information bound. It does not by itself provide a complete verifiable-QSS proof against arbitrary active insiders who send inconsistent states or announcements; such behavior must be detected by authentication, monitoring, and parameter-estimation abort tests.

2.3. Security Model and Heralding

The numerical security claim is asymptotic and restricted to collective Gaussian attacks with reverse reconciliation. For every candidate honest player, all other players may collude with Eve. The dealer's laboratory, random-number generators, classical authentication, HHLA, and detector calibration are trusted. Under these assumptions, the conditional key fraction per accepted round is

$$K_k^{\text{acc}} = [\beta I_{kD} - \chi_{DE}]_+, \quad [x]_+ = \max(x, 0), \quad (13)$$

where β is the reconciliation efficiency, I_{kD} is the mutual information between P_k and the dealer, and χ_{DE} bounds Eve's information about the dealer's accepted measurement.

The public herald variable H is available to Eve. Parameter estimation is therefore performed on the distribution conditioned on $H = 1$, and Eve's Holevo information is evaluated for that same accepted ensemble. The rate per transmitted pulse is

$$R_k^{\text{tx}} = P_s p_{\text{sift}} (1 - \text{FER}) K_k^{\text{acc}}, \quad (14)$$

where p_{sift} is the basis/sifting factor and FER is the frame-error rate. Failed heralds generate no raw key, but they are not ignored: their number determines P_s and must be included in finite-size accounting. The final secret-bit throughput at repetition rate f_{rep} is $f_{\text{rep}} R_{\text{QSS}}^{\text{tx}}$.

The accepted-event covariance matrix is used to bound χ_{DE} . In the minimal two-mode equivalent model,

$$\Gamma_{AD} = \begin{pmatrix} a\mathbf{I}_2 & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I}_2 \end{pmatrix}, \quad \mathbf{I}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{Z} = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (15)$$

Here, bold uppercase symbols denote matrices, and bold lowercase symbols denote column vectors. Thus, $\mathbf{I}_2$ and $\mathbf{Z}$ are matrix blocks, not vectors. Their explicit use in the symplectic invariants A , B , C_m , and D_m is derived in Appendix C. The scalar block coefficients are

$$a = V, \quad b = T_g(V + \chi_{\text{line}}), \quad c = \sqrt{T_g(V^2 - 1)}. \quad (16)$$

The global and conditional symplectic spectra are obtained from the positive eigenvalues of $|i\Omega\Gamma|$. Defining

$$h(v) = \frac{v+1}{2} \log_2 \frac{v+1}{2} - \frac{v-1}{2} \log_2 \frac{v-1}{2}, \quad (17)$$

the reverse-reconciliation Holevo term is evaluated as

$$\chi_{DE}^{(m)} = \sum_j h(v_j) - \sum_j h(\tilde{v}_j^{(m)}), \quad (18)$$

where $\{v_j\}$ and $\{\tilde{v}_j^{(m)}\}$ are the symplectic eigenvalues before and after the dealer's measurement m . Trusted detector and amplifier ancillas must be included explicitly when their noise is purified in the receiver model. This matrix prescription avoids notational ambiguity and algebraic inconsistencies in closed-form calculations.

The analysis is not a composable finite-size proof. In particular, it does not derive confidence intervals for the postselected covariance matrix, entropy-accumulation terms, leakage from error correction, or a security penalty for the finite-cutoff non-Gaussian filter. These limitations are stated explicitly rather than absorbed into the asymptotic curves [25,26].

3. Processing of the Amplified Output Quadratures

The accepted detector record is referred to the channel input by applying the calibrated inverse gain exactly once. Introducing a primed record and dividing it by the same gain a second time would apply the calibration twice and produce an incorrect double scaling.

Let $q \in \{x, p\}$, and let q_D^{amp} be the accepted detector record after the HHLA. A calibrated linear model is

$$q_D^{\text{amp}} = g_{\text{eff}} q_D^{\text{pre}} + z_D, \quad (19)$$

where q_D^{pre} is the preamplifier quadrature and z_D is the trusted receiver noise. The once-rescaled record is

$$\tilde{q}_D = \frac{q_D^{\text{amp}}}{g_{\text{eff}}}. \quad (20)$$

For candidate honest player P_k , the announced contribution of the other players, expressed on the same preamplifier input scale, is

$$q_{\bar{k}} = \sum_{j \neq k} \sqrt{T_j^{\text{path}}} q_j. \quad (21)$$

The residual used for parameter estimation and reconciliation is therefore

$$q_f^{(k)} = \tilde{q}_D - q_{\bar{k}} = \frac{q_D^{\text{amp}}}{g_N \sqrt{G_D}} - \sum_{j \neq k} \sqrt{T_j^{\text{path}}} q_j. \quad (22)$$

No additional division by $g_N \sqrt{G_D}$ is applied to Equation (22). The detector-noise conversion in Equations (9) and (10) is a separate input-referencing operation and must not

be confused with rescaling the classical data. Table 2 summarizes the application of the effective gain, coalition subtraction, trusted detector noise, and heralding probability in the data-processing procedure.

Table 2. Summary of gain and noise bookkeeping.

Quantity	Definition	Applied How Many Times?
Quadrature gain	$g_{\text{eff}} = g_N \sqrt{G_D}$	Once in Equation (20).
Coalition subtraction	$q_{\bar{k}}$	Once, after both terms are on the same scale.
Trusted detector noise	$\chi_{\text{det}}^{(m)}$	Included once in $\chi_{\text{tot}}^{(m)}$.
Heralding probability	Measured $P_s = N_{H=1}/N_{\text{sent}}$	Multiplies the accepted key fraction once.

4. Numerical Model and Performance Analysis

We use Gaussian modulation and reverse reconciliation. The most distant player is labeled Alice and the dealer is labeled Bob for compatibility with standard CVQKD notation. For equally spaced players over total distance L , the distance from P_k to the dealer is

$$l_k = \frac{n-k+1}{n}L, \quad (23)$$

and the fiber transmittance is

$$T_k = 10^{-\gamma l_k/10}, \quad (24)$$

where γ is the fiber attenuation in dB/km. The total accepted-event excess noise for each candidate link should be estimated from disclosed accepted samples. To reproduce the original baseline model, the node contributions are parameterized as

$$\epsilon_{\text{tot}} = \sum_{k=1}^n \epsilon_k, \quad \epsilon_k = \frac{T_k}{T_{g,1}} \epsilon_0, \quad (25)$$

where ϵ_0 is the assumed excess-noise variance per node and $T_{g,1}$ is the effective transmittance of the most distant link. This parameterization is a simulation assumption, not a substitute for experimental estimation.

The line noise and total input-referred noises are

$$\chi_{\text{line}} = \frac{1 - T_g}{T_g} + \epsilon_{\text{tot}}, \quad (26)$$

$$\chi_{\text{tot}}^{\text{het}} = \chi_{\text{line}} + \frac{\chi_{\text{det}}^{\text{het}}}{T_g}, \quad (27)$$

$$\chi_{\text{tot}}^{\text{hom}} = \chi_{\text{line}} + \frac{\chi_{\text{det}}^{\text{hom}}}{T_g}. \quad (28)$$

With $V = V_A + 1$, the mutual information is

$$I_{AD}^{\text{het}} = \log_2 \left(\frac{V + \chi_{\text{tot}}^{\text{het}}}{1 + \chi_{\text{tot}}^{\text{het}}} \right), \quad (29)$$

$$I_{AD}^{\text{hom}} = \frac{1}{2} \log_2 \left(\frac{V + \chi_{\text{tot}}^{\text{hom}}}{1 + \chi_{\text{tot}}^{\text{hom}}} \right). \quad (30)$$

The Holevo information is evaluated from Equation (18); Appendix A provides the measurement-conditioned covariance matrices for both receiver choices.

4.1. Reproducible Numerical Workflow and Parameters

Figure 3 summarizes the numerical implementation. For each calibrated player number and distance, the code scans the admissible modulation, NLA gain, deterministic gain, and cutoff values. Unphysical points are rejected before the key rate is evaluated. The same accepted covariance matrix is then used consistently for parameter estimation, mutual information, the Holevo bound, and the heralding-normalized throughput. Appendix C gives the corresponding block-matrix derivation and step-by-step pseudocode.

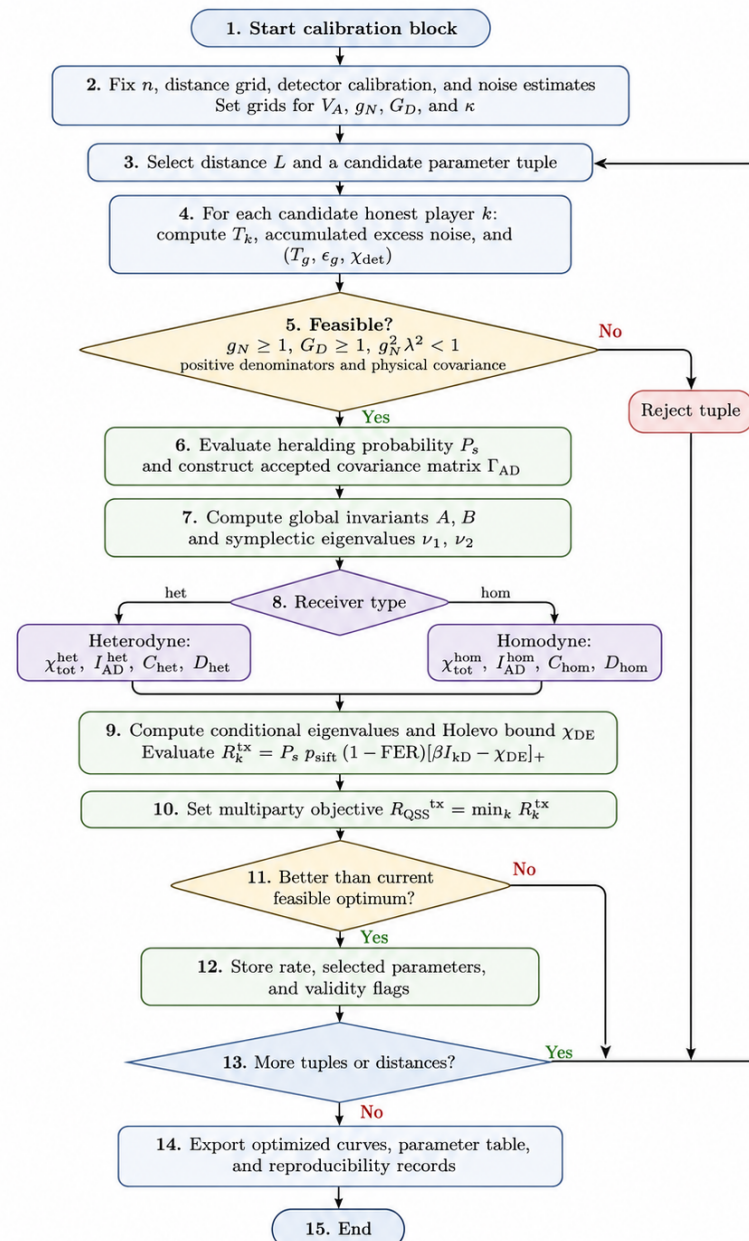


Figure 3. Flowchart of the numerical implementation. Calibration parameters and scan ranges are fixed before a key-generation block. For every candidate parameter tuple, the algorithm checks the NLA and covariance-matrix feasibility constraints, evaluates the accepted-event equivalent channel, constructs Γ_{AD} , calculates the global and measurement-conditioned symplectic spectra, obtains the worst-player transmitted-pulse rate, and retains the feasible tuple that maximizes that rate.

Table 3 consolidates the manuscript-specific notation with the numerical values and scan ranges used in the reproducible calculations. Standard quantities are defined at first use in the text, whereas the table retains only the symbols needed to interpret or reproduce

the numerical algorithm. The representative gain-scan figures use the values stated individually in their captions and are not used to define the optimized homodyne envelopes.

Table 3. Key notation, numerical parameters, and scan ranges used in the simulations. A colon denotes an equally spaced grid.

Symbol	Meaning	Definition, Value, or Scan Range
n	Number of players	Heterodyne sensitivity study: 5; homodyne optimization: {5, 50, 100}.
L	Total distance	0.5:0.5:130 km for both receiver models.
γ	Fiber attenuation	0.2 dB/km.
ϵ_0	Excess noise per player	Baseline 0.001 SNU; heterodyne scan {0.001, 0.003, 0.005, 0.010} SNU.
v_{el}	Electronic noise	Baseline 0.01 SNU; heterodyne scan {0, 0.01, 0.03, 0.05} SNU.
η	Detector efficiency	Baseline 0.50; heterodyne scan {0.30, 0.50, 0.70, 0.90}.
β	Reconciliation efficiency	Baseline 0.98; heterodyne scan {0.90, 0.95, 0.98, 0.99}.
V_A	Modulation variance	Heterodyne baseline 5 SNU and scan {1, 5, 10, 20} SNU; homodyne grid {1, 2, 5, 10, 20, 40} SNU.
T_{BS}	Injection transmittance	Heterodyne baseline 0.99 and scan {0.95, 0.97, 0.99, 0.995}; homodyne fiber-only benchmark $T_{\text{BS}} = 1$.
g_N	NLA amplitude gain	Heterodyne baseline 1.10; homodyne grid spacing $\Delta g_N = 0.02$ over $1 \leq g_N < \min\{2, \sqrt{(V_A + 2)/V_A}\}$.
G_D	Deterministic power gain	Heterodyne baseline 4; homodyne grid {1, 2, 4, 8, 16}.
κ	Normalized cutoff	Baseline 2; probability scan 1:0.01:3.5; throughput scan {1.5, 2, 2.5, 3}.
$p_{\text{sift}}, \text{FER}$	Sifting and frame-error factors	$p_{\text{sift}} = 1$ and $\text{FER} = 0$ in the asymptotic physical-layer simulations; basis sifting and frame-error effects can be included through Equation (14).
R_{min}	Reporting floor	Positive-rate plots and maximum-distance results use 10^{-6} bit/pulse.
T_g, ϵ_g	Accepted-event equivalent channel	Transmittance and input-referred excess noise obtained from moment matching after successful heralding.
$\chi_{\text{line}}, \chi_{\text{det}}^{(m)}, \chi_{\text{tot}}^{(m)}$	Noise quantities	Line, trusted receiver, and total input-referred noise for $m \in \{\text{het}, \text{hom}\}$.
$\Gamma_{AD}, \mathbf{I}_2, \mathbf{Z}$	Covariance-matrix notation	Accepted player–dealer covariance matrix, identity block, and phase-space sign block; explicit forms are given in Equation (15).
$A, B, C_m, D_m; v_j, \tilde{v}_j^{(m)}$	Symplectic quantities	Global and measurement-conditioned invariants and symplectic eigenvalues used in the Holevo calculation; derived in Appendix C.
$P_s, K_k^{\text{acc}}, R_k^{\text{tx}}, R_{\text{QSS}}^{\text{tx}}$	Rate quantities	Heralding probability, accepted-round key fraction, transmitted-pulse pairwise rate, and worst-player multiparty rate.

4.2. Sensitivity Analysis Summary

The five-player heterodyne sensitivity study uses the baseline $n = 5$, $g_N = 1.10$, $G_D = 4$, $\epsilon_0 = 0.001$ SNU per player, $v_{\text{el}} = 0.01$ SNU, $\eta = 0.50$, $\beta = 0.98$, $V_A = 5$ SNU, and $T_{\text{BS}} = 0.99$. The conventional reference uses $g_N = G_D = 1$. The asymptotic physical-layer calculation sets $p_{\text{sift}} = 1$ and $\text{FER} = 0$ and uses the explicitly stated Gaussian-input model for the heralding probability.

For a circular Gaussian heterodyne outcome distribution,

$$p(\alpha_m) = \frac{1}{\pi\sigma_\alpha^2} \exp\left(-\frac{|\alpha_m|^2}{\sigma_\alpha^2}\right), \quad \kappa = \frac{\alpha_c}{\sigma_\alpha}, \quad (31)$$

Equation (3) yields

$$P_s(g_N, \kappa) = g_N^2 e^{-(1-g_N^2)\kappa^2} \left(1 - e^{-\kappa^2/g_N^2}\right) + e^{-\kappa^2}. \quad (32)$$

The corresponding transmitted-pulse rate is

$$R_{\text{het}}^{\text{tx}} = P_s(g_N, \kappa) [\beta I_{AD}^{\text{het}} - \chi_{DE}^{\text{het}}]_+. \quad (33)$$

This is a cutoff-dependent analytical estimate, not an experimentally measured success probability, and it does not model finite-cutoff changes in higher moments or non-Gaussian composable-security corrections.

For the baseline $g_N = 1.10$ and $\kappa = 2.0$, Equation (32) gives $P_s = 0.6005$. Increasing the per-player excess noise from 0.001 to 0.010 SNU reduces the HHLA maximum positive-rate distance from approximately 105.5 to 43.0 km. At 20 km the HHLA/no-amplifier rate ratio decreases from 1.094 to 1.044, and at 40 km with $\epsilon_0 = 0.010$ SNU it falls below unity (0.907). The cutoff scan also shows that, for $g_N = 1.10$, P_s decreases from 0.797 to 0.254 as κ increases from 1.5 to 3.0. These two dominant limitations are summarized in Figure 4.

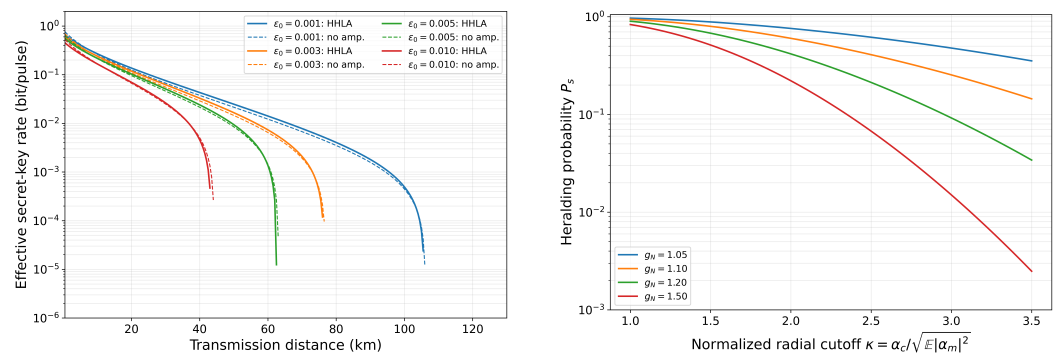


Figure 4. Compact sensitivity summary for the $n = 5$ heterodyne model. Left: transmitted-pulse key rate versus distance for several per-player excess-noise levels; solid HHLA curves use $g_N = 1.10$, $G_D = 4$, and $\kappa = 2.0$, while dashed curves are the corresponding no-amplifier references. Right: Gaussian-input heralding probability versus normalized cutoff for several NLA gains.

Additional scans of detector efficiency, electronic noise, reconciliation efficiency, modulation variance, beam-splitter transmittance, and cutoff-dependent throughput, together with the numerical summary table, are provided in Appendix B. They show that the HHLA benefit is strongest for inefficient receivers, while aggressive cutoff choices and realistic excess noise can remove the net throughput advantage. The main text therefore retains the dominant trends, while Appendix B provides the complete numerical evidence.

4.3. Gain and Cutoff Optimization

The gains must be selected before a key-generation block from calibration data that are independent of the raw key. The practical objective is the worst-player transmitted-pulse throughput,

$$(g_N^*, G_D^*, \alpha_c^*, V_A^*) = \arg \max_{(g_N, G_D, \alpha_c, V_A) \in \mathcal{F}} \min_k R_k^{\text{tx}}. \quad (34)$$

The feasible set $\mathcal{F}$ imposes

$$g_N \geq 1, \quad G_D \geq 1, \quad g_N^2 \lambda^2 < 1, \quad P_s \geq P_s^{\min}, \quad (35)$$

together with hardware gain limits, a physical covariance matrix, acceptable filter non-Gaussianity, and a positive key rate for every required player. A coarse grid followed

by a derivative-free local search is sufficient because the objective includes postselection and is generally non-smooth. For each trial point, the algorithm (i) applies the empirical acceptance filter, (ii) estimates P_s and the accepted covariance matrix, (iii) computes T_g , ϵ_g , and $\chi_{\text{det}}^{(m)}$, (iv) evaluates Equation (14) for every player, and (v) retains the smallest rate.

Values $g_N < 1$ are attenuation, not noiseless amplification. They may be plotted as a diagnostic attenuator baseline but must be excluded from the reported NLA optimization domain and must not be described as an amplifier gain. Between key-generation blocks, the calibration and optimization may be repeated; gains are not adapted using secret raw-key values within a block.

4.4. Computational Cost, Applicability, and Tradeoffs

Let N_L , N_N , N_D , N_V , and N_k denote the numbers of distance, NLA-gain, deterministic-gain, modulation, and cutoff grid points. Because each trial evaluates all n candidate honest-player links and only constant-size covariance matrices, the grid-search cost scales as $\mathcal{O}(nN_LN_NN_DN_VN_k)$. Storing only the best feasible tuple at each distance requires $\mathcal{O}(N_L)$ memory, whereas retaining complete gain–distance surfaces requires $\mathcal{O}(N_LN_N)$ or more. The present asymptotic Gaussian calculations are therefore computationally modest, but event-level postselection, finite-size confidence regions, and composable optimization would add a sample-size-dependent cost.

The physical and methodological drawbacks are equally important. Increasing g_N or the cutoff can improve a conditional signal but lowers P_s , so the transmitted-pulse rate can decrease. A deterministic phase-insensitive amplifier adds noise, while a phase-sensitive amplifier requires phase locking and only amplifies the selected quadrature. Detector calibration error, amplifier saturation, finite dynamic range, and finite-cutoff non-Gaussianity can invalidate the equivalent Gaussian model. The objective is non-convex, and no universal gain setting applies across node number, distance, and noise. Finally, the reported scope is an (n, n) sequential access structure with equally spaced players, the stated per-player noise model, asymptotic collective Gaussian attacks, and trusted dealer-side hardware. Arbitrary access structures, general active-insider attacks, composable finite-size security, and a full experimental HHLA model are outside the present claim. These limitations explain why the HHLA can improve rates in selected detector-limited regimes without guaranteeing a longer maximum distance in every operating condition.

4.5. Representative Heterodyne Gain Scans and Comparisons

Figures 5–12 provide a detailed view of the heterodyne simulations used to examine how the HHLA gain should be selected for different network sizes. The three-dimensional scans in Figures 5–7 vary the NLA gain and transmission distance while fixing $G_D = 4$, $\epsilon_0 = 0.001$ SNU, $v_{\text{el}} = 0.01$ SNU, $\eta = 0.5$, and $\beta = 0.98$. The total quadrature variance in these representative gain scans is $V = 20$. These figures retain the idealized gain-only heralding approximation $P_s = 1/g_N^2$ so that the gain dependence can be compared directly with the original numerical study. By contrast, the sensitivity analysis in Section 4.2 and Appendix B uses the finite-cutoff acceptance model and therefore provides the more complete transmitted-pulse throughput assessment. In addition, the portions of the surfaces with $g_N < 1$ represent attenuation rather than noiseless amplification and are not included in the physical NLA optimization domain.

For the five-player case, Figure 5 shows that the positive-key-rate surface extends beyond 100 km over part of the displayed gain range. Increasing g_N initially shifts the positive-rate boundary toward longer distance because the accepted data are described by a larger effective transmittance. The improvement becomes progressively weaker once g_N is above approximately 3, indicating a broad saturation region rather than an indefinitely

increasing benefit. This behavior is expected because the conditional channel improvement must be balanced against the decreasing heralding probability. Thus, the figure identifies a wide feasible gain region for $n = 5$, but it does not by itself define a unique optimum.

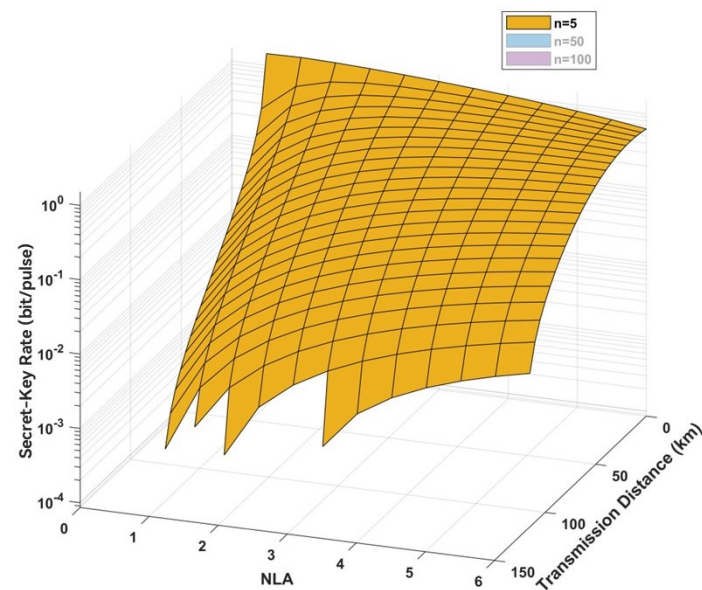


Figure 5. Heterodyne key-rate surface for $n = 5$ as a function of NLA gain and distance. Parameters: $G_D = 4$, $V = 20$, $\epsilon_0 = 0.001$ SNU, $v_{el} = 0.01$ SNU, $\eta = 0.5$, and $\beta = 0.98$. The rate per transmitted pulse uses the idealized gain-only factor $P_s = 1/g_N^2$.

When the number of players is increased to $n = 50$, the accumulated channel noise and insertion loss reduce both the height and the distance extent of the positive-rate surface. As shown in Figure 6, the maximum positive-rate distance remains slightly above 40 km, while the useful NLA-gain region is concentrated approximately within $1 \leq g_N \leq 3$. Compared with the five-player result, the surface contracts more rapidly at large gain, showing that the success-probability penalty becomes increasingly important as the multiparty channel becomes noisier.

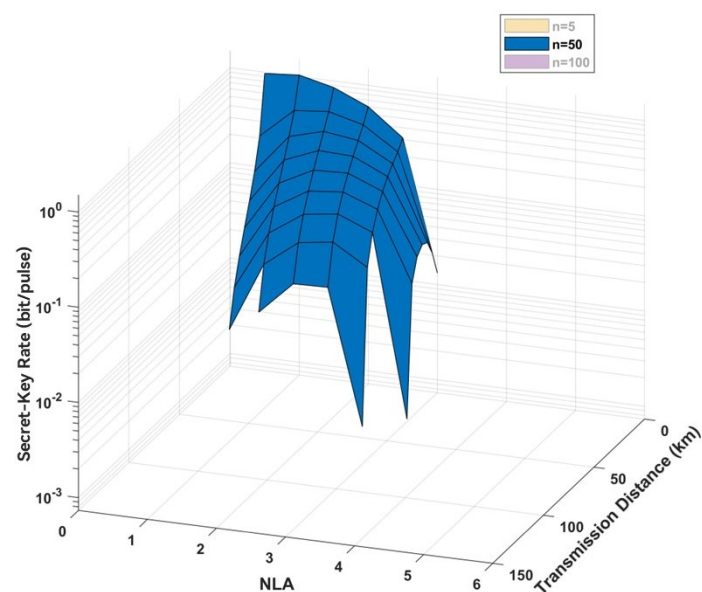


Figure 6. Heterodyne key-rate surface for $n = 50$ as a function of NLA gain and distance. The parameters are the same as in Figure 5, and the rate uses the idealized gain-only heralding factor $P_s = 1/g_N^2$.

Figure 7 gives the corresponding result for $n = 100$. The positive-rate region is further compressed, and the maximum displayed distance is only slightly above 20 km. A positive rate is mainly obtained for gains up to approximately $g_N = 2$. This contraction illustrates the central scalability tradeoff of the sequential CVQSS architecture: each additional player contributes to the accumulated excess noise and loss, whereas the HHLA acts only at the dealer and cannot remove all multiparty penalties.

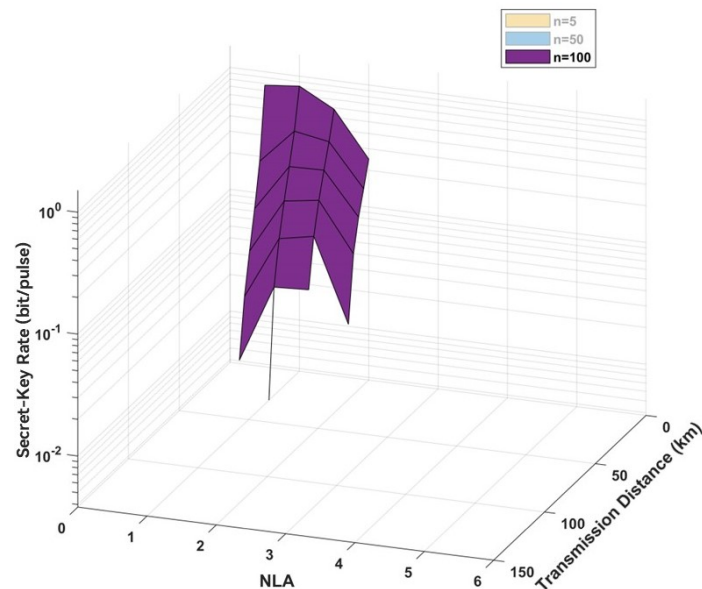


Figure 7. Heterodyne key-rate surface for $n = 100$ as a function of NLA gain and distance. The parameters are the same as in Figure 5, and the rate uses the idealized gain-only heralding factor $P_s = 1/g_N^2$.

Figure 8 superposes the positive-rate regions for the three network sizes and makes the scaling trend more explicit. The yellow, blue, and purple regions correspond to $n = 5$, 50, and 100, respectively. As n increases, both the maximum distance and the admissible gain interval decrease. Within the physical amplification region $g_N \geq 1$, an interval close to $1 \leq g_N \leq 2$ produces a positive rate for all three displayed node numbers. Nevertheless, the existence of a positive rate is not sufficient to establish optimality: a gain that slightly extends the long-distance boundary may substantially reduce the short-distance transmitted-pulse rate. The overlapping region is therefore used only to define an initial feasible search range, whereas the final gain is selected by the constrained objective in Equation (34).

To examine this issue more closely, Figure 9 magnifies the gain dependence over the short-distance interval from 0 to 1 km. The rate is relatively stable for moderate gain but decreases when the heralding penalty becomes dominant. The reduction is particularly visible for the $n = 50$ curve, for which a gain that remains feasible at long distance can noticeably lower the initial key rate. In the representative scans, $1 \leq g_N \leq 1.5$ provides a useful common compromise among positive rate, acceptance probability, and short-distance stability. This interval should not be interpreted as a universal optimum; the preferred value depends on n , distance, detector parameters, modulation variance, and the selected cutoff.

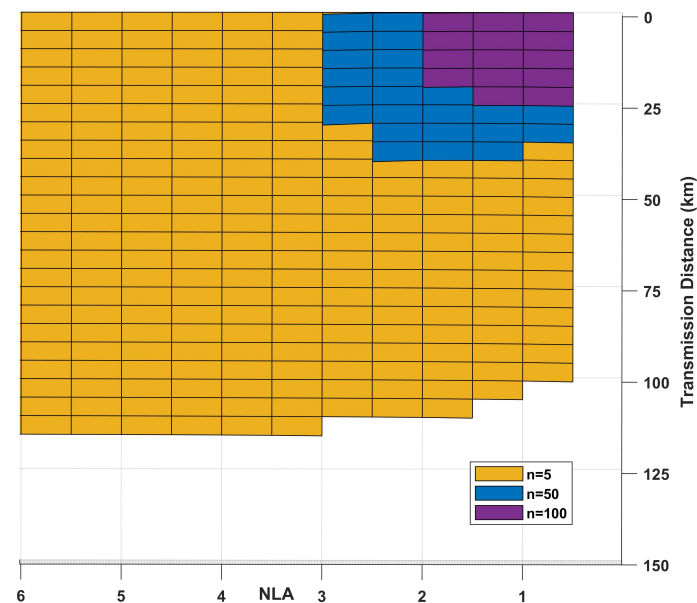


Figure 8. Heterodyne positive-rate regions versus gain and distance for $n = 5$ (yellow), $n = 50$ (blue), and $n = 100$ (purple). The portion $g_N < 1$ is an attenuation baseline and is excluded from the NLA optimization domain.

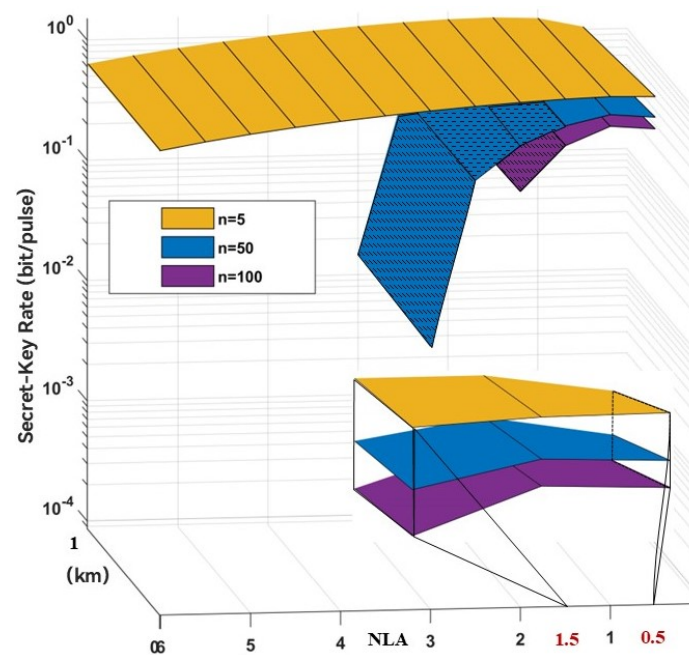


Figure 9. Heterodyne short-distance key rate versus g_N for $n = 5, 50$, and 100 . Yellow, blue, and purple denote the three node numbers, respectively. Points with $g_N < 1$ are attenuation baselines, and the curves use the idealized gain-only heralding factor.

The effect of using a common moderate gain is shown in Figure 10. Here, $g_N = 1.5$ and $G_D = 4$ are applied to all three network sizes. For $n = 5$, the HHLA-assisted curve reaches approximately 98 km, about 7.5 km farther than the corresponding conventional CVQSS curve. For $n = 50$, the maximum distance is approximately 44 km, giving an improvement of about 3 km. At $n = 100$, the HHLA-assisted curve does not improve the maximum distance under this common-gain setting; however, it remains above the conventional curve over an intermediate range of approximately 2–24 km. The result shows that one fixed gain can be effective for small and medium networks but becomes increasingly suboptimal as the number of players grows.

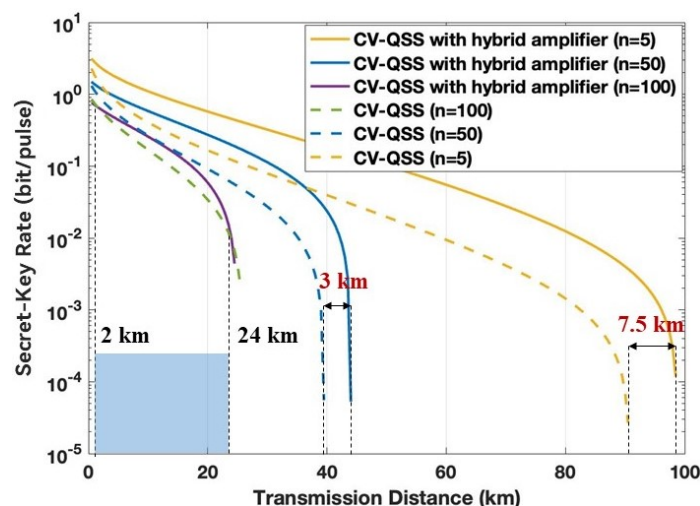


Figure 10. Comparison of conventional and HHLA-assisted CVQSS with heterodyne detection for the common setting $g_N = 1.5$ and $G_D = 4$. Parameters: $\gamma = 0.2$ dB/km, $\epsilon_0 = 0.001$ SNU, $v_{el} = 0.01$ SNU, $\eta = 0.5$, and $\beta = 0.98$. Yellow, blue, and purple solid curves denote HHLA-assisted CVQSS for $n = 5$, 50, and 100, respectively; the corresponding dashed curves denote conventional CVQSS. The HHLA curves use the idealized gain-only heralding factor.

Figure 11 illustrates the tradeoff more clearly by increasing the NLA gain to $g_N = 2.1$ while retaining $G_D = 4$; for the $n = 50$ curve, the modulation variance is $V_A = 60$ SNU. For $n = 5$, the maximum distance increases to approximately 108 km, about 18 km beyond the conventional scheme. For $n = 50$, however, the two schemes reach nearly the same maximum distance of approximately 39 km. The HHLA-assisted curve is higher only over an intermediate interval of roughly 12–39 km. At very short distance, its rate is lower: the plotted initial values are approximately 0.277 and 1.315 bit/pulse for the HHLA-assisted and conventional schemes, respectively. This difference is a direct consequence of postselection, because only successfully heralded events contribute to the transmitted-pulse key rate. Hence, maximizing the conditional gain alone can extend a low-rate tail while simultaneously reducing the useful throughput at shorter distance.

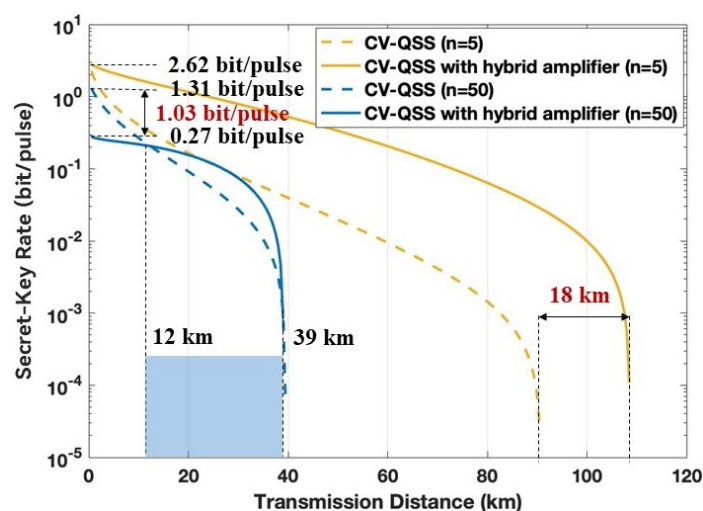


Figure 11. Heterodyne comparison at the larger gain $g_N = 2.1$ with $G_D = 4$. The remaining parameters are as in Figure 10; for $n = 50$, $V_A = 60$ SNU. Yellow and blue solid curves denote HHLA-assisted CVQSS for $n = 5$ and $n = 50$, respectively, and the corresponding dashed curves denote conventional CVQSS. The HHLA curves use the idealized gain-only heralding factor.

The preceding comparisons indicate that the gain should be adapted to the network size rather than fixed for all operating conditions. Figure 12 therefore uses separately selected values: $g_N = 4$ for $n = 5$, $g_N = 1.3$ for $n = 50$, and $g_N = 1.1$ for $n = 100$, with $G_D = 4$. In the displayed scan, the five-player maximum distance is approximately 112.5 km, representing an increase of about 22 km relative to conventional CVQSS. For $n = 50$, the HHLA-assisted distance is approximately 44 km, about 4.5 km longer than the reference. For $n = 100$, the improvement in maximum distance is only about 0.5 km, although the HHLA-assisted curve remains higher over part of the positive-rate region. These values demonstrate the benefit of node-dependent gain selection, but they are examples from the idealized gain-only grid scan rather than a universal optimization rule.

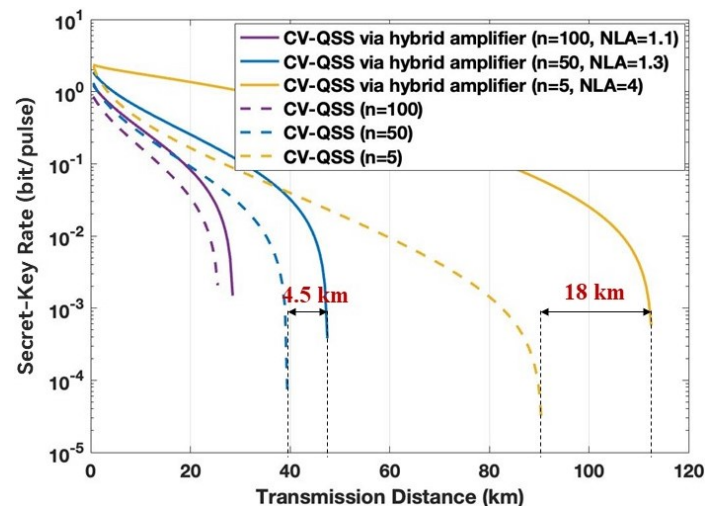


Figure 12. Heterodyne comparison using separately selected gains: $g_N = 4$ for $n = 5$, $g_N = 1.3$ for $n = 50$, and $g_N = 1.1$ for $n = 100$, with $G_D = 4$. Yellow, blue, and purple solid curves denote HHLA-assisted CVQSS for $n = 5$, 50, and 100, respectively; the corresponding dashed curves denote conventional CVQSS. The HHLA curves use the idealized gain-only heralding factor.

Taken together, Figures 5–12 show that the HHLA can improve the conditional channel and the transmitted-pulse rate in selected gain–distance regions, but the benefit decreases as the number of players grows and as the NLA gain becomes too large. The practical selection rule must therefore maximize $P_s K^{\text{acc}}$ under the physicality, cutoff, detector, and minimum-player-rate constraints, rather than maximize gain or transmission distance in isolation. The finite-cutoff results in Section 4.2 and Appendix B consequently provide the conservative basis for the conclusions, while the present figures retain the detailed gain-dependent behavior of the original simulations.

Appendix A gives the complete homodyne mutual information, Holevo bound, trusted receiver-noise model, physicality tests, cutoff-dependent heralding probability, and constrained gain optimization. Under the stated per-player excess-noise model, the optimized transmitted-pulse rate reaches the 10^{-6} bit/pulse reporting floor at approximately 25.5 km for $n = 100$.

5. Conclusions

We studied a dealer-side HHLA for sequential CVQSS and clarified the features that distinguish the multiparty problem from an amplifier-assisted point-to-point CVQKD link. The analysis (i) conditions parameter estimation and the Holevo bound on successful heralding, (ii) uses a cutoff-dependent acceptance probability in the throughput, (iii) applies the inverse gain once in the input-referred data processing, (iv) models all non-candidate players as a colluding adversarial set and takes the worst-player rate, (v) defines a con-

strained gain-and-cutoff optimization, and (vi) gives parallel heterodyne and homodyne covariance-matrix treatments.

The five-player heterodyne sensitivity analysis quantifies the effects of excess noise, receiver efficiency, electronic noise, reconciliation efficiency, modulation variance, injection loss, and the NLA cutoff; the complete scans are collected in Appendix B. A reproducible workflow, consolidated notation-and-parameter table, explicit matrix notation, and the derivation of the invariants used by the code are provided in Section 4.1 and Appendix C. Under the stated Gaussian-input cutoff model, the HHLA provides a modest rate improvement over part of the metropolitan regime, especially for inefficient detectors, but it does not robustly extend the maximum distance. At $\epsilon_0 = 0.010$ SNU, the advantage disappears at sufficiently long distance, and increasing the normalized cutoff reduces the heralding probability sharply. Appendix A gives a homodyne implementation that uses the total input-referred noise in I_{AD}^{hom} , rejects nonphysical complex solutions, and optimizes the transmitted-pulse rate over a constrained parameter grid. The resulting maximum reported distances are approximately 108, 42, and 25.5 km for $n = 5, 50$, and 100, respectively. These conclusions remain conditional on the asymptotic collective-attack model and on a Gaussian-equivalent description of accepted data. A composable finite-size proof, explicit treatment of finite-cutoff non-Gaussianity, authenticated active-insider verification, and experimental calibration of the HHLA are important directions for future work.

Author Contributions: Conceptualization, K.Z.; methodology, K.Z. and L.Z.; software, K.Z. and Y.Y.; validation, Y.G.; formal analysis, K.Z. and Y.Y.; investigation, K.Z.; resources, K.Z.; data curation, K.Z.; writing—original draft preparation, K.Z. and S.D.; writing—review and editing, Y.G. and K.Z.; visualization, Y.Y.; supervision, Y.G.; project administration, K.Z.; funding acquisition, K.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Scientific Research Fund of Hunan Provincial Education Department (Grant No. 22B0918) and the Social Science Foundation of Hunan Province (Grant No. 23JL018).

Data Availability Statement: The numerical data supporting the findings of this study are available from the corresponding author upon reasonable request.

Acknowledgments: The authors thank the anonymous reviewers for their constructive comments, which helped improve the clarity and reproducibility of this work.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Appendix A. Homodyne Security Model and Numerical Results

This appendix gives the complete homodyne calculation. It uses the same accepted-event equivalent channel as the heterodyne calculation but changes the receiver noise, mutual-information prefactor, and measurement-conditioned covariance matrix. The security statement remains asymptotic and collective-attack-based, and all rates are normalized per transmitted pulse.

Appendix A.1. Accepted Covariance Matrix and Receiver Noise

Let the accepted premeasurement covariance matrix be

$$\Gamma_{AD} = \begin{pmatrix} a\mathbf{I}_2 & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I}_2 \end{pmatrix}, \quad a = V, \quad b = T_g(V + \chi_{\text{line}}), \quad c = \sqrt{T_g(V^2 - 1)}. \quad (\text{A1})$$

For homodyne detection with an ideal phase-sensitive deterministic amplifier aligned with the measured quadrature, the trusted detector noise and total input-referred noise are [23,24]

$$\chi_{\text{hom}} = \frac{1 - \eta + v_{\text{el}}}{\eta G_D}, \quad (\text{A2})$$

$$\chi_{\text{tot}}^{\text{hom}} = \chi_{\text{line}} + \frac{\chi_{\text{hom}}}{T_g}. \quad (\text{A3})$$

The amplifier is assumed to be inside the dealer's calibrated receiver. Residual phase mismatch, nonzero phase-sensitive-amplifier noise, and calibration uncertainty must be included in v_D^{hom} or in the experimentally estimated excess noise in an implementation.

Appendix A.2. Mutual Information and Holevo Bound

Because only one quadrature is retained, the reverse-reconciliation mutual information is [23]

$$I_{AD}^{\text{hom}} = \frac{1}{2} \log_2 \left(\frac{V + \chi_{\text{tot}}^{\text{hom}}}{1 + \chi_{\text{tot}}^{\text{hom}}} \right). \quad (\text{A4})$$

Equation (A4) is evaluated with the *total* noise. Using $\frac{1}{2} \log_2 [a/(a - c^2/b)]$ with the pre-detection value $b = T_g(V + \chi_{\text{line}})$ omits χ_{hom} and is not the mutual information of the practical homodyne record.

Define the global symplectic invariants

$$A = a^2 + b^2 - 2c^2, \quad B = (ab - c^2)^2, \quad (\text{A5})$$

and

$$v_{1,2} = \sqrt{\frac{A \pm \sqrt{A^2 - 4B}}{2}}. \quad (\text{A6})$$

For the trusted homodyne detector model, the conditional invariants are

$$C_{\text{hom}} = \frac{A\chi_{\text{hom}} + V\sqrt{B} + T_g(V + \chi_{\text{line}})}{T_g(V + \chi_{\text{tot}}^{\text{hom}})}, \quad (\text{A7})$$

$$D_{\text{hom}} = \sqrt{B} \frac{V + \sqrt{B}\chi_{\text{hom}}}{T_g(V + \chi_{\text{tot}}^{\text{hom}})}, \quad (\text{A8})$$

and the nontrivial conditional symplectic eigenvalues are

$$\hat{v}_{3,4}^{\text{hom}} = \sqrt{\frac{C_{\text{hom}} \pm \sqrt{C_{\text{hom}}^2 - 4D_{\text{hom}}}}{2}}. \quad (\text{A9})$$

Here, D_{hom} is already the determinant-like invariant; it is not squared a second time in the discriminant. The remaining trusted ancillary eigenvalue is unity and contributes zero entropy. Consequently,

$$\chi_{DE}^{\text{hom}} = h(v_1) + h(v_2) - h(\hat{v}_3^{\text{hom}}) - h(\hat{v}_4^{\text{hom}}), \quad (\text{A10})$$

where $h(v)$ is defined below Equation (15). The transmitted-pulse rate is

$$R_{k,\text{hom}}^{\text{tx}} = P_s(g_N, \kappa) \left[\beta I_{AD,k}^{\text{hom}} - \chi_{DE,k}^{\text{hom}} \right]_+. \quad (\text{A11})$$

The same circular-Gaussian acceptance model as Equation (32) is used so that the homodyne and heterodyne curves have identical heralding normalization. This assumes that the MB-NLA acceptance record is generated and calibrated independently of the final quadrature choice; a homodyne-only postselection implementation would require a separately measured one-dimensional acceptance law.

Appendix A.3. Parameter Optimization and Validity Tests

The numerical code maximizes Equation (A11) independently at each calibrated distance, which produces a reproducible upper envelope rather than assigning gains after observing secret raw-key values. The scan uses

$$V_A \in \{1, 2, 5, 10, 20, 40\}, \quad G_D \in \{1, 2, 4, 8, 16\}, \quad \kappa = 2, \quad (\text{A12})$$

with g_N sampled in steps of 0.02 over

$$1 \leq g_N < \min \left[2, \sqrt{\frac{V_A + 2}{V_A}} \right]. \quad (\text{A13})$$

The upper bound enforces $g_N^2 \lambda^2 < 1$ with $\lambda^2 = V_A / (V_A + 2)$. The boundary $g_N = 1$ is retained because it identifies operating points at which postselection is counterproductive and the receiver reduces to deterministic phase-sensitive preamplification. For every trial point the code requires positive equivalent-channel denominators, real symplectic discriminants, $v_j \geq 1$, finite rates, and a transmitted-pulse rate above the reporting floor. It never applies $\text{real}()$ to a nonphysical complex result.

The common numerical parameters are $\gamma = 0.2$ dB/km, $\epsilon_0 = 0.001$ SNU per player, $v_{\text{el}} = 0.01$ SNU, $\eta = 0.5$, and $\beta = 0.98$. To isolate the receiver model and compare with the original fiber-only curves, $T_{\text{BS}} = 1$ is used here; injection-coupler loss is examined separately in Appendix B. A rate is reported only when $R^{\text{tx}} \geq 10^{-6}$ bit/pulse.

Appendix A.4. Homodyne Results

Figure A1 compares the optimized HHLA feasible-set envelope with a conventional homodyne receiver whose modulation variance is optimized over the same grid. The optimized receiver raises the rate over substantial short- and medium-distance intervals. At the longest distances, however, the optimum approaches weak NLA gain or the $g_N = 1$ boundary because the cutoff-dependent heralding penalty offsets the conditional gain.

Table A1. Selected homodyne results. The maximum distance is the last grid point with $R^{\text{tx}} \geq 10^{-6}$ bit/pulse.

n	$L_{\text{max}}^{\text{no amp}}$ (km)	$L_{\text{max}}^{\text{opt}}$ (km)	$R_{\text{no amp}}^{\text{tx}}$ at 20 km	$R_{\text{opt}}^{\text{tx}}$ at 20 km	Edge Optimum (g_N, G_D, V_A)
5	107.0	108.0	0.1513	0.2726	(1.18, 1, 5)
50	41.5	42.0	0.08187	0.1438	(1.08, 1, 10)
100	25.5	25.5	0.02810	0.04099	(1.04, 1, 20)

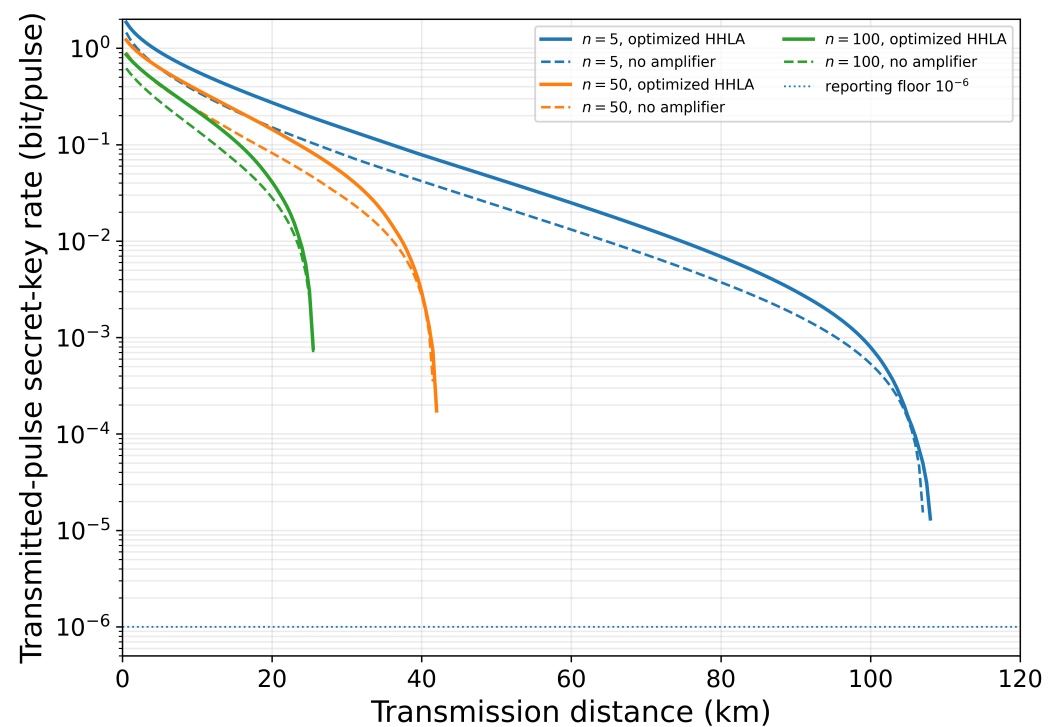


Figure A1. Homodyne transmitted-pulse rates for $n = 5, 50$, and 100 . Solid curves are the constrained HHLA feasible-set envelopes and dashed curves are no-amplifier references with V_A optimized over the same grid. All HHLA points include the cutoff-dependent P_s with $\kappa = 2$; the horizontal dotted line is the 10^{-6} bit/pulse reporting floor.

Appendix B. Detailed Sensitivity Analysis

This appendix contains the full sensitivity scans supporting the compact summary in Section 4.2. All curves use the same $n = 5$ heterodyne covariance calculation and the baseline stated there. Unless the scanned quantity is the cutoff itself, HHLA rates include $P_s = 0.6005$ for $g_N = 1.10$ and $\kappa = 2.0$.

Appendix B.1. Receiver Parameters

Figure A2 shows that deterministic preamplification is most beneficial when detector efficiency is low because it reduces the trusted receiver-noise penalty referred to the channel input. At 20 km, the HHLA/no-amplifier ratio is 1.438 for $\eta = 0.30$, 1.094 for $\eta = 0.50$, and 0.754 for $\eta = 0.90$. Changing v_{el} from 0 to 0.05 SNU produces a smaller change in the absolute HHLA rate within this trusted-receiver model.

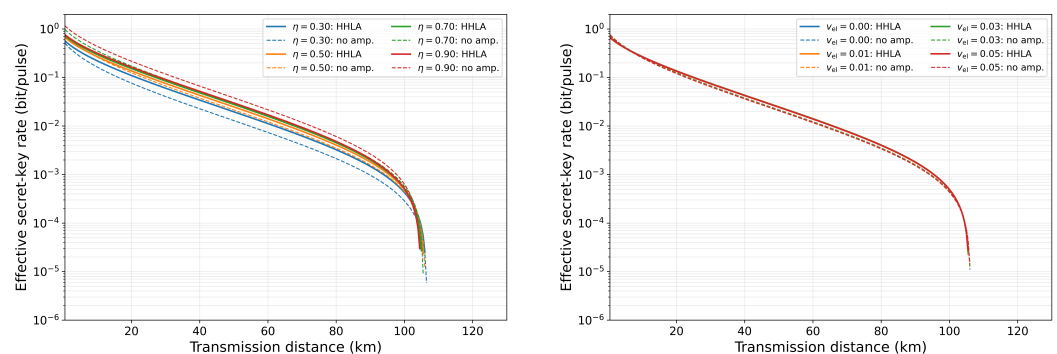


Figure A2. Receiver-parameter sensitivity of the $n = 5$ heterodyne model. Left: detector efficiency η . Right: electronic noise v_{el} . Solid curves include cutoff-dependent heralding; dashed curves show the corresponding no-amplifier reference.

Appendix B.2. Reconciliation, Modulation, and Injection Loss

Figure A3 reports reconciliation and modulation sensitivity. Reducing β from 0.98 to 0.90 lowers the HHLA maximum positive-rate distance from about 105.5 to 81.0 km. At 20 km, $V_A = 1, 5, 10$, and 20 SNU give HHLA rates of approximately 0.0673, 0.1367, 0.1537, and 0.1603 bit/pulse, respectively; however, the maximum distance is not monotonic and decreases to about 99 km at $V_A = 20$ SNU. Thus, V_A should be optimized jointly with the gains.

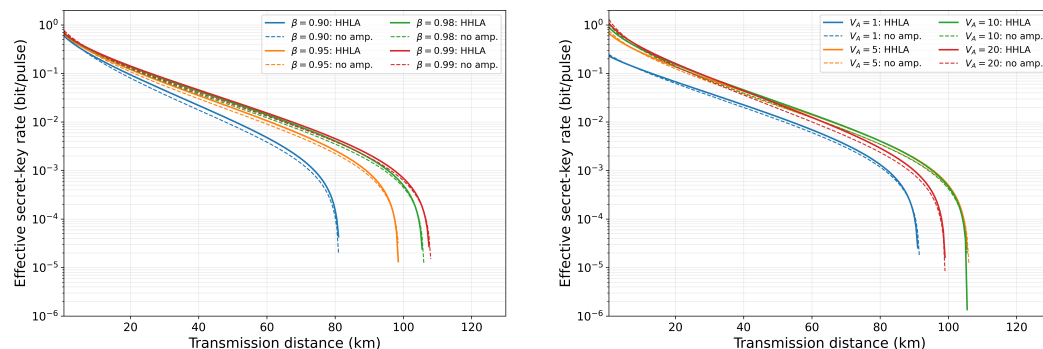


Figure A3. Sensitivity to reconciliation efficiency (left) and modulation variance (right). The baseline cutoff is $\kappa = 2.0$, corresponding to $P_s = 0.6005$ for $g_N = 1.10$.

To model the local injection couplers, the farthest player's channel transmittance is multiplied by T_{BS}^{n-1} and the contribution of player j by T_{BS}^{n-j} . Figure A4 shows that increasing T_{BS} from 0.95 to 0.995 raises the HHLA rate at 20 km from 0.1096 to 0.1405 bit/pulse and increases the maximum positive-rate distance from about 101 to 106 km.

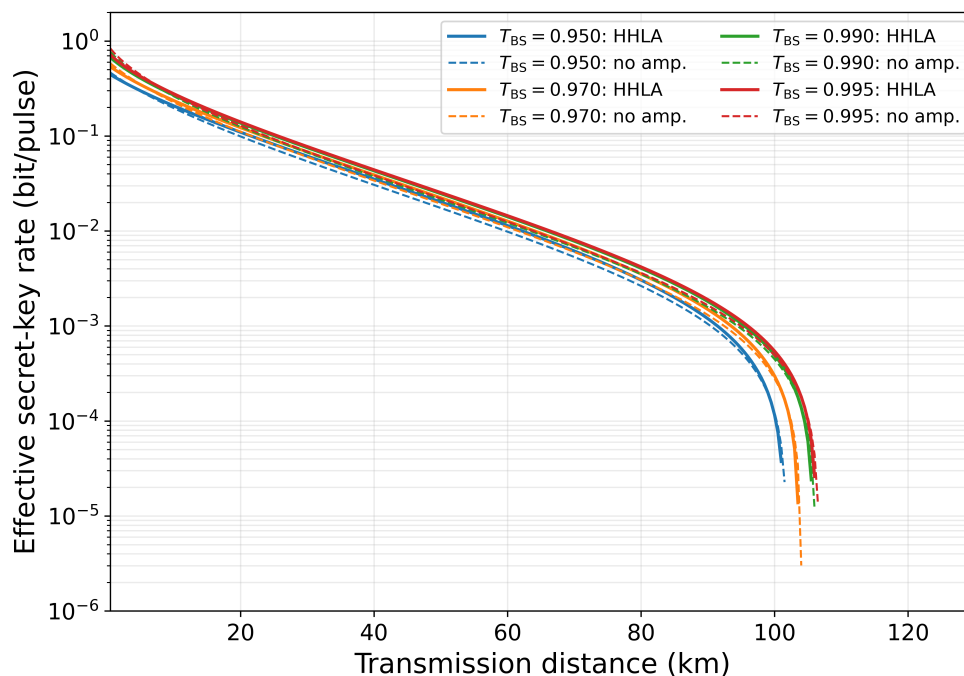


Figure A4. Sensitivity to the transmittance of each player injection beam splitter. Downstream insertion loss is included explicitly in the five-player path model.

Appendix B.3. Cutoff-Dependent Throughput

For $g_N = 1.10$, Equation (32) gives $P_s = 0.797, 0.601, 0.409$, and 0.254 for $\kappa = 1.5, 2.0, 2.5$, and 3.0 , respectively. Figure A5 shows the resulting transmitted-pulse rate. A cutoff

selected only to approximate the ideal NLA can eliminate the net throughput advantage, so the optimization in Section 4.3 must maximize $P_s K^{\text{acc}}$ rather than the conditional rate alone.

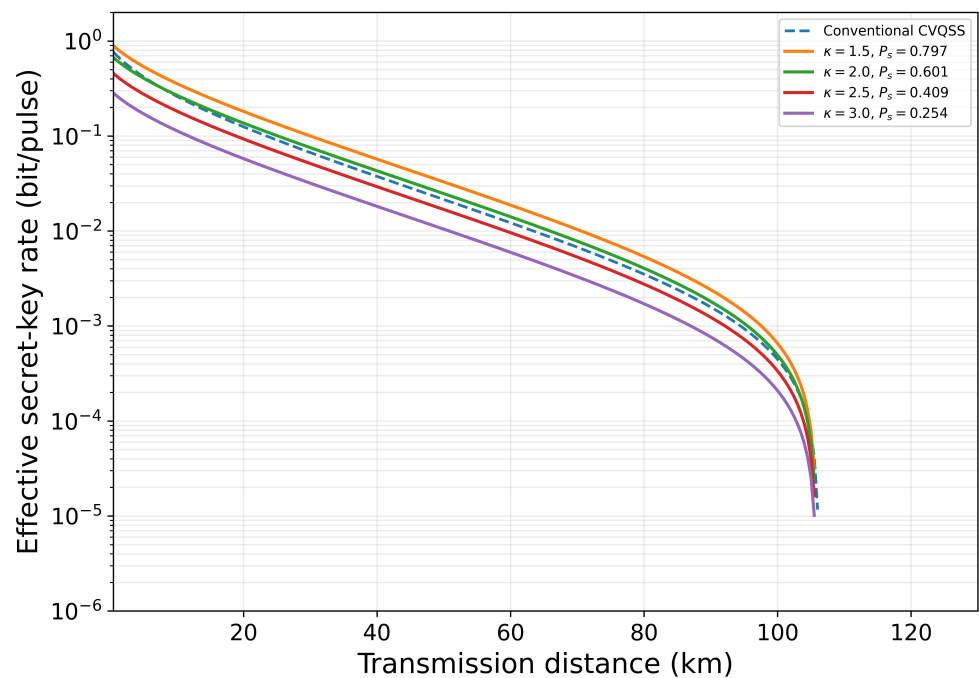


Figure A5. Effective transmitted-pulse throughput versus distance for $g_N = 1.10$ and four normalized cutoff values, together with conventional CVQSS.

Appendix B.4. Numerical Summary

Table A2. Selected numerical sensitivity results for the five-player heterodyne model. The HHLA values include $P_s = 0.6005$ unless the cutoff is the scanned parameter.

Operating Point	$R_{\text{HHLA}}^{\text{tx}}$ at 20 km	HHLA/No-Amplifier Ratio at 20 km	HHLA Maximum Distance (km)
$\epsilon_0 = 0.001$ SNU	0.1367	1.094	105.5
$\epsilon_0 = 0.010$ SNU	0.0697	1.044	43.0
$\eta = 0.30$	0.1099	1.438	106.0
$\eta = 0.90$	0.1630	0.754	104.5
$\beta = 0.90$	0.0939	1.171	81.0
$\beta = 0.99$	0.1420	1.088	107.5
$V_A = 1$ SNU	0.0673	1.080	91.0
$V_A = 20$ SNU	0.1603	1.135	99.0
$T_{\text{BS}} = 0.95$	0.1096	1.108	101.0
$T_{\text{BS}} = 0.995$	0.1405	1.092	106.0

Appendix C. Covariance-Matrix Invariants and Numerical Algorithm

Appendix C.1. Explicit Matrix Form and Notation

With the quadrature ordering $\mathbf{r}_{AD} = (q_A, p_A, q_D, p_D)^T$, Equation (15) is the explicit 4×4 matrix

$$\mathbf{\Gamma}_{AD} = \begin{bmatrix} a & 0 & c & 0 \\ 0 & a & 0 & -c \\ c & 0 & b & 0 \\ 0 & -c & 0 & b \end{bmatrix}. \quad (\text{A14})$$

The off-diagonal sign change follows from the matrix $\mathbf{Z} = \sigma_z = \text{diag}(1, -1)$. It encodes opposite correlations in the two conjugate quadratures; it is not multiplied as a vector, and no component-wise Pauli-vector notation is used.

Appendix C.2. Connection to the Global Invariants A and B

Write the covariance matrix in block form as $\mathbf{\Gamma}_{AD} = \begin{pmatrix} \mathbf{A}_0 & \mathbf{C}_0 \\ \mathbf{C}_0^\top & \mathbf{B}_0 \end{pmatrix}$, where $\mathbf{A}_0 = a\mathbf{I}_2$, $\mathbf{B}_0 = b\mathbf{I}_2$, and $\mathbf{C}_0 = c\mathbf{Z}$. Then,

$$\det \mathbf{A}_0 = a^2, \quad \det \mathbf{B}_0 = b^2, \quad \det \mathbf{C}_0 = c^2 \det \mathbf{Z} = -c^2. \quad (\text{A15})$$

Consequently, the two symplectic invariants used in the code are

$$A = \det \mathbf{A}_0 + \det \mathbf{B}_0 + 2 \det \mathbf{C}_0 = a^2 + b^2 - 2c^2, \quad (\text{A16})$$

$$B = \det \mathbf{\Gamma}_{AD} = (ab - c^2)^2. \quad (\text{A17})$$

The global symplectic eigenvalues follow directly as

$$v_{1,2} = \sqrt{\frac{A \pm \sqrt{A^2 - 4B}}{2}}. \quad (\text{A18})$$

Thus, the appearance of A and B in the MATLAB implementation is a compact representation of the determinant operations on the $\mathbf{I}_2$ and $\mathbf{Z}$ covariance blocks.

Appendix C.3. Measurement-Conditioned Invariants C_m and D_m

The dealer measurement is incorporated by the Gaussian conditional-covariance update

$$\mathbf{\Gamma}_{A|m} = \mathbf{A}_0 - \mathbf{C}_0(\mathbf{B}_0 + \mathbf{\Gamma}_m)^{-1}\mathbf{C}_0^\top, \quad (\text{A19})$$

where $\mathbf{\Gamma}_m$ is the calibrated trusted measurement-noise matrix. For heterodyne detection it is isotropic, whereas homodyne detection uses the measured-quadrature projector and the Moore–Penrose inverse. Because $\mathbf{Z}\mathbf{I}_2\mathbf{Z} = \mathbf{I}_2$ and $\mathbf{Z}^\top = \mathbf{Z}$, the block products reduce to scalar combinations of a , b , c , and the trusted noise. Including the trusted detector ancillas gives the heterodyne invariants used in the numerical implementation,

$$C_{\text{het}} = \frac{A(\chi_{\text{det}}^{\text{het}})^2 + B + 1 + 2\chi_{\text{det}}^{\text{het}}(a\sqrt{B} + b) + 2c^2}{[T_g(V + \chi_{\text{tot}}^{\text{het}})]^2}, \quad (\text{A20})$$

$$D_{\text{het}} = \left[\frac{a + \sqrt{B}\chi_{\text{det}}^{\text{het}}}{T_g(V + \chi_{\text{tot}}^{\text{het}})} \right]^2. \quad (\text{A21})$$

The conditional eigenvalues are

$$\tilde{v}_{3,4}^{\text{het}} = \sqrt{\frac{C_{\text{het}} \pm \sqrt{C_{\text{het}}^2 - 4D_{\text{het}}}}{2}}. \quad (\text{A22})$$

For homodyne detection, the corresponding C_{hom} and D_{hom} are given in Appendix A. In both cases, C_m is the conditional analogue of the symplectic trace invariant and D_m is determinant-like; the code therefore uses $C_m^2 - 4D_m$ and does not square D_m again.

Appendix C.4. Numerical Algorithm

For every calibration block, the implementation performs the following operations:

1. Fix n , the distance grid, detector calibration, noise estimates, and the admissible grids for (V_A, g_N, G_D, κ) using data independent of the secret raw key.
2. For each candidate player and distance, calculate T_k , the accumulated excess noise, the equivalent parameters (T_g, ϵ_g) , and the trusted detector noise.
3. Reject a parameter tuple if $g_N < 1$, $G_D < 1$, $g_N^2 \lambda^2 \geq 1$, an equivalent-channel denominator is non-positive, or the covariance matrix is nonphysical.
4. Evaluate P_s , construct Γ_{AD} , calculate A and B , and obtain $v_{1,2}$.
5. Select heterodyne or homodyne detection, calculate I_{kD} , form C_m and D_m , obtain the conditional symplectic eigenvalues, and evaluate χ_{DE} .
6. Compute $R_k^{\text{tx}} = P_s p_{\text{sift}}(1 - \text{FER})[\beta I_{kD} - \chi_{DE}]_+$ for every candidate honest player.
7. Form the multiparty objective $\min_k R_k^{\text{tx}}$ and retain the feasible tuple with the largest value. Store the rate, selected parameters, and all validity flags for reproducibility.

References

1. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613.
2. Blakley, G.R. Safeguarding cryptographic keys. In *Proceedings of the National Computer Conference*; AFIPS Press: Montvale, NJ, USA, 1979; Volume 48, pp. 313–317.
3. Hillery, M.; Bužek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829–1834.
4. Schmid, C.; Trojek, P.; Bourennane, M.; Kurtsiefer, C.; Żukowski, M.; Weinfurter, H. Experimental single qubit quantum secret sharing. *Phys. Rev. Lett.* **2005**, *95*, 230505.
5. Grice, W.P.; Qi, B. Quantum secret sharing using weak coherent states. *Phys. Rev. A* **2019**, *100*, 022339.
6. Hsu, J.L.; Chong, S.K.; Hwang, T.; Tsai, C.W. Dynamic quantum secret sharing. *Quantum Inf. Process.* **2013**, *12*, 331–344.
7. Yang, C.W.; Liu, P.Y.; Tsai, C.W.; Lin, J. An improved semi-quantum secret sharing protocol with enhanced verification to counter man-in-the-middle attacks. *Chin. J. Phys.* **2025**, *97*, 897–904.
8. Tsai, C.W.; Wang, C.H.; Lin, J.; Yang, C.W. Multiparty-to-multiparty mediated quantum secret sharing protocol in a restricted quantum environment. *EPJ Quantum Technol.* **2025**, *12*, 99.
9. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C. et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **2020**, *12*, 1012–1236.
10. Zhang, Y.; Li, Z.; Chen, Z.; Weedbrook, C.; Zhao, Y.; Wang, X.; Huang, Y.; Xu, C.; Zhang, X.; Wang, Z. et al. Continuous-variable QKD over 50 km commercial fiber. *Quantum Sci. Technol.* **2019**, *4*, 035006.
11. Lau, H.K.; Weedbrook, C. Quantum secret sharing with continuous-variable cluster states. *Phys. Rev. A* **2013**, *88*, 042313.
12. Kogias, I.; Xiang, Y.; He, Q.Y.; Adesso, G. Unconditional security of entanglement-based continuous-variable quantum secret sharing. *Phys. Rev. A* **2017**, *95*, 012315.
13. Peng, R.; Guo, Y.; Wang, Y.; Liao, Q. Decentralized continuous-variable quantum secret sharing. *Quantum Inf. Process.* **2023**, *22*, 368.
14. Liao, Q.; Fei, Z.; Huang, L.; Fu, X. Practical continuous-variable quantum secret sharing using local local oscillator. *Commun. Phys.* **2025**, *8*, 138.
15. Liao, Q.; Liu, X.; Ou, B.; Fu, X. Continuous-variable quantum secret sharing based on multi-ring discrete modulation. *IEEE Trans. Commun.* **2023**, *71*, 6051–6060.
16. Ferreyrol, F.; Barbieri, M.; Blandino, R.; Fossier, S.; Tualle-Brouri, R.; Grangier, P. Implementation of a nondeterministic optical noiseless amplifier. *Phys. Rev. Lett.* **2010**, *104*, 123603.
17. Ferreyrol, F.; Blandino, R.; Barbieri, M.; Tualle-Brouri, R.; Grangier, P. Experimental realization of a nondeterministic optical noiseless amplifier. *Phys. Rev. A* **2011**, *83*, 063801.
18. Zavatta, A.; Fiurášek, J.; Bellini, M. A high-fidelity noiseless amplifier for quantum light states. *Nat. Photonics* **2011**, *5*, 52–60.
19. Fiurášek, J.; Cerf, N.J. Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. *Phys. Rev. A* **2012**, *86*, 060302.
20. Walk, N.; Ralph, T.C.; Symul, T.; Lam, P.K. Security of continuous-variable quantum cryptography with Gaussian postselection. *Phys. Rev. A* **2013**, *87*, 020303.
21. Zhao, J.; Dias, J.; Haw, J.Y.; Symul, T.; Bradshaw, M.; Blandino, R.; Ralph, T.; Assad, S.M.; Lam, P.K. Quantum enhancement of signal-to-noise ratio with a heralded linear amplifier. *Optica* **2017**, *4*, 1421–1428.

22. Zhou, K.; Wu, X.; Mao, Y.; Chen, Z.; Liao, Q.; Guo, Y. Performance improvement of discretely modulated continuous-variable quantum key distribution with untrusted source via heralded hybrid linear amplifier. *Entropy* **2020**, *22*, 882.
23. Fossier, S.; Diamanti, E.; Debuisschert, T.; Tualle-Brouiri, R.; Grangier, P. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *J. Phys. B* **2009**, *42*, 114014.
24. Chrzanowski, H.M.; Walk, N.; Assad, S.M.; Janousek, J.; Hosseini, S.; Ralph, T.C.; Symul, T.; Lam, P.K. Measurement-based noiseless linear amplification for quantum communication. *Nat. Photonics* **2014**, *8*, 333–338.
25. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 070501.
26. Laudenbach, F.; Pacher, C.; Fung, C.H.F.; Poppe, A.; Peev, M.; Schrenk, B.; Hentschel, M.; Walther, P.; Hübel, H. Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations. *Adv. Quantum Technol.* **2018**, *1*, 1800011.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.