

# Parameter-Based Channel Estimation for OFDM CV-QKD Systems With CRLB Benchmarking and Secret Key Rate Analysis

Mohammed Kamel AbuFoul and Salama Ikki

Electrical and Computer Engineering Department, Lakehead University, Thunder Bay, ON P7B 5E1, Canada

**Abstract**—This paper develops a parameter-based channel estimation framework for OFDM Continuous-Variable Quantum Key Distribution (CV-QKD). Rather than estimating effective channel coefficients or relying on interpolation from revealed subcarriers, the proposed approach characterizes the channel through its physical propagation parameters, delay and complex gain, and reconstructs the full frequency response from them. A maximum-likelihood estimator is formulated over the revealed subcarriers, with the complex gain obtained in closed form for each candidate delay, reducing the search to one dimension. The Cramér–Rao lower bound is derived as a fundamental benchmark. Simulation results confirm that the proposed reconstruction improves channel accuracy and enhances the secret key rate with fewer revealed subcarriers.

**Index Terms**—OFDM CV-QKD, Quantum Communication, Channel Estimation, Maximum-Likelihood Estimation, Cramér–Rao Lower Bound, Secret Key Rate.

## I. INTRODUCTION

Continuous-Variable Quantum Key Distribution (CV-QKD) is a promising candidate for high-rate quantum-secure communication because it is compatible with coherent detection and standard optical components. As CV-QKD moves toward wireless and terahertz environments, the channel becomes harder to characterize due to path loss, frequency selectivity, turbulence, and mobility [1], and the Secret Key Rate (SKR) depends not only on the reconciliation efficiency but also on the quality of channel information available to the legitimate parties [2]. Orthogonal Frequency Division Multiplexing (OFDM) is well suited to frequency-selective CV-QKD links because it decomposes the channel into narrowband subcarriers and naturally supports pilot-based estimation and equalization [3]. Conventional OFDM channel estimation reveals a subset of subcarriers and interpolates the rest, but interpolation errors accumulate when the channel is highly selective or pilots are scarce. In CV-QKD this matters more than in classical systems because every revealed symbol is a resource consumed from key generation [4]. A parameter-based approach avoids this by estimating the underlying physical propagation parameters and reconstructing the full channel response from them.

Recent work has extended CV-QKD to wireless, free-space optical (FSO), satellite, UAV-assisted, and terahertz channels. OFDM- and OTFS-assisted CV-QKD over doubly selective THz channels was studied in [5]–[7], showing that multicarrier waveforms and delay-Doppler processing significantly affect the SKR. FSO and satellite systems have been analyzed

with respect to atmospheric attenuation, turbulence, pointing errors, finite-size effects, and phase-reference attacks [8]–[11]. On the processing side, reconciliation improvements [12], [13], high-speed polarization-multiplexed experiments [14], and RIS-assisted MIMO THz channel estimation [15] have all demonstrated that imperfect CSI degrades the SKR. However, these works either adopt statistical channel models or estimate effective channel coefficients, without deriving estimation-theoretic bounds for the underlying physical parameters of an OFDM CV-QKD link.

This paper addresses that gap by developing a parameter-based channel estimation framework for OFDM CV-QKD. The physical channel parameters are estimated from revealed subcarriers, the full frequency response is reconstructed, and the Cramér–Rao lower bound (CRLB) is derived as a fundamental benchmark. To the best of the authors’ knowledge, this is the first work to study physical parameter estimation and CRLB benchmarking for OFDM CV-QKD channels. The main contributions are:

- *Parameter-based OFDM CV-QKD channel estimation framework:* The channel is characterized through its propagation delays, and complex gains rather than independent subcarrier coefficients, enabling full channel reconstruction from a small number of revealed subcarriers.
- *MLE-based reconstruction with reduced search complexity:* Maximum-likelihood estimation is formulated over the revealed subcarriers. The complex gain is obtained in closed form for each candidate delay, reducing the nonlinear problem to a one-dimensional delay search.
- *CRLB for physical channel parameters:* The CRLB is derived for the physical parameters and propagated via the transformation rule to bound the reconstructed channel estimation error.
- *SKR enhancement through improved channel estimation:* This work connects channel-estimation accuracy directly to SKR performance, demonstrating that the parameter-based approach improves the SKR independently of the reconciliation algorithm.

*Organization:* The remainder of this paper is organized as follows. Section II presents the OFDM CV-QKD system model and signaling framework. Section III derives the CRLB benchmark for the physical channel parameters. Section IV

develops the MLE-based channel estimation and reconstruction algorithm. The SKR analysis under estimated channel responses is presented in Section V. Simulation results are given in Section VI, and Section VII concludes the paper.

*Notation:* Scalars are denoted by lowercase letters, vectors by bold lowercase, and matrices by bold uppercase.  $(\cdot)^T$  and  $(\cdot)^H$  denote the transpose and Hermitian transpose, respectively.  $\mathbf{A} = \text{diag}(\mathbf{a})$  is a diagonal matrix with  $\mathbf{a}$  on its main diagonal, and  $[\mathbf{A}]_{i,j}$  denotes its  $(i, j)$ -th entry.  $\Re\{\cdot\}$  and  $\Im\{\cdot\}$  denote the real and imaginary parts.  $|\cdot|$  is the modulus of a scalar and  $\|\cdot\|_2$  the Euclidean norm of a vector.  $\mathcal{CN}(\mu, \sigma^2)$  denotes a circularly symmetric complex Gaussian distribution with mean  $\mu$  and variance  $\sigma^2$ , and  $\mathbb{E}[\cdot]$  denotes the statistical expectation.

## II. SYSTEM MODEL AND SIGNALING

The considered CV-QKD system operates over a frequency-selective wireless channel using OFDM signaling with heterodyne detection, as illustrated in Fig. 1. The channel is assumed static over one OFDM block, and a subset of transmitted symbols is publicly revealed over an authenticated channel to support parameter estimation.

*OFDM Signaling:* Alice modulates  $M$  subcarriers with i.i.d. complex Gaussian symbols,

$$x[m] \sim \mathcal{CN}(0, V_s), \quad m \in [0, M-1], \quad (1)$$

where  $V_s$  is the modulation variance. No deterministic pilots are used; instead, a subset of data symbols is revealed post-transmission for channel estimation, consistent with standard CV-QKD protocols.

*Multipath Channel Model:* The channel consists of  $D$  propagation paths. Path  $d$  is characterized by amplitude  $\rho_d$ , phase  $\phi_d$ , and delay  $\tau_d$ , giving the frequency-domain response

$$H[m] = \sum_{d=1}^D \rho_d e^{j\phi_d} e^{-j2\pi m \Delta f \tau_d}. \quad (2)$$

Large-scale propagation loss is captured by the transmittance

$$T \triangleq 10^{-\frac{\alpha L}{10}}, \quad (3)$$

where  $\alpha$  is the atmospheric attenuation coefficient (dB/km) and  $L$  is the Alice–Bob distance (km). The path weights  $\{\rho_d\}$  account for relative small-scale gain variations. Bob’s received signal on subcarrier  $m$  follows a beam-splitter model,

$$y[m] = \sqrt{T} H[m] x[m] + v[m]. \quad (4)$$

*Noise Model:* The noise term combines trusted Alice-side preparation noise and untrusted Eve-injected noise,

$$v[m] = \sqrt{T} H[m] x_0[m] + \sqrt{1-T} s_E[m], \quad (5)$$

where  $x_0[m] \sim \mathcal{CN}(0, \sigma_{x_0}^2)$  and  $s_E[m] \sim \mathcal{CN}(0, \sigma_E^2)$  are mutually independent and independent of  $x[m]$ . Conditioned on  $H[m]$ , the noise is zero-mean proper complex Gaussian with variance

$$\sigma_v^2[m] = T |H[m]|^2 \sigma_{x_0}^2 + (1-T) \sigma_E^2. \quad (6)$$

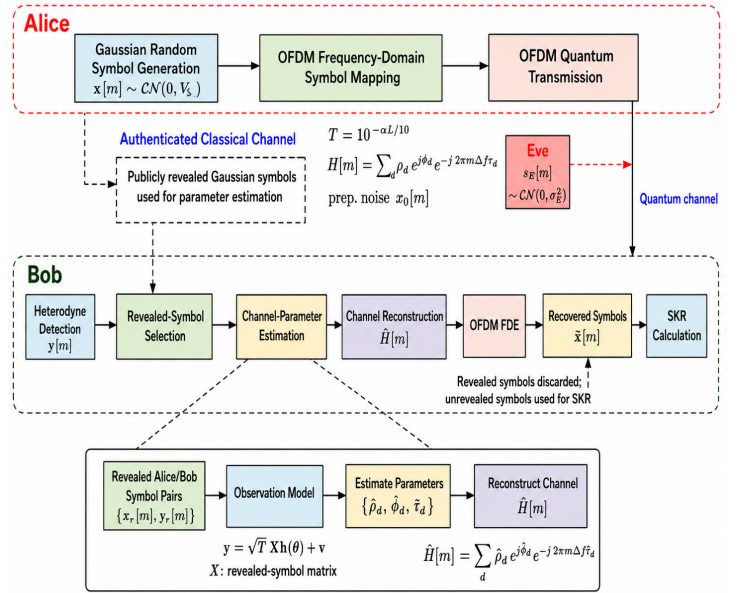


Fig. 1: CV-QKD protocol diagram of the OFDM parameter-based channel-estimation-aided scheme.

*Vector Model:* Stacking over one OFDM block with  $\mathbf{y}, \mathbf{h}(\boldsymbol{\theta}) \in \mathbb{C}^{M \times 1}$  and  $\mathbf{X} = \text{diag}(x[0], \dots, x[M-1])$ , the received signal is

$$\mathbf{y} = \sqrt{T} \mathbf{X} \mathbf{h}(\boldsymbol{\theta}) + \mathbf{v}, \quad (7)$$

where  $\mathbf{v} \sim \mathcal{CN}(\mathbf{0}, \mathbf{C}_v)$ ,  $\mathbf{C}_v = \text{diag}(\sigma_v^2[0], \dots, \sigma_v^2[M-1])$ , and the unknown deterministic parameter vector is

$$\boldsymbol{\theta} \triangleq [\rho_1, \phi_1, \tau_1, \dots, \rho_D, \phi_D, \tau_D]^T \in \mathbb{R}^{3D \times 1}. \quad (8)$$

The modulation variance  $V_s$  is known at Alice;  $\mathbf{y}$  and the revealed symbols are available at Bob;  $\boldsymbol{\theta}$  is estimated from the revealed subset over the authenticated public channel.

## III. PERFORMANCE BENCHMARK ANALYSIS

This section derives the CRLB for the parameter vector  $\boldsymbol{\theta}$  in (8) under the Eve-noise-dominant regime, which represents the worst case for a secure link. When the untrusted noise component dominates,  $(1-T)\sigma_E^2 \gg T|H[m]|^2\sigma_{x_0}^2$ , the subcarrier noise variance in (6) reduces to a subcarrier-independent constant,

$$\sigma_v^2[m] \approx (1-T)\sigma_E^2 \triangleq \sigma_c^2, \quad (9)$$

and the observation on each revealed subcarrier becomes  $(y[m] | x[m], \boldsymbol{\theta}) \sim \mathcal{CN}(\sqrt{T}x[m]H[m], \sigma_c^2)$ . Since  $\sigma_c^2$  does not depend on  $\boldsymbol{\theta}$ , the Fisher Information Matrix (FIM),  $\mathbf{J}(\boldsymbol{\theta})$ , is determined entirely by the mean gradient, giving

$$\mathbf{J}_{ij} = \frac{2T}{\sigma_c^2} \Re \left\{ \sum_{m \in \mathcal{M}_r} |x[m]|^2 \frac{\partial H^*[m]}{\partial \theta_i} \frac{\partial H[m]}{\partial \theta_j} \right\}, \quad (10)$$

where  $\mathcal{M}_r$  is the set of revealed subcarrier indices.

*Single-Path Benchmark:* For a single propagation path,  $H[m] = \rho e^{j\phi} e^{-j\omega_m \tau}$  with  $\omega_m = 2\pi m \Delta f$ , and  $\boldsymbol{\theta} =$

$[\tau, \phi, \rho]^T$ . The partial derivatives of  $\mu[m] = \sqrt{T}x[m]H[m]$  are

$$\frac{\partial \mu[m]}{\partial \rho} = \frac{\mu[m]}{\rho}, \quad \frac{\partial \mu[m]}{\partial \phi} = j\mu[m], \quad \frac{\partial \mu[m]}{\partial \tau} = -j\omega_m \mu[m]. \quad (11)$$

Defining the energy-weighted subcarrier sums

$$E_0 = \sum_{m \in \mathcal{M}_r} |x[m]|^2, \quad E_1 = \sum_{m \in \mathcal{M}_r} \omega_m |x[m]|^2, \quad E_2 = \sum_{m \in \mathcal{M}_r} \omega_m^2 |x[m]|^2. \quad (12)$$

and using  $|\mu[m]|^2 = T\rho^2|x[m]|^2$ , the single-path FIM evaluates to

$$\mathbf{J}(\tau, \phi, \rho) = \frac{2T\rho^2}{\sigma_c^2} \begin{bmatrix} E_2 & -E_1 & 0 \\ -E_1 & E_0 & 0 \\ 0 & 0 & E_0/\rho^2 \end{bmatrix}, \quad (13)$$

and the CRLB follows as  $\text{CRLB}(\boldsymbol{\theta}) = \mathbf{J}^{-1}(\tau, \phi, \rho)$ .

*Generalized Multipath FIM:* For a  $D$ -path channel with  $\boldsymbol{\theta} = [\boldsymbol{\theta}_1^T, \dots, \boldsymbol{\theta}_D^T]^T$ ,  $\boldsymbol{\theta}_d = [\tau_d, \phi_d, \rho_d]^T$ , the FIM has a symmetric block structure

$$\mathbf{J} = \begin{bmatrix} \mathbf{J}_{1,1} & \cdots & \mathbf{J}_{1,D} \\ \vdots & \ddots & \vdots \\ \mathbf{J}_{D,1} & \cdots & \mathbf{J}_{D,D} \end{bmatrix}, \quad (14)$$

where the  $(d, d')$  cross-block is

$$\mathbf{J}_{d,d'} = \frac{2T}{\sigma_c^2} \sum_{m \in \mathcal{M}_r} |x[m]|^2 \Re \left\{ \Gamma_{d,d'}[m] \mathbf{p}_d[m] \mathbf{p}_{d'}^H[m] \right\}, \quad (15)$$

with the mutual overlap phasor  $\Gamma_{d,d'}[m] = e^{j(\phi_{d'} - \phi_d)} e^{-j\omega_m(\tau_{d'} - \tau_d)}$  and the gradient vector  $\mathbf{p}_d[m] = [\rho_d \omega_m, -\rho_d, -j]^T$ . When paths are well separated in delay, the rapid phase oscillations of  $\Gamma_{d,d'}[m]$  across  $\mathcal{M}_r$  average to zero, decoupling the cross-blocks and reducing each diagonal block to the single-path result in (13).

*CRLB of the Channel Frequency Response:* The CRLB for the full reconstructed response  $\mathbf{h}(\boldsymbol{\theta}) \in \mathbb{C}^{M \times 1}$  is obtained via the Jacobian transformation as:

$$\text{CRLB}_{\mathbf{h}}(\boldsymbol{\theta}) = \boldsymbol{\Gamma}_{\mathbf{h}}(\boldsymbol{\theta}) \mathbf{J}^{-1}(\boldsymbol{\theta}) \boldsymbol{\Gamma}_{\mathbf{h}}^T(\boldsymbol{\theta}), \quad (16)$$

where  $\boldsymbol{\Gamma}_{\mathbf{h}}(\boldsymbol{\theta}) \in \mathbb{R}^{1 \times 3D}$  is the Jacobian of  $\mathbf{h}$  with respect to  $\boldsymbol{\theta}$ .

#### IV. MAXIMUM LIKELIHOOD ESTIMATION

Using the revealed subcarrier set  $\mathcal{M}_r$  with  $M_r = |\mathcal{M}_r|$ , let  $\mathbf{y}_r \in \mathbb{C}^{M_r \times 1}$  and  $\mathbf{X}_r \in \mathbb{C}^{M_r \times M_r}$  collect the received samples and their corresponding diagonal symbol matrix. Each path complex gain is defined as  $\zeta_d \triangleq \rho_d e^{j\phi_d}$ , giving the gain vector  $\boldsymbol{\zeta} = [\zeta_1, \dots, \zeta_D]^T$ . The delay steering matrix  $\mathbf{S}_r(\boldsymbol{\tau}) \in \mathbb{C}^{M_r \times D}$  has entries  $[\mathbf{S}_r(\boldsymbol{\tau})]_{k,d} = e^{-j\omega_{m_k} \tau_d}$ , and the dictionary matrix  $\mathbf{A}_r(\boldsymbol{\tau}) \triangleq \mathbf{X}_r \mathbf{S}_r(\boldsymbol{\tau})$  compactly represents the revealed observation model as

$$\mathbf{y}_r = \sqrt{T} \mathbf{A}_r(\boldsymbol{\tau}) \boldsymbol{\zeta} + \mathbf{v}_r. \quad (17)$$

---

#### Algorithm 1 Differential Evolution Algorithm

---

**Require:**  $\mathbf{y}_r, \mathbf{X}_r$ , population size  $N_p$ , generations  $G$ , search region  $\mathcal{T} = [0, \tau_{\max}]^D$ , crossover rate  $C_r$ , mutation factor  $\mu$ , separation threshold  $\Delta_{\min}$ , penalty weight  $\lambda$ .

**Ensure:**  $\hat{\boldsymbol{\tau}}, \hat{\boldsymbol{\zeta}}$ .

- 1: **Initialisation:** For  $i = 1, \dots, N_p$ , draw  $\tau_{i,d}^{(0)} \sim \mathcal{U}(0, \tau_{\max})$  and sort:  $\boldsymbol{\tau}_i^{(0)} \leftarrow \text{sort}(\tau_{i,d}^{(0)})$ .
  - 2: **for**  $g = 0$  **to**  $G - 1$  **do**
  - 3:   **for**  $i = 1$  **to**  $N_p$  **do**
  - 4:     Evaluate  $\tilde{\mathcal{J}}_c(\boldsymbol{\tau}_i^{(g)})$  using (19).
  - 5:     **Mutation:** Pick distinct  $r_1, r_2, r_3 \neq i$ ; form  $\mathbf{z}_i^{(g)} = \boldsymbol{\tau}_{r_1}^{(g)} + \mu(\boldsymbol{\tau}_{r_2}^{(g)} - \boldsymbol{\tau}_{r_3}^{(g)})$ .
  - 6:     **Crossover:** Draw  $d_{\text{rand}} \sim \mathcal{U}(\{1, \dots, D\})$ ; for each  $d$ , set  $u_{i,d}^{(g)} = z_{i,d}^{(g)}$  if  $q_d \leq C_r$  or  $d = d_{\text{rand}}$ , else  $u_{i,d}^{(g)} = \tau_{i,d}^{(g)}$ .
  - 7:     **Clip & Sort:**  $u_{i,d}^{(g)} \leftarrow \text{clip}(u_{i,d}^{(g)}, 0, \tau_{\max})$ ;  $\mathbf{u}_i^{(g)} \leftarrow \text{sort}(\mathbf{u}_i^{(g)})$ .
  - 8:     **Selection:**  $\boldsymbol{\tau}_i^{(g+1)} \leftarrow \mathbf{u}_i^{(g)}$  if  $\tilde{\mathcal{J}}_c(\mathbf{u}_i^{(g)}) \leq \tilde{\mathcal{J}}_c(\boldsymbol{\tau}_i^{(g)})$ , else  $\boldsymbol{\tau}_i^{(g+1)} \leftarrow \boldsymbol{\tau}_i^{(g)}$ .
  - 9:   **end for**
  - 10: **end for**
  - 11: **Output:**  $\hat{\boldsymbol{\tau}} = \arg \min_i \tilde{\mathcal{J}}_c(\boldsymbol{\tau}_i^{(G)})$ ;  $\hat{\boldsymbol{\zeta}} = \hat{\boldsymbol{\zeta}}(\hat{\boldsymbol{\tau}})$  via (19).
- 

*Concentrated MLE Formulation:* Under the Eve-noise-dominant condition established in Section III,  $\mathbf{v}_r \sim \mathcal{CN}(\mathbf{0}, \sigma_c^2 \mathbf{I}_{M_r})$ , so maximizing the log-likelihood reduces to the nonlinear least-squares problem

$$(\hat{\boldsymbol{\tau}}, \hat{\boldsymbol{\zeta}}) = \arg \min_{\boldsymbol{\tau}, \boldsymbol{\zeta}} \|\mathbf{y}_r - \sqrt{T} \mathbf{A}_r(\boldsymbol{\tau}) \boldsymbol{\zeta}\|_2^2. \quad (18)$$

Since (17) is linear in  $\boldsymbol{\zeta}$  for any fixed  $\boldsymbol{\tau}$ , the complex gains are obtained in closed form as

$$\hat{\boldsymbol{\zeta}}(\boldsymbol{\tau}) = \frac{1}{\sqrt{T}} (\mathbf{S}_r^H \mathbf{X}_r^H \mathbf{X}_r \mathbf{S}_r)^{-1} \mathbf{S}_r^H \mathbf{X}_r^H \mathbf{y}_r, \quad (19)$$

requiring  $M_r \geq D$  for identifiability. Substituting (19) back into (18) concentrates the search over delays only,

$$\hat{\boldsymbol{\tau}} = \arg \max_{\boldsymbol{\tau} \in \mathcal{T}} \mathbf{y}_r^H \mathbf{P}_{\mathbf{A}}(\boldsymbol{\tau}) \mathbf{y}_r, \quad (20)$$

where  $\mathbf{P}_{\mathbf{A}}(\boldsymbol{\tau}) = \mathbf{A}_r(\mathbf{A}_r^H \mathbf{A}_r)^{-1} \mathbf{A}_r^H$  is the projection onto the column space of  $\mathbf{A}_r(\boldsymbol{\tau})$  and  $\mathcal{T} = \{\boldsymbol{\tau} \in \mathbb{R}^D : 0 \leq \tau_d \leq \tau_{\max}\}$ . Once  $\hat{\boldsymbol{\tau}}$  is found, the path parameters and the full channel response follow directly from  $\hat{\boldsymbol{\zeta}} = \hat{\boldsymbol{\zeta}}(\hat{\boldsymbol{\tau}})$ ,  $\hat{\rho}_d = |\hat{\zeta}_d|$ ,  $\hat{\phi}_d = \angle \hat{\zeta}_d$ , and

$$\hat{H}[m] = \sum_{d=1}^D \hat{\zeta}_d e^{-j2\pi m \Delta f \hat{\tau}_d}. \quad (21)$$

*Differential Evolution Delay Search:* The objective in (20) is non-convex and multi-modal, so a global Differential Evolution (DE) routine is used to avoid local optima. The full procedure is given in Algorithm 1. Briefly, a population of  $N_p$  candidate delay vectors is initialised uniformly over  $\mathcal{T}$  and sorted to enforce path ordering. At each generation, mutation,

binomial crossover, boundary clipping, and greedy selection are applied. The fitness function augments the residual energy with a separation penalty to prevent path collapse,

$$\tilde{\mathcal{J}}_c(\tau) = \|\mathbf{y}_r - \sqrt{T} \mathbf{A}_r \hat{\boldsymbol{\zeta}}(\tau)\|_2^2 + \lambda \sum_{d=1}^{D-1} [\max(0, \Delta_{\min} - (\tau_{d+1} - \tau_d))]^2. \quad (22)$$

After  $G$  generations, the best survivor gives  $\hat{\tau}$ , from which  $\hat{\boldsymbol{\zeta}}$  is recovered via (19).

## V. SECRET KEY RATE ANALYSIS WITH ESTIMATED CHANNEL RESPONSE

This section connects channel-estimation accuracy to the achievable SKR. All system and reconciliation parameters are fixed across the compared schemes; only the channel response used by Bob for Frequency-Domain Equalization (FDE) changes. Following the notation of Section II, the preparation-noise variance is denoted here as  $V_0 = \sigma_{x_0}^2$ .

*Estimated-CSI FDE Model:* Let  $\hat{H}_q[m]$  denote the channel response available at Bob, where  $q \in \{\text{Perfect, Param, Interp}\}$  corresponds to perfect CSI, the proposed parameter-based reconstruction, and conventional interpolation, respectively. Including heterodyne detection with efficiency  $\eta$  and trusted detector noise  $n_{\text{det}}[m] \sim \mathcal{CN}(0, S)$ , Bob applies single-tap FDE as

$$\hat{x}_q[m] = \frac{\sqrt{\eta} y[m] + \sqrt{1-\eta} n_{\text{det}}[m]}{\sqrt{\eta T} \hat{H}_q[m]}. \quad (23)$$

Substituting (4)–(5) into (23) and defining the mismatch factor  $\mu_q[m] \triangleq H[m]/\hat{H}_q[m]$ , the equalized output takes the unit-gain form

$$\hat{x}_q[m] = x[m] + \tilde{n}_q[m], \quad (24)$$

where the effective noise is

$$\begin{aligned} \tilde{n}_q[m] = & (\mu_q[m] - 1)x[m] + \mu_q[m]x_0[m] \\ & + \frac{\sqrt{1-T}}{\sqrt{T} \hat{H}_q[m]} s_E[m] + \frac{\sqrt{1-\eta}}{\sqrt{\eta T} \hat{H}_q[m]} n_{\text{det}}[m]. \end{aligned} \quad (25)$$

The first term in (25) is the CSI-mismatch noise; it vanishes under perfect CSI and grows as  $\hat{H}_q[m]$  deviates from  $H[m]$ . The corresponding effective noise variance is

$$\begin{aligned} \sigma_{\text{eff},q}^2[m] = & |\mu_q[m] - 1|^2 V_s + |\mu_q[m]|^2 V_0 \\ & + \frac{1-T}{T|\hat{H}_q[m]|^2} \sigma_E^2 + \frac{1-\eta}{\eta T|\hat{H}_q[m]|^2} S. \end{aligned} \quad (26)$$

which includes the CSI-induced excess noise

$$\xi_{\text{CSI},q}[m] = \frac{|\varepsilon_q[m]|^2}{|\hat{H}_q[m]|^2} V_s, \quad \varepsilon_q[m] \triangleq \hat{H}_q[m] - H[m]. \quad (27)$$

This term is absent if  $H[m]$  is simply substituted into a perfect-CSI SKR expression, making such an approach overly optimistic.

*Mutual Information and Holevo Bound:* Under heterodyne detection, the Alice–Bob mutual information per complex symbol on subcarrier  $m$  is

$$I_{AB,q}[m] = \log_2 \left( 1 + \frac{V_s}{\sigma_{\text{eff},q}^2[m]} \right), \quad (28)$$

and its average over the unrevealed data subcarriers  $\mathcal{M}_d$  is  $\bar{I}_{AB,q} = |\mathcal{M}_d|^{-1} \sum_{m \in \mathcal{M}_d} I_{AB,q}[m]$ . The parameter-estimation overhead factor is  $\gamma_{\text{PE}} = |\mathcal{M}_d|/M$ .

The Holevo information under a collective Gaussian attack is evaluated from the per-subcarrier covariance matrix

$$\mathbf{V}_{AB,q}[m] = \begin{bmatrix} a_q[m] \mathbf{I}_2 & c_q[m] \mathbf{Z} \\ c_q[m] \mathbf{Z} & b_q[m] \mathbf{I}_2 \end{bmatrix}, \quad (29)$$

with  $\mathbf{Z} = \text{diag}(1, -1)$  and entries

$$a_q[m] = V, \quad b_q[m] = V_s + \sigma_{\text{eff},q}^2[m], \quad c_q[m] = \sqrt{V^2 - 1}. \quad (30)$$

where  $V = V_s + V_0$ . Imperfect channel estimation enters through  $b_q[m]$  via the excess noise in (27). The symplectic eigenvalues are

$$\lambda_{1,q}^2[m], \lambda_{2,q}^2[m] = \frac{\Delta_q[m] \pm \sqrt{\Delta_q^2[m] - 4\mathcal{D}_q^2[m]}}{2}, \quad (31)$$

where  $\Delta_q[m] = a_q^2 + b_q^2 - 2c_q^2$  and  $\mathcal{D}_q[m] = a_q b_q - c_q^2$ . The conditional eigenvalue under heterodyne detection is

$$\lambda_{3,q}[m] = a_q[m] - \frac{c_q^2[m]}{b_q[m] + 1}, \quad (32)$$

where  $+1$  accounts for the heterodyne shot-noise unit. The Holevo information per subcarrier follows from the bosonic entropy  $G(x) = \frac{x+1}{2} \log_2 \frac{x+1}{2} - \frac{x-1}{2} \log_2 \frac{x-1}{2}$  as

$$\chi_{BE,q}[m] = G(\lambda_{1,q}[m]) + G(\lambda_{2,q}[m]) - G(\lambda_{3,q}[m]), \quad (33)$$

with average  $\bar{\chi}_{BE,q} = |\mathcal{M}_d|^{-1} \sum_{m \in \mathcal{M}_d} \chi_{BE,q}[m]$ .

*Achievable SKR:* The normalized SKR for estimation method  $q$  is

$$K_q = \gamma_{\text{PE}}(1 - P_B) [\beta \bar{I}_{AB,q} - \bar{\chi}_{BE,q} - \Delta(N_{\text{privacy}})]^+, \quad (34)$$

where  $\beta$  is the reconciliation efficiency,  $P_B$  the block error probability, and  $\Delta(N_{\text{privacy}})$  the finite-size privacy-amplification offset. Since  $\beta$ ,  $P_B$ , and  $N_{\text{privacy}}$  are identical across all three schemes, any difference among the resulting key rates is caused solely by the channel response used in FDE, through the excess noise term in (27).

## VI. SIMULATION RESULTS AND DISCUSSION

This section evaluates the impact of channel-estimation accuracy on the secret key rate (SKR) of the proposed OFDM-based CV-QKD system. Three channel-knowledge cases are considered. The first case is the perfect-CSI benchmark, where Bob uses the true channel response  $H[m]$ . The second case is the proposed parameter-based reconstruction, where Bob estimates the multipath parameters and reconstructs the full

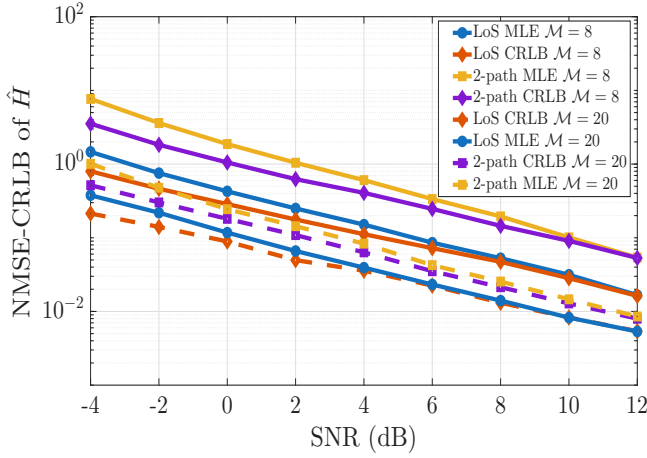


Fig. 2: NMSE of the reconstructed OFDM channel response  $\hat{H}$  versus SNR for LoS and two-path channels using MLE and the corresponding CRLB benchmark with  $M = 8$  and  $M = 20$  revealed symbols.

channel response. The third case is the conventional OFDM interpolation baseline, where the channel is first estimated on the publicly revealed subcarriers and then interpolated over the remaining subcarriers.

To quantify the channel estimation accuracy for the estimated channel  $\hat{H}[m]$ , we adopt the Normalized Mean Square Error (NMSE) as the performance metric, which is defined as

$$\text{NMSE} = \frac{\sum_{m=1}^M |H[m] - \hat{H}[m]|^2}{\sum_{m=1}^M |H[m]|^2}, \quad (35)$$

where  $M$  denotes the total number of subcarriers.

Unless otherwise stated, the simulations use a carrier frequency of  $f_c = 15$  THz, atmospheric attenuation coefficient  $\alpha = 50$  dB/km, detector efficiency  $\eta = 0.98$ , trusted detector-noise variance  $S = 1$ , and Eve/environment noise variance  $\sigma_E^2 = 1$ . The OFDM system uses  $M = 64$  subcarriers spaced by  $\Delta f = 2$  MHz, and maximum delay spread  $\tau_{\max} = 20$  ns. A two-path frequency-selective channel is considered, i.e.,  $D = 2$ , with path powers selected from a VehA-inspired multipath profile and delays normalized within the considered delay window. The variances are listed as  $V_0 = 1$  and  $V_s = 5$ .

Fig. 2 shows the NMSE of the reconstructed OFDM channel response  $\hat{H}$  versus SNR for LoS and two-path channels. The MLE performance is compared with the corresponding CRLB for  $M = 8$  and  $M = 20$  revealed symbols. As expected, the NMSE decreases with SNR and improves when more symbols are revealed, since additional observations enhance channel-parameter estimation. The LoS case achieves lower NMSE than the two-path case due to its simpler channel structure and fewer unknown parameters. The MLE curves follow the CRLB trends, while the remaining gap, especially for the two-path channel at low SNR, is mainly due to finite observations and nonlinear multipath estimation. These results confirm that accurate parameter-based reconstruction of  $H[m]$  reduces channel mismatch before OFDM FDE and is essential

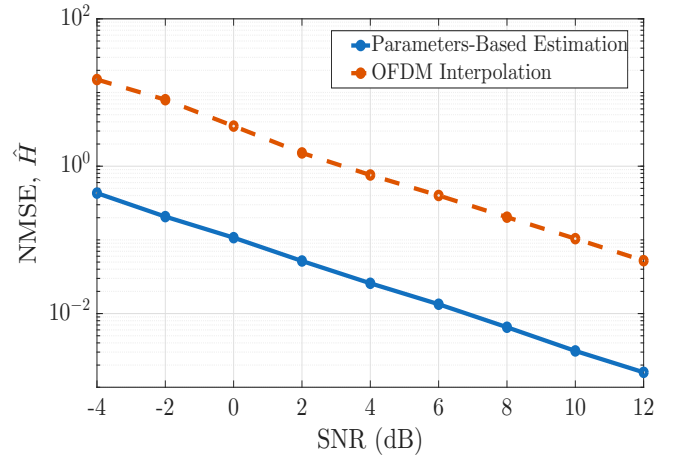


Fig. 3: NMSE of the reconstructed OFDM channel response  $\hat{H}$  versus SNR for the proposed parameter-based estimation and conventional OFDM interpolation when  $M = 16$ .

for improving the SKR.

Fig. 3 compares the NMSE of the reconstructed OFDM channel response  $\hat{H}$  for the proposed parameter-based estimation and conventional OFDM interpolation. Both methods improve as the SNR increases, since the revealed Gaussian symbols provide more reliable channel observations. However, the proposed method consistently outperforms interpolation over the entire SNR range. This gain comes from exploiting the physical multipath structure of the channel, where the full response  $H[m]$  is reconstructed from the estimated path delays, phases, and amplitudes. In contrast, OFDM interpolation only estimates the channel at the revealed subcarriers and then approximates the remaining subcarriers, which introduces interpolation error in frequency-selective channels. The performance gap confirms that parameter-based reconstruction provides a more accurate  $\hat{H}[m]$ , which reduces the channel-mismatch noise after OFDM FDE and supports the SKR improvement.

Fig. 4 shows the SKR versus Alice–Bob distance. The perfect-CSI case provides the upper bound because Bob equalizes the received symbols using the true channel response  $H[m]$ . The proposed parameter-based method achieves a higher SKR and a longer secure distance than OFDM interpolation for both reconciliation efficiencies. This improvement follows from the lower channel-reconstruction error of the parameter-based estimator, which reduces the CSI-induced mismatch noise after OFDM FDE and increases the effective Alice–Bob mutual information. It is worth noting that the comparison here is not concerned with reconciliation performance itself or block error probability; these are set to identical values across all schemes. The two values of  $\beta$  are included solely to illustrate how the SKR gap between the estimation methods persists across different reconciliation efficiency assumptions, confirming that the observed improvement is due to channel estimation alone. As expected, the curves with  $\beta = 0.95$  outperform those with  $\beta = 0.7$ , since a larger reconciliation efficiency increases the useful term  $\beta I_{AB}$ . The

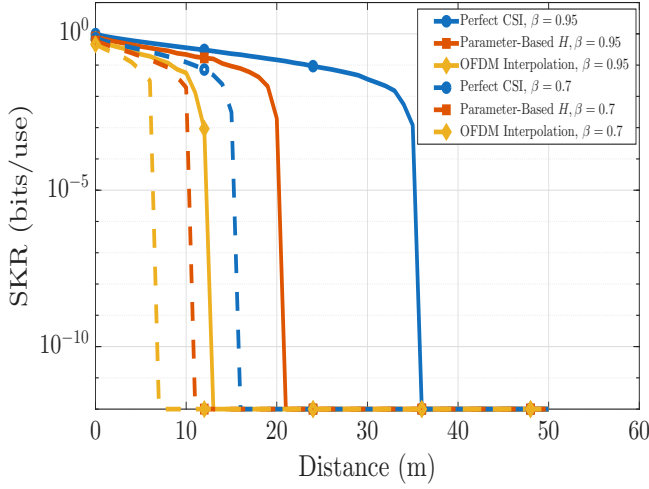


Fig. 4: SKR versus distance for perfect CSI, parameter-based channel reconstruction, and conventional OFDM interpolation under different reconciliation efficiencies when  $\mathcal{M} = 16$ .

abrupt drop of each curve corresponds to the distance at which  $\beta I_{AB} - \chi_{BE} \leq 0$ , where the achievable SKR becomes zero. These results confirm that improving the accuracy of  $\hat{H}[m]$  directly extends the secure operating distance.

## VII. CONCLUSION

This paper studied channel-parameter-based estimation for OFDM-enabled CV-QKD over frequency-selective quantum channels. The proposed method reconstructs the full channel response from estimated multipath parameters, avoiding the interpolation error of conventional OFDM channel estimation. Simulation results showed that the proposed estimator achieves lower channel NMSE and improves the SKR by reducing OFDM FDE mismatch noise. Compared with OFDM interpolation, the proposed approach provides higher SKR and extends the secure distance. These results highlight the importance of accurate channel estimation for reliable OFDM-based CV-QKD.

## VIII. ACKNOWLEDGMENT

This work was financially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) under the Discovery Grant (DG) program.

## REFERENCES

- [1] I. B. Djordjevic, "Hybrid qkd protocol outperforming both dv- and cv-qkd protocols," *IEEE Photonics Journal*, vol. 12, no. 1, pp. 1–8, 2020.
- [2] T. Ismail, A. H. Sabeeh, M. Yasser, and N. Alshaer, "Finite-size and modulation optimization in cv-qkd over uav-based fso link with adaptive optics," *IEEE Communications Letters*, vol. 29, no. 12, pp. 3033–3037, 2025.
- [3] X. Liu, C. Xu, Y. Noori, S. X. Ng, and L. Hanzo, "The road to near-capacity cv-qkd reconciliation: An fec-agnostic design," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 2089–2112, 2024.
- [4] S. Kumar and S. P. Dash, "Skr analysis of one- and two-way cv-qkd mimo fso communication system," *IEEE Communications Letters*, vol. 29, no. 10, pp. 2456–2460, 2025.
- [5] X. Liu, C. Xu, S. X. Ng, and L. Hanzo, "Otf-based cv-qkd systems for doubly selective thz channels," *IEEE Transactions on Communications*, vol. 73, no. 8, pp. 6274–6289, 2025.
- [6] X. Liu, C. Xu, S. Wang, S. Xin Ng, and L. Hanzo, "Hybrid beamforming assisted ofts-based cv-qkd systems for doubly selective thz channels," *IEEE Transactions on Communications*, vol. 73, no. 11, pp. 11 931–11 946, 2025.
- [7] X. Liu, N. Wang, C. Xu, S. X. Ng, P. V. Trinh, S. Sugiura, and L. Hanzo, "Tetherless thz cv-qkd – would it work?" *IEEE Wireless Communications*, pp. 1–9, 2025.
- [8] N. Alshaer and T. Ismail, "Performance evaluation and security analysis of uav-based fso/cv-qkd system employing dp-qpsk/cd," *IEEE Photonics Journal*, vol. 14, no. 3, pp. 1–11, 2022.
- [9] T. Ismail, A. H. Sabeeh, M. Yasser, and N. Alshaer, "Finite-size and modulation optimization in cv-qkd over uav-based fso link with adaptive optics," *IEEE Communications Letters*, vol. 29, no. 12, pp. 3033–3037, 2025.
- [10] T. V. Nguyen, H. T. Le, H. T. T. Pham, V. Mai, and N. T. Dang, "Enhancing design and performance analysis of satellite entanglement-based cv-qkd/fso systems," *IEEE Access*, vol. 11, pp. 112 097–112 107, 2023.
- [11] S. Ahmed, N. Alshaer, K. A. Alaghbari, and T. Ismail, "Security analysis of gaussian and discrete modulations in fso/cv-qkd systems employing llo under phase and amplitude attacks," *IEEE Access*, vol. 10, pp. 100 041–100 053, 2022.
- [12] X. Liu, C. Xu, Y. Noori, S. X. Ng, and L. Hanzo, "The road to near-capacity cv-qkd reconciliation: An fec-agnostic design," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 2089–2112, 2024.
- [13] M. Almeida, D. Pereira, M. Facão, A. N. Pinto, and N. A. Silva, "Reconciliation efficiency impact on discrete modulated cv-qkd systems key rates," *Journal of Lightwave Technology*, vol. 41, no. 19, pp. 6134–6141, 2023.
- [14] Z. Li, X. Wang, D. Qi, Z. Chen, and S. Yu, "High-speed implementation of continuous-variable quantum key distribution with polarization multiplexing," *Journal of Lightwave Technology*, vol. 44, no. 1, pp. 47–55, 2026.
- [15] S. Kumar, S. P. Dash, D. Ghose, and G. C. Alexandropoulos, "Ris-assisted mimo cv-qkd at thz frequencies: Channel estimation and secret key rate analysis," *IEEE Transactions on Communications*, vol. 73, no. 12, pp. 15 612–15 624, 2025.