Performance Analysis of MDI-QKD in Thermal-Loss and Phase Noise Channels

1st Heyang Peng
University of Luxembourg
The Interdisciplinary Center for Security Reliability and Trust (SnT)
Luxembourg
https://orcid.org/0009-0005-1754-4500

2nd Seid Koudia
University of Luxembourg
The Interdisciplinary Center for Security Reliability and Trust (SnT)
Luxembourg
https://orcid.org/0000-0002-7533-6778

3rd Symeon Chatzinotas, IEEE Fellow
University of Luxembourg
The Interdisciplinary Center for Security Reliability and Trust (SnT)
Luxembourg
https://orcid.org/0000-0001-5122-0001

***Abstract*—Measurement-device-independent quantum key distribution (MDI-QKD), enhances quantum cryptography by mitigating detector-side vulnerabilities. This study analyzes MDI-QKD performance in thermal-loss and phase noise channels, modeled as depolarizing and dephasing channels to capture thermal and phase noise effects. Based on this channel framework, we derive analytical expressions for Bell state measurement probabilities, quantum bit error rates (QBER), and secret key rates (SKR) of MDI-QKD. Our simulations reveal that SKR decreases exponentially with transmission distance, with performance further degraded by increasing thermal noise and phase noise, particularly under high thermal noise conditions. These findings offer insights into enhancing MDI-QKD's noise resilience, supporting secure key generation in practical, noisy environments.**

***Index Terms*—MDI-QKD, thermal-loss channel, phase noise channel, secret key rate, quantum bit error rate**

I. Introduction

Quantum key distribution (QKD) enables secure key sharing between two parties, Alice and Bob, ensuring encrypted communication with total confidentiality guaranteed by the laws of quantum physics [1], [2]. The first QKD protocol, BB84, introduced by Bennett and Brassard, utilized discrete variables (DV) with single-photon states, establishing a robust framework for secure communications [1]. Subsequent developments extended QKD to continuous-variable (CV) protocols, such as the squeezed-state protocol, leveraging entangled states for enhanced performance [3]–[5]. However, pratical transmission media, such as optical fibers, introduce thermal noise and phase noise, which arise from physical phenomena like random photon scattering due to thermal fluctuations in the fiber material and phase drifts caused by environmental pertubations such as temperature variations or mechanical vibrations. These degrade QKD performance by reducing secret key rates (SKR) and increasing quantum bit error rates (QBER), posing significant challenges to practical deployment [6]–[8]. While studies have explored thermal noise and phase noise effects on both DV- and CV-QKD protocols, research indicates that CV-QKD is robust in low-to-moderate loss regimes, whereas DV-QKD performs better in high-loss scenarios [9]–[12]. The specific impact of these noise sources on Measurement-Device-Independent QKD (MDI-QKD), however, remains underexplored. MDI-QKD, a DV protocol, eliminates detector-side vulnerabilities, making it a cornerstone for practical quantum networks where a secure long-distance key distribution is critical [13]–[17]. Given its pivotal role in enabling secure quantum communication across metropolitan or satellite-based networks [18], understanding MDI-QKD's behavior under thermal noise and phase noise is essential.

In this work, we model thermal-loss and phase noise channels as depolarizing and dephasing channels to capture thermal (N_{th}) and phase noise (σ_θ) effects. The depolarizing channel captures thermal noise's uniform state mixing across all polarization bases, critical for SKR impacts, while the dephasing channel isolates phase noise's coherence loss in the X-basis, vital for eavesropping detection in MDI-QKD, thus, we chose this combined models. Assuming ideal single-photon sources and perfect detectors—eliminating dark counts and other practical imperfections—we derive analytical expressions for projection probabilities onto Bell states, QBER, and SKR, focusing on the channel's impact on system performance. Through numerical simulations under these idealized conditions, we evaluate MDI-QKD performance across varying noise levels and transmission distances. Our study provides a theoretical framework to optimize MDI-QKD's noise resilience, addressing key challenges for its deployment in noisy quantum communication systems and supporting its application in secure quantum networks.

The paper is structured as follows. In Section II, we establish the theoretical and modeling framework for the thermal-loss and phase-noise channels. Section III presents the MDI-QKD analysis in terms of secret key rate (SKR) and quantum bit error rate (QBER) under the influence of thermal-loss and phase noise. Section IV presents numerical simulations evaluating the performance of MDI-QKD in the presence of these noise effects. Finally, Section V concludes the paper.

II. Thermal Noise and Phase noise in MDI-QKD

In MDI-QKD, Alice and Bob transmit single-photon states through optical fiber channels to an untrusted third party, Charlie, as shown in Figure. 1. In realistic scenarios, these fiber channels are subject to thermal-loss and phase noise – two key

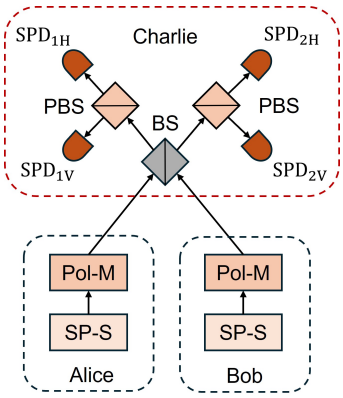

Fig. 1. MDI-QKD protocol, SP-S: Single Photon Source, Pol-M: Polarization Modulator, BS: Beamsplitter., PBS: Polarization Beamsplitter, SPD: Single Photon Detector

factors that can compromise security if not properly adressed. To accurately model these effects, we treat the channels as a combination of depolarizing and dephasing channels. These models capture the essential quantum characteristics of the communication channels and provide a solid theoretical foundation for analyzing the impact of noise. In the following, we present the channel models and their derivations in detail.

1. Thermal-loss Channel

Thermal-loss channels are common environmental disturbances in QKD, especially in fibre-optic transmission, introduction of background thermal noise denoted by N_{th} due to scattering and absorption. To model this effect, we adopt the approach in [6], treating the thermal-loss channel as equivalent to a depolarizing channe, as it effectively captures the uniform randomization of photon polarization states across all bases. The depolarizing channel acts on a single-qubit density matrix $\hat{\rho}$ as follows:

$$\hat{\rho}' \to (1-\lambda)\hat{\rho} + \frac{\lambda}{2}\mathbb{I} \tag{1}$$

where $\mathbb{I} = |H\rangle\langle H| + |V\rangle\langle V|$ is the identity operator in the polarization basis. The depolarization parameter λ quantifies the extent of noise-induced mixing. Its derivation stems from a beamsplitter model, where Alice's input state is a single photon $|1\rangle_A$, with the environment in a thermal state:

$$\hat{\rho}_{\text{th}} = \sum_{n=0}^{\infty} \frac{N_{\text{th}}^n}{(1+N_{\text{th}})^{n+1}} |n\rangle\langle n|_E \tag{2}$$

with N_{th} being the average number of thermal noise photons. For an input state $|1,n\rangle_{AE}$, the output state $\hat{\rho}'_{AF}$ is traced over the environment mode F, yielding the unnormalized output $\hat{\rho}'_A$:

$$\hat{\rho}'_A = \frac{\eta}{\gamma^4}\hat{\rho}_A + \frac{N_{\text{th}}(1+N_{\text{th}})(1-\eta)^2}{\gamma^4}\mathbb{I} \tag{3}$$

where η is the channel transmissivity and $\gamma = 1+N_{\text{th}}-N_{\text{th}}\eta$ is the normalization factor dependent on N_{th} and η.

The single-photon success probability, or the likelihood of detecting a single photon at Charlie, is:

$$P_S = \text{Tr}(\hat{\rho}'_A) = \frac{\eta + 2N_{\text{th}}(1+N_{\text{th}})(1-\eta)^2}{\gamma^4} \tag{4}$$

As a consequence, the normalized conditional density matrix is:

$$\hat{\rho}'_A/P_S = (1-\lambda)\hat{\rho}_A + \frac{\lambda}{2}\mathbb{I} \tag{5}$$

with:

$$\lambda = \frac{2N_{\text{th}}(1+N_{\text{th}})(1-\eta)^2}{\eta + 2N_{\text{th}}(1+N_{\text{th}})(1-\eta)^2} \tag{6}$$

This model illustrates how thermal noise N_{th} and channel transmissivity η jointly determine the depolarization and success probability of single-photon transmission. Since Alice and Bob operate through independent channels, with parameters λ_A, P_S^A and λ_B, P_S^B.

2. Phase Noise Channel

Phase noise arises from environmental perturbations, such as temperature fluctuations or mechanical vibrations, which disrupt the phase coherence of quantum states. In MDI-QKD, this noise particularly impacts the X-basis, where phase information is critical to detect eavesdropping attempts. We represent phase noise as a dephasing channel as in [6], which selectively affects the non-diagonal elements of the density matrix. The phase noise channel transforms the density matrix as:

$$\hat{\rho} \to \begin{bmatrix} \rho_{00} & \bar{r}^2\rho_{01} \\ \bar{r}^2\rho_{10} & \rho_{11} \end{bmatrix} \tag{7}$$

where $\bar{r}^2 = e^{-\sigma_\theta^2}$, and σ_θ is the standard deviation of the phase noise. This effect originates from a random phase rotation, modeled as:

$$\hat{\rho} \to \int_{-\pi}^{\pi} f(\theta) e^{i\hat{n}\theta}\hat{\rho}e^{-i\hat{n}\theta}d\theta \tag{8}$$

Here, number operator $\hat{n}$ is the photon number in the state, θ is the random phase angle. The phase distribution is a wrapped normal distribution:

$$f_{WN}(\theta) = \frac{1}{\sigma_\theta\sqrt{2\pi}} \sum_{k=-\infty}^{\infty} e^{-(\theta+2\pi k)^2/2\sigma_\theta^2} \tag{9}$$

Indeed, the expectation value of the phase shift affects the off-diagonal terms:

$$\rho_{01} \to \langle e^{i\theta}\rangle\rho_{01}, \quad \bar{r} = \int_{-\pi}^{\pi} f_{WN}(\theta)e^{i\theta}d\theta = e^{-\sigma_\theta^2/2} \tag{10}$$

The $\bar{r}^2$ factor quantifies the coherence loss, decreasing as σ_θ increases, directly impacting the X-basis measurements in MDI-QKD. Since diagonal terms remain unchanged, phase

TABLE I
MDI-QKD CODING RULE

Alice&Bob	Bell State: $\|\psi^-\rangle$	Bell State: $\|\psi^+\rangle$
Z-basis	Bit flip	Bit flip
X-basis	Bit flip	No Bit flip

noise does not contribute to errors but complicates eavesdropping detection. Consequentely, the combined channel, which integrates thermal loss and phase noise, is:

$$\hat{\rho} \to (1-\lambda)\begin{bmatrix} \rho_{00} & \bar{r}^2\rho_{01} \\ \bar{r}^2\rho_{10} & \rho_{11} \end{bmatrix} + \frac{\lambda}{2}\mathbb{I} \tag{11}$$

III. MDI-QKD Analysis: SKR and QBER

In MDI-QKD, Alice and Bob send single-photon states through their respective noisy channels to Charlie, who performs a Bell state measurement, projecting onto:

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle), \quad |\psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) \tag{12}$$

Assuming single-photon sources and ideal detectors, with Z and X bases each chosen with probability $\frac{1}{2}$, we analyze the channel effects and derive the secret key rate (SKR) and quantum bit error rate (QBER). We use $|H\rangle$ (i.e., $|H\rangle|H\rangle$) as an illustrative example.

1) State Evolution Through Channels: Alice prepares $|H\rangle_A$, with density matrix:

$$\hat{\rho}_A = |H\rangle\langle H|_A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \tag{13}$$

Bob symmetrically prepares $|H\rangle_B$, $\hat{\rho}_B = |H\rangle\langle H|_B$.

2) After Channel Transmission: After passing through the thermal-loss and phase noise channels, the state arrives at Charlie with probability P_S^A and P_S^B, and the conditional density matrix becomes:

$$\hat{\rho}_{A'} = (1-\lambda_A)\hat{\rho}_A + \frac{\lambda_A}{2}\mathbb{I} = \begin{bmatrix} 1-\frac{\lambda_A}{2} & 0 \\ 0 & \frac{\lambda_A}{2} \end{bmatrix} \tag{14}$$

Phase noise does not affect the Z-basis, as it only scales off-diagonal elements. Bob's state undergoes a similar transformation. The joint density matrix: The joint state is:

$$\hat{\rho}_{A'B'} = \hat{\rho}_{A'} \otimes \hat{\rho}_{B'} \tag{15}$$

3) Bell State Measurement: The projection probability is defined as:

$$P_{\psi^\pm} = \mathrm{Tr}(\hat{\rho}_{A'B'}|\psi^\pm\rangle\langle\psi^\pm|) \tag{16}$$

Accordingly, the probability of $\hat{\rho}_{A'B'}$ projecting onto $|\psi^+\rangle$ is:

$$\begin{aligned} P_{\psi^+}^{HH} &= \langle\psi^+|\hat{\rho}_{A'B'}|\psi^+\rangle \\ &= \frac{1}{2}\left[(1-\frac{\lambda_A}{2})\frac{\lambda_B}{2} + \frac{\lambda_A}{2}(1-\frac{\lambda_B}{2})\right] \\ &= \frac{\lambda_A+\lambda_B-\lambda_A\lambda_B}{4} \end{aligned} \tag{17}$$

See Appendix A.1 for derivation. Similarly, projecting onto $|\psi^-\rangle$ is:

$$P_{\psi^-}^{HH} = \langle\psi^-|\hat{\rho}_{A'B'}|\psi^-\rangle = 0 \tag{18}$$

See Appendix A.1 for derivation. This probability reflects erroneous detection events due to depolarizing noise, impacting the Z-basis error rate. The projection probabilities for various other mixing states can be obtained in the same way.

4) QBER and SKR Derivation: In Table. I outlines the coding rules for MDI-QKD. The analysis of error rates and secret key rates is central to evaluating the security of MDI-QKD. The Z-basis is used for key generation, and the error rate reflects the probability of erroneous detection from identical inputs. Accounting for the average gain across all possible inputs, including both valid and invalid detections:

$$Q_{\mathrm{Z}} = \frac{2-2\lambda_A-2\lambda_B+3\lambda_A\lambda_B}{4}P_S^AP_S^B \tag{19}$$

See Appendix A.2 for explicit derivation.
Only different inputs (H_AV_B and V_AH_B) contribute to the key, as they produce usable key bits:

$$Q_{\mathrm{Z}}^{1,1} = \frac{2-\lambda_A-\lambda_B+2\lambda_A\lambda_B}{4}P_S^AP_S^B \tag{20}$$

We refer the reader to Appendix A.3 for explicit derivation. Caused by erroneous detection of identical inputs, the Z-basis error rate E_Z quantifies the probability of projecting onto the Bell state $|\psi^+\rangle$ when Alice and Bob send identical states such as H_AH_B or V_AV_B, which should not contribute to the key, and is given by:

$$E_{\mathrm{Z}} = \frac{\lambda_A+\lambda_B-\lambda_A\lambda_B}{2\left(1-\lambda_A-\lambda_B+\frac{3}{2}\lambda_A\lambda_B\right)} \tag{21}$$

See Appendix A.4 for explicit derivation. Where E_{Z} quantifies the disturbance due to depolarizing noise in the Z-basis. We note that λ_A, λ_B diminishes Q_Z by elevating the rate of invalid detections, which reduces the SKR and the fraction of valid key bits. In contrast, the X-basis is employed to estimate eavesdropping, influenced by both depolarization and phase noise.

$$e_{\mathrm{X}}^{1,1} = \frac{2(1-\bar{r}^2)(1+\lambda_A\lambda_B)-(1-2\bar{r}^2)(\lambda_A+\lambda_B)}{4(1-\lambda_A-\lambda_B+2\lambda_A\lambda_B)} \tag{22}$$

$$\begin{aligned} R &= I(A:B) - \chi(B:E) = Q_Z^{1,1}[1-H(e_X^{1,1})] - Q_Z f H(E_Z) \\ &= \frac{P_S^AP_S^B}{4}\Bigg[(2-\lambda_A-\lambda_B+2\lambda_A\lambda_B) \quad \left[1-H\left(\frac{2(1-\bar{r}^2)(1+\lambda_A\lambda_B)-(1-2\bar{r}^2)(\lambda_A+\lambda_B)}{4(1-\lambda_A-\lambda_B+2\lambda_A\lambda_B)}\right)\right] \\ &\quad -(2-2\lambda_A-2\lambda_B+3\lambda_A\lambda_B)\,H\left(\frac{\lambda_A+\lambda_B-\lambda_A\lambda_B}{2\left(1-\lambda_A-\lambda_B+\frac{3}{2}\lambda_A\lambda_B\right)}\right)\Bigg] \end{aligned} \tag{23}$$

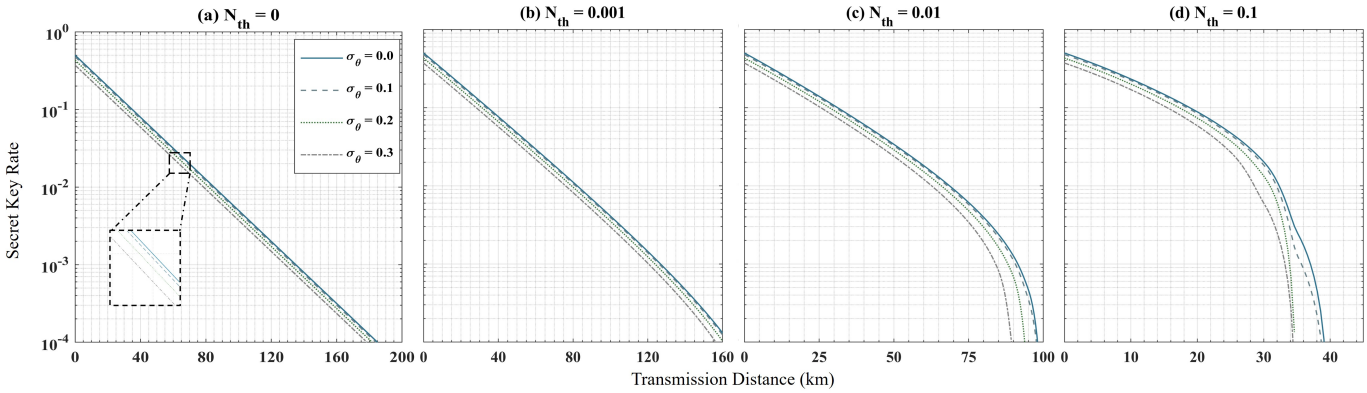

Fig. 2. SKR as a function of transmission distance under varying thermal noise (N_{th}) and phase noise (σ_θ) in the MDI-QKD system, with N_{th} ranging from 0 to 0.1 and σ_θ from 0 to 0.3, highlighting the dominant impact of thermal noise on secure distance reduction.

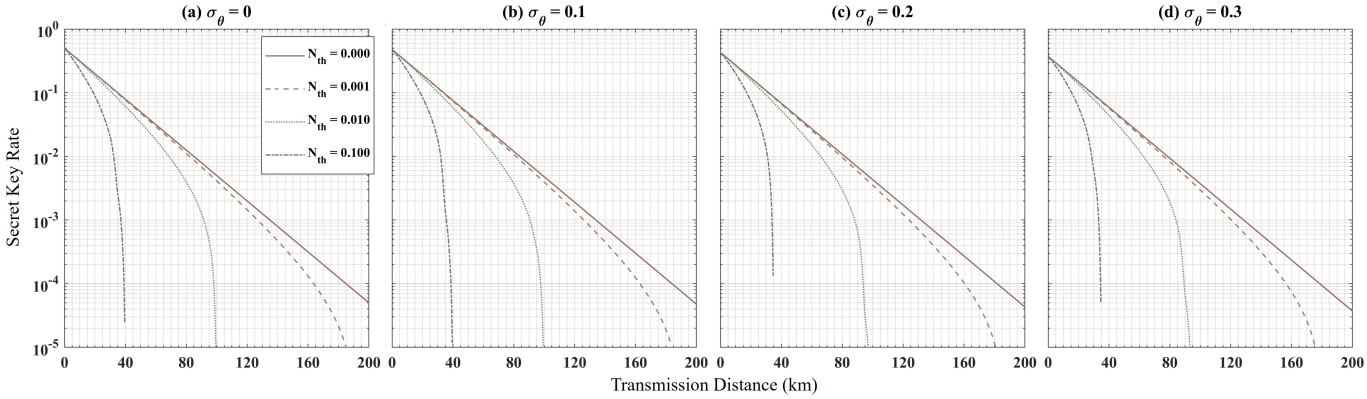

Fig. 3. SKR as a function of transmission distance under varying phase noise (σ_θ) and thermal noise (N_{th}) in the MDI-QKD system, with σ_θ ranging from 0 to 0.3 and N_{th} from 0 to 0.1, showing the limited impact of phase noise compared to thermal noise.

See Appendix A.5 and A.6 for derivation. A key figure of merit in quantum security protocols in general, and MDI-QKD in particular, is the SKR. This quantifies the number of secure key bits that Alice and Bob can distill from their correlated measurements, achieved through Charlie's Bell state measurement, while accounting for potential information leakage to an eavesdropper, Eve. To rigorously formulate this balance, we employ the Devetak-Winter bound [19] under reverse reconciliation. Based on Eq. 19, Eq. 20 and Eq. 21, the SKR is expressed in (23). Here, $I(A:B) = Q_Z^{1,1}[1-H(e_X^{1,1})]$ represents the mutual information between Alice (A) and Bob (B), encapsulating the amount of shared information available for key generation after Charlie's measurements. The factor $1 - H(e_X^{1,1})$ adjusts the effective key rate by subtracting the information that could potentially be leaked to Eve through errors in the X-basis, as she might exploit these discrepancies to infer key bits, thereby leaving $I(A:B)$ as the secure information content per valid detection.

The Holevo information, $\chi(B:E) = Q_Z f H(E_Z)$, quantifies the upper bound on Eve's knowledge about Bob's key bits, representing the information she could theoretically extract from the system. We set the parameter $f = 1$ as ideal error correction efficiency, meaning all Z-basis errors are perfectly reconciled, a simplifying assumption for this analysis. Thus, $\chi(B:E)$ represents the information leakage Eve could access by observing all Z-basis outcomes, weighted by the entropy of errors that must be corrected to ensure key security.

This Devetak-Winter formulation ensures the SKR accounts for both the usable shared information and Eve's potential knowledge, effectively mitigating the impacts of thermal noise N_{th} and phase noise $\bar{r}^2$ on the key generation process in MDI-QKD.

This section has established a theoretical model for MDI-QKD that incorporates the effects of thermal-loss and phase-noise channels. By capturing the combined influence of thermal noise (N_{th}) and phase noise (through $\bar{r}^2$) on the secret key rate, the model lays the groundwork for the simulation-based performance analysis presented in the next section.

IV. Simulation and Analysis of Channel Noise Effects on MDI-QKD Performance

In the previous section, we established the MDI-QKD model under thermal-loss and phase-noise channels, forming the basis for the simulation framework. A key parameter in the model is the transmissivity η, which quantifies channel efficiency and depends on the physical transmission medium. While the

model is general, in our simulations we compute η for a fiber-optic channel using the standard exponential attenuation model: $\eta = 10^{-\alpha L/10}$, where $\alpha = 0.2dB/km$, denotes the fiber attenuation coefficient and L represents the total transmission distance between Alice, Bob, and Charlie.

Upon completing the simulation setup, we evaluate the SKR across a range of thermal noise levels N_{th} and phase noise parameters σ_θ, over varying transmission distances. This section presents and analyzes the simulation results to provide deeper insight into how these noise sources influence system performance.

Figure 2 examines the impact of thermal noise N_{th} on SKR for several values of phase noise σ_θ. The results reveal that SKR is highly sensitive to thermal noise: as N_{th} increases, the maximum transmission distance supporting nonzero SKR significantly decreases. Even small increases in thermal noise lead to noticeable reductions in both SKR magnitude and secure distance. In contrast, variations in phase noise within the considered range have only a marginal effect on SKR, especially at longer distances. This suggests that the overall system performance is predominantly constrained by thermal noise, with phase noise playing a secondary role.

Figure 3 reverses the focus, illustrating how SKR responds to increasing phase noise σ_θ across different levels of thermal noise. While SKR shows slight degradation as σ_θ increases, particularly at short to medium distances, the overall sensitivity remains low within the practical phase noise range. In scenarios with negligible thermal noise, increasing σ_θ leads to a modest decline in SKR, reflecting increased phase uncertainty. However, once thermal noise is present at non-negligible levels, it dominates the SKR decay, rendering the system relatively insensitive to further phase noise variations.

The underlying reason for this disparity lies in the respective effects of each noise type on the system's key rate components. Phase noise introduces a multiplicative attenuation factor $r^2 = \exp(-\sigma_\theta^2)$, which affects the X-basis QBER (e_X^{11}). However, this factor decreases gradually with σ_θ, resulting in only moderate increases in error rates. On the other hand, thermal noise alters the photon-number statistics of the source states, directly impacting the yields λ_A and λ_B, and subsequently degrading the gain (Q_Z^{11}, Q_Z) and increasing the bit error rate E_Z. These combined effects substantially reduce the SKR.

Overall, the simulation results clearly demonstrate that thermal noise is the dominant limiting factor for SKR in MDI-QKD systems, significantly constraining the achievable secure transmission distance. In contrast, phase noise within realistic operating conditions exerts only a limited influence, indicating a degree of robustness to phase fluctuations in optical fibers. These findings highlight the importance of minimizing thermal noise in practical implementations to preserve key rate performance and extend operational range.

V. Conclusion

In this work, we investigated the performance of MDI-QKD over thermal-loss and phase-noise channels, assuming ideal single-photon sources and perfect detector efficiencies. Employing the Devetak–Winter bound under reverse reconciliation, we derived the secret key rate (SKR) to assess the system's performance. Our findings indicate that thermal noise has a more pronounced impact on SKR than phase noise, playing a dominant role in limiting the overall efficiency of the MDI-QKD protocol. These analytical insights provide a foundation for future studies aimed at exploring practical MDI-QKD implementations across a broad range of channel conditions.

Acknowledgment

This work was supported by the project Lux4QCI (GA 101091508) funded by the Digital Europe Program, and the project LUQCIA Funded by the European Union – Next Generation EU, with the collaboration of the Department of Media, Connectivity and Digital Policy of the Luxembourgish Government in the framework of the RRF program. H.P and S.K thank Leonardo Oleynik for discussion.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp. 175–179, 1984.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.

[3] N. J. Cerf, M. Levy, and G. Van Assche, "Security of quantum key distribution using squeezed states," *Physical Review A*, vol. 63, no. 2, pp. 022311, 2001.

[4] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, 2003.

[5] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Reviews of Modern Physics*, vol. 84, no. 2, pp. 621–669, 2012.

[6] S. P. Kish, P. J. Gleeson, A. Walsh, P. K. Lam, and S. M. Assad, "Comparison of discrete variable and continuous variable quantum key distribution protocols with phase noise in the thermal-loss channel," *Quantum*, vol. 8, 1382, 2024.

[7] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, pp. 16025, 2016.

[8] S. Koudia, L. Oleynik, M. Bayraktar, and S. Chatzinotas, "Physical layer aspects of quantum communications: A survey," *arXiv preprint arXiv:2501.XXXXX*, 2025.

[9] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, pp. 15043, 2017.

[10] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with gaussian post-selection," *Physical Review X*, vol. 8, no. 2, pp. 021059, 2018.

[11] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics*, vol. 92, no. 2, pp. 025002, 2020.

[12] S. Koudia, L. Oleynik, M. Bayraktar, J. ur Rehman, and S. Chatzinotas, "Spatial-Mode Diversity and Multiplexing for Continuous Variables Quantum Communications," *arXiv preprint arXiv:2501.XXXXX*, 2025.

[13] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 108, no. 13, pp. 130503, 2012.

[14] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, and others, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical Review Letters*, vol. 117, no. 19, pp. 190501, 2016.

[15] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, "Twin-field quantum key distribution over 830 km fiber," *Physical Review Letters*, vol. 126, no. 1, pp. 010501, 2021.

[16] S. Pirandola, C. Ottaviani, G. Spedalieri, et al., "High-rate measurement-device-independent quantum cryptography," *Nature Photonics*, vol. 9, pp. 397–402, 2015.
[17] J. ur Rehman, et al., "Diversity and multiplexing in quantum MIMO channels," *arXiv preprint arXiv:2501.XXXXX*, 2025.
[18] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, and others, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.
[19] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 461, no. 2053, pp. 207–235, 2005.

APPENDIX A

In MDI-QKD, the secure exchange of cryptographic keys between Alice and Bob relies on Charlie's Bell state measurements. The precision of these measurements, encapsulated in projection probabilities, forms the cornerstone to obtain critical performance metrics such as QBER and SKR, which collectively quantify the ability of the system. This appendix provides a detailed derivation of the Z-basis projection probabilities $P_{\psi^+}^{HH}$ and $P_{\psi^-}^{HH}$ and the X-basis projection probability $P_{\psi^+}^{DD}$ as representative examples, illustrating the distinct impacts of depolarizing noise (via λ) and phase noise (via $\bar{r}^2$). Subsequently, we derive the total count rate Q_Z , effective key rate $Q_Z^{1,1}$, Z-basis error rate E_Z , X-basis error rate $e_X^{1,1}$ and R, using these projection probabilities.

A.1 Derivation of Bell State Projection Probabilities

Charlie's Bell state measurements project the joint state $\hat{\rho}_{A'B'}$ onto the Bell states $|\psi^+\rangle$ or $|\psi^-\rangle$. These probabilities are pivotal, as they reflect how thermal noise (via λ) and phase noise (via $\bar{r}^2$) alter the quantum state, influencing key generation and error rates. As examples, we derive $P_{\psi^+}^{HH}$ and $P_{\psi^-}^{HH}$ for the identical input of the Z-basis $|H\rangle_A|H\rangle_B$, and $P_{\psi^+}^{DD}$ for the identical input of the X-basis $|D\rangle_A|D\rangle_B$, while summarizing the remaining probabilities in A.1.3 to provide a complete overview.

A.1.1 Z-basis: $P_{\psi^+}^{HH}$ and $P_{\psi^-}^{HH}$: For the input $|H\rangle_A|H\rangle_B$, Alice and Bob prepare horizontally polarized photons, forming the initial state $\hat{\rho}_A \otimes \hat{\rho}_B$. After transmission through independent noisy channels the indivudual states in Eq. (11), this evolves into outcoming states states $\hat{\rho}_{A'}$ and $\hat{\rho}_{B'}$. According to Eq. (15), the joint density matrix $\hat{\rho}_{A'B'} = \hat{\rho}_{A'} \otimes \hat{\rho}_{B'}$ in the Z-basis is:

$$\hat{\rho}_{A'B'} = \hat{\rho}_{A'} \otimes \hat{\rho}_{B'} = \begin{bmatrix} \left(1-\frac{\lambda_A}{2}\right)\left(1-\frac{\lambda_B}{2}\right) & 0 & 0 & 0 \\ 0 & \left(1-\frac{\lambda_A}{2}\right)\frac{\lambda_B}{2} & 0 & 0 \\ 0 & 0 & \frac{\lambda_A}{2}\left(1-\frac{\lambda_B}{2}\right) & 0 \\ 0 & 0 & 0 & \frac{\lambda_A}{2}\frac{\lambda_B}{2} \end{bmatrix} \tag{24}$$

This diagonal form reflects the Z-basis input's lack of superposition, rendering phase noise ($\bar{r}^2$) ineffective here, as it only affects off-diagonal terms. Depolarizing noise (λ_A, λ_B), however, mixes polarizations, potentially causing errors in detection. The Bell state $|\psi^+\rangle$ and $|\psi^-\rangle$ are expressed in vector form:

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\1\\0\end{bmatrix}, \quad \langle\psi^+| = \frac{1}{\sqrt{2}}\begin{bmatrix}0 & 1 & 1 & 0\end{bmatrix} \tag{25}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\-1\\0\end{bmatrix}, \quad \langle\psi^-| = \frac{1}{\sqrt{2}}\begin{bmatrix}0 & 1 & -1 & 0\end{bmatrix} \tag{26}$$

The projection probability onto $|\psi^+\rangle$, as given by Eq.(17), can be formulated using the vector representation of Eq.(25) as follows:

$$P_{\psi^+}^{HH} = \frac{1}{2}[0\,1\,1\,0]\hat{\rho}_{A'B'}\begin{bmatrix}0\\1\\1\\0\end{bmatrix}$$

Matrix operations with the given Eq. (24) produce the result given in Eq. (17) as:

$$P_{\psi^+}^{HH} = \frac{\lambda_A + \lambda_B - \lambda_A\lambda_B}{4}$$

This non-zero probability signifies an erroneous detection event where identical inputs $|H\rangle_A|H\rangle_B$ are mistaken for $|\psi^+\rangle$, a state typically associated with different inputs. This error, induced by depolarizing noise, increases with λ_A and λ_B, directly contributing to the error rate on the Z-basis and necessitating error correction, which reduces the yield of the secure key. Similarly, the projection probability onto $|\psi^-\rangle$ in Eq. (18) is expressed as:

$$P_{\psi^-}^{HH} = \frac{1}{2}[0\,1\,-1\,0]\hat{\rho}_{A'B'}\begin{bmatrix}0\\1\\-1\\0\end{bmatrix}$$

Matrix operations with the given Eq. (24) produce the result given in Eq. (18) as:

$$P_{\psi^-}^{HH} = \frac{1}{2}\left[\left(1-\frac{\lambda_A}{2}\right)\frac{\lambda_B}{2} - \frac{\lambda_A}{2}\left(1-\frac{\lambda_B}{2}\right)\right] = 0$$

The zero outcome reflects the absence of coherence required for $|\psi^-\rangle$, distinguishing it from $|\psi^+\rangle$. This contrasts with $P_{\psi^+}^{HH}$, emphasizing the distinct roles of Bell states in error generation under thermal noise.

A.1.2 X-Basis: $P_{\psi^+}^{DD}$: For the X-basis input $|D\rangle_A|D\rangle_B$, the joint density matrix after transmission through both channels, as described in Eq. (11), is expressed as:

$$\hat{\rho}_{A'B'} = \hat{\rho}_{A'} \otimes \hat{\rho}_{B'} = \begin{bmatrix} \frac{(1-\lambda_A)(1-\lambda_B)}{4} & \frac{(1-\lambda_A)(1-\lambda_B)\bar{r}^2}{4} & \frac{(1-\lambda_A)(1-\lambda_B)\bar{r}^2}{4} & \frac{1-\lambda_B}{4} \\ \frac{(1-\lambda_A)(1-\lambda_B)\bar{r}^2}{4} & \frac{1-\lambda_A}{4} & \frac{1-\lambda_B}{4} & \frac{(1-\lambda_A)(1-\lambda_B)\bar{r}^2}{4} \\ \frac{(1-\lambda_A)(1-\lambda_B)\bar{r}^2}{4} & \frac{1-\lambda_B}{4} & \frac{1-\lambda_A}{4} & \frac{(1-\lambda_A)(1-\lambda_B)\bar{r}^2}{4} \\ \frac{1-\lambda_A}{4} & \frac{(1-\lambda_A)(1-\lambda_B)\bar{r}^2}{4} & \frac{(1-\lambda_A)(1-\lambda_B)\bar{r}^2}{4} & \frac{1}{4} \end{bmatrix} \tag{27}$$

This matrix, derived from the tensor product of individual states $\hat{\rho}_{A'}$ and $\hat{\rho}_{B'}$, exhibits off-diagonal terms scaled by $\bar{r}^2$, reflecting phase noise's impact on the initial superposition, alongside depolarizing noise's mixing effects parameterized by λ_A and λ_B. Similarly, performing matrix operations, projecting onto $|\psi^+\rangle$ yields:

$$P_{\psi^+}^{DD} = \frac{(1+\bar{r}^2) + (1-\bar{r}^2)(\lambda_A + \lambda_B - \lambda_A\lambda_B)}{4} \tag{28}$$

We note that Phase noise ($\bar{r}^2 < 1$) reduces the off-diagonal contribution, lowering $P_{\psi^+}^{DD}$ and increasing X-basis errors, critical for eavesdropping detection.

A.1.3 Summary of all projection probabilities: With similar derivation methods, the remaining probabilities are provided for direct use:

$$\begin{aligned}
P_{\psi^+}^{HH} &= P_{\psi^+}^{VV} = \frac{\lambda_A + \lambda_B - \lambda_A\lambda_B}{4} \\
P_{\psi^-}^{HH} &= P_{\psi^-}^{VV} = 0 \\
P_{\psi^+}^{HV} &= P_{\psi^+}^{VH} = \frac{2 - 2\lambda_A - \lambda_B + \lambda_A\lambda_B}{4} \\
P_{\psi^-}^{HV} &= P_{\psi^-}^{VH} = \frac{\lambda_A\lambda_B}{4} \\
P_{\psi^+}^{AA} &= P_{\psi^+}^{DD} = \frac{(1+\bar{r}^2) + (1-\bar{r}^2)(\lambda_A + \lambda_B - \lambda_A\lambda_B)}{4} \\
P_{\psi^-}^{AA} &= P_{\psi^-}^{DD} = \frac{(1-\lambda_A)(1-\lambda_B)(1-\bar{r}^2) + \lambda_A\lambda_B}{4} \\
P_{\psi^+}^{AD} &= P_{\psi^+}^{DA} = \frac{(1-\lambda_A)(1-\bar{r}^2-\bar{r}^2\lambda_B+\lambda_B) + \lambda_A}{4} \\
P_{\psi^-}^{AD} &= P_{\psi^-}^{DA} = \frac{(1-\lambda_A)(1-\lambda_B)(1+\bar{r}^2) + \lambda_A\lambda_B}{4}
\end{aligned}$$

A.2 Derivation of Z-basis total count rate Q_Z

The total count rate Q_Z quantifies the average probability that Charlie detects a Bell state on the Z-basis across all possible input combinations ($H_AH_B, V_AV_B, H_AV_B, V_AH_B$). This metric encompasses both valid key-generating events (e.g., H_AV_B and V_AH_B) and invalid detections (e.g., H_AH_B and V_AV_B) that contribute to errors. In MDI-QKD, Charlie's measurement projections onto $|\psi^+\rangle$ or $|\psi^-\rangle$ as valid responses, regardless of whether they correspond to the intended key bits, reflecting the overall detection performance of the system. Influenced primarily by depolarizing noise (λ_A, λ_B), Q_Z is crucial for assessing the measurement efficiency and noise impact:

$$\begin{aligned}
Q_Z = &\frac{1}{2}P_S^A P_S^B \\
&\left(P_{\psi^+}^{HH} + P_{\psi^+}^{VV} + P_{\psi^+}^{HV} + P_{\psi^-}^{HV} + P_{\psi^+}^{VH} + P_{\psi^-}^{VH}\right)
\end{aligned} \tag{29}$$

Here, the factor $\frac{1}{2}$ averages over the equal probabilities of Alice and Bob selecting $|H\rangle$ or $|V\rangle$, and $P_S^A P_S^B$ represents the joint success probability of photon transmission through the noisy channels. By including projections in both Bell states, $|\psi^+\rangle$ and $|\psi^-\rangle$, Q_Z accounts for all detection events, whether valid key-generating outcomes or erroneous detections, shaping the system performance under depolarizing noise. Substituting the probabilities listed in A.1.3 into Eq. (29), the result reflects the interplay between successful photon transmissions ($P_S^A P_S^B$) and noise-induced detections, which produces Eq. (19) :

$$Q_Z = \frac{2 - 2\lambda_A - 2\lambda_B + 3\lambda_A\lambda_B}{4} P_S^A P_S^B$$

An increase in Q_Z with rising λ_A and λ_B signifies a greater proportion of invalid detections, requiring robust error correction to maintain security.

A.3 Derivation of Z-basis effective key rate $Q_Z^{1,1}$

The effective key rate $Q_Z^{1,1}$ isolates the probability of detecting Bell states from different inputs (H_AV_B, V_AH_B), which generate usable key bits critical for the secure keys in MDI-QKD. Unlike the total count rate, this metric focuses solely on valid events that align with the protocol's coding rules in Table. I, directly contributing to the mutual information $I(A:B)$ in the SKR. It is expressed as:

$$Q_Z^{1,1} = \frac{1}{2}\left(P_{\psi^+}^{HV} + P_{\psi^-}^{HV} + P_{\psi^+}^{VH} + P_{\psi^-}^{VH}\right) P_S^A P_S^B \tag{30}$$

Here, the factor $\frac{1}{2}$ averages over the equal probabilities of Alice and Bob selecting opposite polarization states ($|H\rangle_A|V\rangle_B$ or $|V\rangle_A|H\rangle_B$). Substituting the probabilities from A.1.3 into Eq. (30), the result captures only valid detection events, sensitive to the effect of depolarizing noise on reducing the state distinguishability, which produces Eq. (20) :

$$Q_Z^{1,1} = \frac{2 - \lambda_A - \lambda_B + 2\lambda_A\lambda_B}{4} P_S^A P_S^B$$

A decrease in $Q_Z^{1,1}$ with increasing λ_A and λ_B highlights the adverse impact of thermal noise on key generation efficiency.

A.4 Derivation of Z-basis error rate E_Z

The Z-basis error rate E_Z quantifies the fraction of erroneous detections where identical inputs (H_AH_B, V_AV_B) are mistaken for valid Bell states, a consequence of the randomization of the polarization states by thermal noise. This metric is pivotal for determining error correction costs, as it measures the noise-induced deviations that must be reconciled to ensure key consistency:

$$E_Z = \frac{P_{\psi^+}^{HH} + P_{\psi^+}^{VV}}{P_{\psi^+}^{HH} + P_{\psi^+}^{VV} + P_{\psi^+}^{HV} + P_{\psi^-}^{HV} + P_{\psi^+}^{VH} + P_{\psi^-}^{VH}} \tag{31}$$

Here, the numerator sums the probabilities of incorrect projections onto $|\psi^+\rangle$ from identical inputs, while the denominator, equivalent to Q_Z Eq. (19), represents the total detection probability in all input combinations of the Z-basis. Substituting the probabilities from A.1.3 into Eq. (31), the result reflects the impact of depolarizing noise, which yields Eq. (21) from the main text:

$$E_Z = \frac{\lambda_A + \lambda_B - \lambda_A\lambda_B}{2\left(1 - \lambda_A - \lambda_B + \frac{3}{2}\lambda_A\lambda_B\right)}$$

The dependence on λ_A and λ_B underscores the role of thermal noise in increasing error rates, thus reducing the yield of secure keys by increasing the resources needed for error correction.

A.5 Derivation of X-basis error rate $e_X^{1,1}$

The X-basis error rate $e_X^{1,1}$ assesses the potential for eavesdropping by measuring the frequency of incorrect detections in the X-basis, influenced by both depolarizing noise (λ_A, λ_B) and phase noise ($\bar{r}^2$). This metric is essential for security analysis, as it indicates deviations from expected coherent outcomes that an eavesdropper might exploit:

$$e_X^{1,1} = \frac{P_{\psi^-}^{DD} + P_{\psi^+}^{DA}}{P_{\psi^+}^{DD} + P_{\psi^-}^{DD} + P_{\psi^+}^{DA} + P_{\psi^-}^{DA}} \tag{32}$$

Align with the protocol's coding rules in Table. I, the numerator captures error events where $|D\rangle_A|D\rangle_B$ projects onto $|\psi^-\rangle$ or $|D\rangle_A|A\rangle_B$ onto $|\psi^+\rangle$, while the denominator sums all possible X-basis detection probabilities.

Using the probabilities from A.1.3 in Eq. (32), resulting in Eq. (22) :

$$e_X^{1,1} = \frac{2(1-\bar{r}^2)(1+\lambda_A\lambda_B) - (1-2\bar{r}^2)(\lambda_A+\lambda_B)}{4(1-\lambda_A-\lambda_B+2\lambda_A\lambda_B)}$$

An increase in $e_X^{1,1}$ with a decrease in $\bar{r}^2$ indicates the critical role of phase noise in security analysis.

A.6 Derivation of SKR R

The SKR: R quantifies secure key bits, balancing key generation with leakage via the Devetak-Winter bound in:

$$R = I(A:B) - \chi(B:E) = Q_Z^{1,1}[1 - H(e_X^{1,1})] - Q_Z f H(E_Z) \tag{33}$$

Here, $Q_Z^{1,1}[1 - H(e_X^{1,1})]$ represents the secure key fraction after accounting for potential eavesdropping losses in the X basis, while $Q_Z H(E_Z)$ quantifies the information lost to error correction in the Z-basis. The binary entropy function $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ (for $0 < x < 1$, with $H(0) = H(1) = 0$) measures the uncertainty of the error probabilities $e_X^{1,1}$ and E_Z, reflecting the amount of information Eve could gain or must be corrected for.

Combining the results of A.2, A.3, A.4 and A.5 into Eq. (33), the final expression reflects the interplay of noise effects, which produces Eq. (23):

$$\begin{aligned} R &= I(A:B) - \chi(B:E) = Q_Z^{1,1}[1 - H(e_X^{1,1})] - Q_Z f H(E_Z) \\ &= \frac{P_S^A P_S^B}{4}\Bigg[(2-\lambda_A-\lambda_B+2\lambda_A\lambda_B) \quad \left[1 - H\left(\frac{2(1-\bar{r}^2)(1+\lambda_A\lambda_B) - (1-2\bar{r}^2)(\lambda_A+\lambda_B)}{4(1-\lambda_A-\lambda_B+2\lambda_A\lambda_B)}\right)\right] \\ &\quad - (2-2\lambda_A-2\lambda_B+3\lambda_A\lambda_B)\, H\left(\frac{\lambda_A+\lambda_B-\lambda_A\lambda_B}{2\left(1-\lambda_A-\lambda_B+\frac{3}{2}\lambda_A\lambda_B\right)}\right)\Bigg] \end{aligned}$$

We highlight that , thermal noise dominates SKR reduction via Q_Z and E_Z, while phase noise affects $e_X^{1,1}$, shaping security trade-offs, as is detailed in the text.