

# QPE-Inspired Adaptive Phase Tracking for Discrete-Variable Quantum Key Distribution under Unitary Channel Drift

Carlos V. S. Augusto

carloscvsa@ita.br

Instituto Tecnológico de Aeronáutica

Lester A. Faria

Instituto Tecnológico de Aeronáutica

---

## Research Article

**Keywords:** quantum key distribution, BB84, BBM92, quantum phase estimation, phase tracking, QBER, secret-key rate, hybrid quantum-classical feedback, phase drift, quantum communication

**Posted Date:** October 14th, 2026

**DOI:** <https://doi.org/10.21203/rs.3.rs-10168390/v1>

**License:** © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

**Additional Declarations:** No competing interests reported.

---

# QPE-Inspired Adaptive Phase Tracking for Discrete-Variable Quantum Key Distribution under Unitary Channel Drift

Carlos V. S. Augusto<sup>1</sup> and Lester A. Faria<sup>1</sup>

<sup>1</sup> Instituto Tecnológico de Aeronáutica. São Paulo. Brazil.

**Abstract:** Environmental phase drift is a critical impairment in discrete-variable quantum key distribution (DV-QKD), particularly when phase coherence is required for superposition-basis measurements or entanglement-based correlations. This work proposes a QPE-inspired adaptive phase tracking framework for mitigating unitary channel drift in BB84 and BBM92 protocols. Across both evaluated phase-drift regimes, the proposed QPE-inspired tracking framework reduced the mean QBER by factors ranging from approximately 5× to 10× relative to the corresponding untracked baselines. The proposed approach combines a discretized quantum phase-sensing stage with a classical feedback loop, enabling adaptive estimation and compensation of residual phase rotations at the receiver. Unlike full quantum state tomography, the method is designed to operate as a lightweight hybrid quantum-classical feedback mechanism, using phase-sensitive calibration information without explicitly reconstructing the transmitted quantum states. State-vector simulations implemented in Qiskit Aer compare untracked BB84 and BBM92 baselines with the proposed QPE-inspired tracking architecture under stochastic phase drift. Simulations with  $N = 1000$  transmission rounds show that the proposed framework maintains the QBER below the 11% asymptotic threshold for both BB84 and BBM92 under two phase-drift regimes: a moderate fiber-like regime with  $\gamma = 0.04$  rad/round and  $\sigma_{ch} \in [0, 0.35]$  rad, and a high-drift aeronautical regime with  $\gamma = 0.15$  rad/round and  $\sigma_{ch} \in [0.02, 0.25]$  rad. In contrast, the corresponding untracked baselines remain above the threshold and yield vanishing asymptotic secret-key rates. A further intercept-resend scenario is evaluated to verify that non-unitary adversarial disturbances remain observable in the total QBER. The proposed framework is therefore positioned as a simulation-based phase-tracking strategy for DV-QKD under unitary channel noise, rather than as a complete security proof against general attacks.

**Keywords—** quantum key distribution; BB84; BBM92; quantum phase estimation; phase tracking; QBER; secret-key rate, hybrid quantum-classical feedback; phase drift; quantum communication.

## 1. INTRODUCTION

Quantum Key Distribution (QKD) is one of the most mature applications of quantum information science, enabling symmetric key establishment based on the physical principles of quantum mechanics, including the no-cloning theorem and measurement-induced disturbance. Since the proposal of the BB84 protocol by Bennett and Brassard [1], QKD has evolved from foundational quantum cryptography into an active field of quantum communication engineering, where theoretical security guarantees must be reconciled with practical channel impairments, device limitations, and classical post-processing constraints.

Discrete-Variable QKD (DV-QKD) networks rely on two foundational architectures to establish secure cryptographic links. Prepare-and-measure protocols, represented by BB84, encode classical bits into the orthogonal and non-orthogonal bases of single-photon states. Conversely, entanglement-based protocols, such as BBM92 [3], distribute shared entangled pairs (*e.g.*, Bell states) to remote nodes, utilizing non-local quantum correlations to collect a symmetric key. In both settings, the observed Quantum Bit Error Rate (QBER) is a central operational parameter. Under the asymptotic assumptions of the Shor-Preskill security proof, secret-key extraction becomes impossible when the QBER exceeds the well-known threshold of approximately 11% for BB84-like protocols [4]. Therefore, physical mechanisms that increase QBER, even when not caused by eavesdropping, may prematurely suppress secret-key generation.

Existing phase-compensation strategies often rely on classical calibration, optical phase-locked loops, pilot tones, or state-characterization procedures. Although effective in specific settings, these approaches may introduce additional overhead, require dedicated reference resources, or remain weakly connected to the algorithmic structure of quantum information processing. This motivates the investigation of hybrid quantum-classical phase-tracking strategies that can exploit quantum phase-estimation principles while retaining the low-latency adaptability of classical feedback control.

In practical optical fiber and free-space optical implementations, transmitted quantum states are affected by time-varying unitary phase rotations. In fiber links, these rotations may arise from thermal gradients, mechanical stress [5], polarization-related instabilities, and optical path-length fluctuations. In free-space and satellite-oriented scenarios, atmospheric turbulence, pointing variations, and Doppler-related effects may further contribute to dynamic phase noise [6]. If left uncompensated, this phase drift degrades the coherence of diagonal-basis states in BB84 and weakens the correlations of entanglement-based protocols such as BBM92, thereby increasing the observed QBER even in the absence of an adversary.

To mitigate continuous phase decoherence without relying on brute-force tomographic alignment, this paper proposes a QPE-inspired adaptive phase-tracking framework for DV-QKD under unitary channel drift. The framework combines a discretized phase-sensing stage, inspired by quantum phase estimation, with a classical adaptive feedback loop. The estimated residual phase is used to update a receiver-side compensation operation, reducing the impact of channel-induced unitary rotations on the measured QBER. The method is evaluated for both BB84 and BBM92, enabling a comparative analysis between prepare-and-measure and entanglement-based QKD under the same phase-drift model.

The main contributions of this work are as follows:

1. A QPE-inspired phase-estimation framework for adaptive compensation of unitary phase drift in discrete-variable QKD.
2. A hybrid quantum-classical feedback architecture coupling discretized phase estimates to a classical adaptive compensation loop.
3. A comparative simulation study of BB84 and BBM92 under stochastic phase drift, using QBER and asymptotic secret-key rate as performance metrics.
4. An adversarial intercept-resend scenario showing that the proposed tracking mechanism reduces unitary phase noise while preserving the visibility of non-unitary measurement-induced disturbances in the total QBER.

The proposed QPE-inspired architecture is evaluated as a simulation-based phase-tracking layer for DV-QKD. The results suggest that adaptive compensation of unitary channel drift can extend the operating regime in which positive asymptotic secret-key generation remains possible. The proposed method is not intended as a replacement for security proofs, decoy-state analysis, or finite-key treatment. Instead, it is evaluated as a phase-tracking layer designed to reduce QBER contributions associated with unitary channel drift. A separate intercept-resend simulation is included as a limited adversarial test to verify that non-unitary disturbances are not artificially removed by the feedback loop [7].

The remainder of this paper is organized as follows. *Section 2* reviews related work on phase noise, QKD security bounds, low-depth phase estimation, and hybrid quantum-classical feedback. *Section 3* presents the phase-drift model and the QBER propagation mechanisms for BB84 and BBM92. *Section 4* introduces the proposed QPE-inspired adaptive tracking framework. *Section 5* describes the simulation methodology. *Section 6* presents the comparative results under environmental phase drift and intercept-resend attacks, including a discussion of resource overhead and feasibility. *Section 7* concludes the paper and outlines future work.

## **2. RELATED WORK**

The pursuit of robust, high-fidelity QKD in noisy environments requires an interdisciplinary approach spanning optical physics, cryptographic theory, quantum information processing, and digital signal processing. The proposed architecture builds upon foundational security proofs while addressing the practical limitations of modern quantum-classical hardware interfaces.

### **2.1. Environmental Phase Noise in Quantum Channels**

The degradation of quantum states due to continuous environmental phase drift is a well-documented bottleneck in both fiber-optic and FSO networks. In continuous-variable (CV-QKD) and Twin-Field QKD (TF-QKD) implementations, optical phase-locked loops (OPLLs) are routinely employed to maintain coherence between remote local oscillators. However, applying active phase tracking to discrete-variable protocols like BB84 and BBM92 remains challenging due to the fragility of single-photon superposition states.

Recent empirical studies on FSO communication, particularly in aeronautical and satellite-to-ground links, highlight that atmospheric turbulence and Doppler shifts induce severe, high-velocity phase walks. These stochastic disturbances rapidly push the QBER beyond secure thresholds. Existing compensation mechanisms typically rely on resource-intensive quantum state tomography or periodic classical alignment, both of which sacrifice valuable key-generation rounds and struggle to track high-frequency jitter [8].

Despite extensive research on phase stabilization in optical communications, most existing approaches focus on calibration procedures, optical pilot tones, or continuous-variable architectures. Comparatively fewer studies investigate adaptive phase-tracking mechanisms specifically designed for discrete-variable QKD protocols such as BB84 and BBM92.

### **2.2. QBER and Security Constraints in DV-QKD**

Any phase-compensation mechanism used in QKD must be evaluated with respect to the security constraints imposed by the underlying protocol. Under the asymptotic assumptions of the Shor-Preskill proof, the secret-key rate of BB84-like protocols vanishes when the QBER exceeds approximately 11% [9].

Furthermore, recent vulnerability surveys emphasize that non-unitary disturbances, specifically intercept-resend attacks, and Photon Number Splitting (PNS), must remain detectable by the receiver. Therefore, an adaptive phase-tracking layer should reduce QBER contributions associated with unitary environmental drift without artificially suppressing measurement-induced disturbances caused by adversarial interactions [10], [11].

### 2.3. Quantum Phase Estimation in the NISQ Era

QPE is the theoretical gold standard for eigenvalue estimation, but textbook implementations require expensively deep Inverse Quantum Fourier Transform (IQFT) circuits and large ancilla registers. Recent literature focused on the NISQ era has optimized low-depth QPE variations, balancing phase resolution against inherent gate-fidelities [12]. By restricting the phase-estimation resolution to the scale of the optical channel noise, the effective circuit depth can be reduced while avoiding excessive quantization noise in the feedback loop [13].

Recent research has also explored simplified and low-depth phase-estimation techniques intended for practical quantum platforms. Rather than pursuing high-precision eigenvalue extraction, these methods aim to obtain sufficiently accurate phase information for control, calibration, and adaptive optimization tasks. This trend is particularly relevant for communication-oriented applications, where phase estimation often acts as an auxiliary subsystem rather than the primary computational objective.

## 3. PHASE DRIFT MODEL AND PERFORMANCE METRICS

### 3.1. Quantum Channel Phase Drift Model

In real-world optical fiber implementations, the transmitted quantum states are subjected to continuous unitary phase rotations caused by thermal fluctuations, mechanical stress, and spontaneous scattering. We model the accumulated phase drift over discrete transmission rounds  $t$  as a random walk driven by a linear drift rate and Gaussian noise.

Let  $\phi_{ch}(t)$  denote the total channel phase applied to the qubit at round  $t$ . The temporal evolution of the phase is defined as:

$$\phi_{ch}(t) = \phi_{ch}(t-1) - \gamma + N(0, \sigma_{ch}^2) \quad (1)$$

where  $\gamma$  represents the constant deterministic phase drift rate per pulse (in radians), and  $N(0, \sigma_{ch}^2)$  models the stochastic environmental jitter as a zero-mean Gaussian distribution with variance  $\sigma_{ch}^2$ .

The phase-shift unitary operator  $U_{CH}(\phi)$  describes the effect of this channel on a propagating qubit:

$$U_{ch}(\phi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi_{ch}(t)} \end{bmatrix} \quad (2)$$

### 3.2. Protocol Baselines and Error Propagation

The impact of  $U_{CH}(\phi)$  depends inherently on the underlying QKD protocol.

#### 1) *Prepare-and-Measure (BB84):*

Alice prepares discrete quantum states in either the rectilinear (Z) basis  $|0\rangle, |1\rangle$  or the diagonal (X) basis  $|+\rangle, |-\rangle$ . The Z-basis eigenstates are invariant under pure dephasing ( $U_{ch}(\phi)|0\rangle = |0\rangle$ ). However, the X-basis superposition states accumulate a relative phase:

$$U_{ch}(\phi) |+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{i\phi_{ch}(t)} |1\rangle) \quad (3)$$

When Bob measures this state in the X-basis, the probability of an erroneous bit flip,  $P_{\{err|X\}}$ , is strictly a function of the uncorrected phase:

$$P_{err|X} = \sin^2 \left( \frac{\phi_{ch}(t)}{2} \right) \quad (4)$$

#### 2) *Entanglement-Based (BBM92):*

Alice and Bob share a maximally entangled bipartite state, typically a Bell state. The channel noise acts locally on Bob's subsystem, yielding the state:

$$|\Phi_{noisy}^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + e^{i\phi_{ch}(t)} |11\rangle) \quad (5)$$

This degradation in fidelity weakens the non-local correlations, making the protocol highly susceptible to phase-induced QBER if left uncorrected.

### 3.3. Asymptotic Secret-Key Rate Reference

In this work, the Shor-Preskill asymptotic bound is used as a reference for evaluating whether the simulated QBER remains compatible with positive secret-key extraction in BB84-like protocols. The analysis does not constitute a finite-key or composable security proof, nor does it include detector imperfections, decoy-state analysis, or full device-level modeling.

Under asymptotic assumptions and ideal error correction, the secret-key rate  $R$ , measured in secure bits per pulse, can be approximated as:

$$R = \frac{1}{2} \max(0, 1 - 2H_2(Q)) \quad (6)$$

where  $Q$  is the measured QBER and  $H_2(Q)$  is the binary Shannon entropy:

$$H_2(Q) = -Q \log_2(Q) - (1 - Q) \log_2(1 - Q). \quad (7)$$

The root of  $1 - 2H_2(Q) = 0$  occurs at approximately  $Q \approx 0.11002$ , commonly associated with the 11% asymptotic threshold for BB84-like protocols. Therefore, in the present simulations, adaptive phase tracking is evaluated according to its ability to reduce the QBER contribution associated with unitary channel drift and preserve a positive asymptotic secret-key rate.

## 4. THE ADAPTIVE QPE-INSPIRED PHASE TRACKING ARCHITECTURE

To mitigate the continuous environmental drift defined in Section III, we propose a hybrid quantum-classical phase-tracking framework. The architecture uses selected transmission rounds to obtain discretized phase information and applies a classical feedback mechanism to update the receiver-side compensation phase.

Figure 1 presents the overall workflow of the proposed QPE-inspired adaptive phase-tracking framework for both BB84 and BBM92 protocols. The architecture combines a unitary channel drift model, a QPE-inspired phase sensing module, and a classical feedback stage responsible for phase compensation before Bob's measurement process. For evaluation purposes, intercept-resend attacks are introduced as non-unitary disturbances in both protocols.

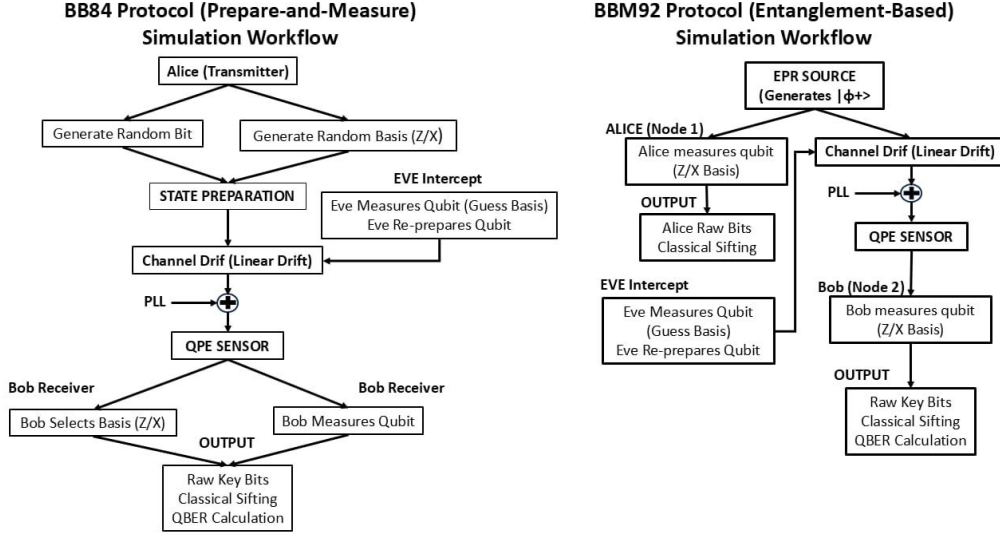


Figure 1 – Overall workflow of the proposed QPE-inspired adaptive phase tracking framework for BB84 and BBM92.

#### 4.1. Quantum Phase Sensing and Ancilla Discretization

Standard continuous-variable tracking destroys the superposition states required for the diagonal (X) basis. To avoid this, the proposed architecture selectively triggers the QPE sub-routine strictly during rectilinear (Z) basis rounds.

When Alice prepares a Z-basis eigenstate (e.g.,  $|1\rangle$ ), the channel drift applies a global phase factor:

$$U_{ch}(\phi_{ch})|1\rangle = e^{i\phi_{ch}}|1\rangle \quad (8)$$

Because this is an eigenstate of the phase operator, the QPE circuit can map this phase onto an auxiliary register of  $n$  ancilla qubits via controlled-phase (CP) operations and an IQFT, without disturbing the measurement statistics of the primary data qubit.

The ideal continuous residual phase in the channel at round  $t$  is defined as:

$$\phi_{res}(t) = \phi_{ch}(t) - \phi_{est}(t-1) \quad (9)$$

However, the QPE measurement yields a classical  $n$ -bit string  $m$ , which discretizes the phase estimate into  $2^n$  bins. The measured residual phase is thus parsed as:

$$\phi_{meas}(t) = \frac{m}{2^n} 2\pi \quad (10)$$

To prevent phase-wrapping artifacts resulting from the circular geometry of the phase space, the measured value must be strictly bounded to the  $[-\pi, \pi]$  interval.

$$\phi'_{meas}(t) = \arctan2(\sin(\phi_{meas}(t)), \cos(\phi_{meas}(t))) \quad (11)$$

The resolution of the QPE sensor is inherently bounded by  $\Delta\phi = \frac{2\pi}{2^n}$ . For the hybrid controller to successfully track channel drift, the ancilla-register size must provide a phase discretization compatible with the characteristic scale of the simulated phase variations while avoiding excessive quantization effects.

In the BB84 configuration, a 6-ancilla register ( $\Delta\phi \approx 0.09$  rad) was empirically sufficient to stabilize the prepare-and-measure protocol. In contrast, the more phase-sensitive BBM92 configuration required an 8-ancilla register ( $\Delta\phi \approx 0.024$  rad) to reduce residual correlation degradation and maintain stable entanglement-based operation.

Unlike canonical Quantum Phase Estimation (QPE), where the ancilla-controlled operations apply successive powers of the target unitary operator  $U^{2^k}$ , the proposed framework employs identical controlled-phase operations  $CP(\pi/4)$  across the ancilla register. This modification was introduced to simplify the phase-sensing stage and adapt the estimation mechanism to a communication-oriented phase-tracking scenario rather than a quantum computing task. Consequently, the proposed circuit should be interpreted as a QPE-inspired phase estimation framework, preserving the concept of ancilla-assisted phase sensing while avoiding the circuit complexity associated with standard QPE implementations.

The objective of this adaptation is not to reproduce the full functionality of canonical QPE, but rather to obtain discretized phase information sufficient for feedback control and adaptive compensation of channel-induced unitary drift. Therefore, the emphasis of the proposed architecture lies in phase tracking performance and QBER mitigation within DV-QKD protocols, rather than in high-precision eigenvalue estimation.

## 4.2. Classical Feedback Loop

The phase estimate generated by the QPE-inspired sensing module is processed by a classical feedback loop responsible for smoothing measurement fluctuations and updating the compensation phase applied at the receiver.

In the present proof-of-concept implementation, the feedback gain was empirically adjusted to maximize phase-tracking stability while avoiding oscillatory behavior. Excessively large gains produced overshoot and increased QBER, whereas excessively small gains reduced the ability of the tracker to follow dynamic channel drift.

The gain values adopted in the simulations were 0.7 for BB84 and 0.4 for BBM92. These values should not be interpreted as globally optimal controller parameters, but rather as empirically selected operating points for the simulated scenarios.

#### 4.3. Pre-Compensation and Predictive Hold

The generated  $\phi_{est}(t)$  dictates the unitary correction applied to Bob's measurement device. A classical voltage is applied to a phase modulator to execute the inverse unitary immediately prior to Bob's basis selection:

$$U_{corr} = U_{ch}(-\phi_{est}(t)) \quad (12)$$

Crucially, because the QPE sensor is only triggered during Z-basis rounds (50% of the transmission over time), the PLL experiences periodic data starvation. During X-basis data-generation rounds, the controller enters a predictive hold state. To prevent the estimate from becoming stale, the controller mathematically extrapolates the phase using the known loop velocity:

$$\phi_{est}(t) = \phi_{est}(t-1) + \gamma_{pred} \quad (13)$$

This predictive hold ensures that the pre-compensation remains tightly aligned with  $\phi_{ch}(t)$  even when active quantum sensing is temporarily suspended to preserve X-basis superposition.

### 5. SIMULATION METHODOLOGY

To evaluate the proposed hybrid quantum-classical tracking architecture, we developed a state-vector simulation framework using the Qiskit Aer simulator [15]. The simulation compares the performance of untracked protocols against the proposed QPE-inspired feedback architecture across varying levels of environmental noise and adversarial interception.

#### 5.1. Channel and Protocol Parameters

The phase-drift model was evaluated under two operating regimes. In the moderate fiber-like regime, the deterministic drift rate was set to  $\gamma = 0.04$  rad/round and the phase-noise standard deviation was swept from 0 to 0.35 rad. In the high-drift

aeronautical regime, the deterministic drift rate was increased to  $\gamma = 0.15$  rad/round and the phase-noise standard deviation was swept from 0.02 to 0.25 rad. These regimes were selected to compare the behavior of the proposed tracking framework under moderate and dynamically severe phase-drift conditions.

Two baseline protocols were evaluated: *i.* the prepare-and-measure BB84 protocol; and *ii.* the entanglement-based BBM92 protocol. For each regime, tracked BB84 and BBM92 configurations were compared with their corresponding untracked baselines using QBER and asymptotic secret-key rate as performance metrics. All updated simulations used  $N = 1000$  transmission rounds per configuration and a fixed random seed of 42.

This study reports representative results obtained using a fixed random seed (42). The objective is to evaluate the behavior of the proposed QPE-inspired tracking framework under controlled and reproducible conditions. A broader Monte Carlo analysis involving multiple random seeds, confidence intervals, and statistical significance assessment is left for future work.

## 5.2. Simulation Configurations

To ensure adequate phase resolution for each protocol, the QPE sensor and classical feedback loop were tuned according to the sensitivity of the simulated QKD architecture

### 1. BB84 Configuration:

The BB84 configuration used a 6-qubit ancilla register and an empirical feedback gain of 0.7. This larger gain was selected to improve the tracking response in the prepare-and-measure configuration.

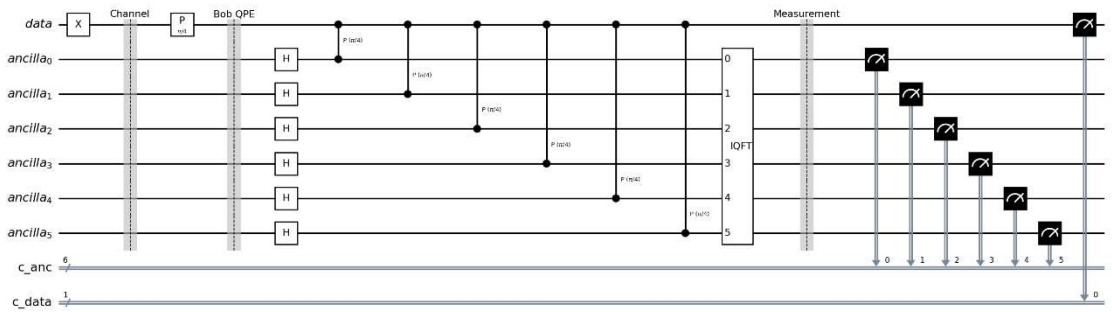


Figure 2 – BB84 QPE PLL Circuit

In Figure 2, let's consider the data qubit as  $d$  and ancilla register as  $a_0, a_1, a_2, a_3, a_4, a_5$ . So, the Initial full state is:

$$|\psi_0\rangle = |0\rangle_d \otimes |000000\rangle_a \quad (14)$$

The following steps of the circuit: *i.* apply  $X$  to the data qubit; *ii.* apply  $P(\pi/4)$  to the data qubit; *iii.* apply  $H$  to all 6 ancillas; and *iv.* phase added by all six CP gates. So, after all 6 CP gates:

$$|\psi_4\rangle = \frac{1}{8} \sum_{a \in \{0,1\}^6} e^{i\frac{\pi}{4}w(a)} |a\rangle_a \otimes |1\rangle_d \quad (15)$$

Because each ancilla receives the same phase pattern, the ancilla register can also be written as a tensor product. After, the IQFT is applied to the 6-qubit ancilla register. Therefore, the measurement probability of ancilla output  $z$  is:

$$p(z) = |\alpha_z|^2 = \frac{1}{64^2} \prod_{k=0}^5 |1 + e^{i\pi/4} e^{-2\pi i z 2^k / 64}|^2 \quad (16)$$

Appendix A contains all the step-by-step equations, in detail, for circuit BB84 with QPE-inspired.

## 2. BBM92 Configuration:

The BBM92 configuration used an 8-qubit ancilla register and a lower empirical feedback gain of 0.4. This more conservative configuration was adopted to reduce overshoot effects and preserve bipartite correlation stability under the simulated phase-drift model.

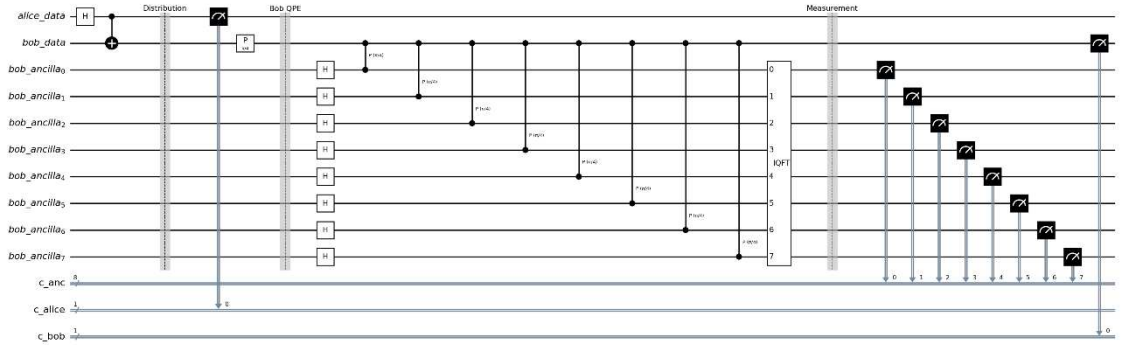


Figure 3 – BBM92 QPE PLL Circuit

In Figure 3, let's consider Alice's qubit as  $A$ , Bob's qubit as  $B$  and Bob's 8-qubit ancilla register as  $R$ . The initial entanglement state is:

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}} (|00\rangle_{AB} + |11\rangle_{AB}) \otimes |00000000\rangle_R \quad (17)$$

The following steps for the circuit: *i.* applying  $H$  gates to Bob's 8 ancillas; *ii.* if Bob's data qubit is  $|0\rangle_B$ , then no CP gate contributes any phase; *iii.* every ancilla bit equal to 1 contributes a phase  $e^{i\pi/4}$ .

The ancilla state after IQFT is:

$$|\Psi_{A=1}^{(4)}\rangle = |1\rangle_A |1\rangle_B \otimes \sum_{z=0}^{255} \alpha_z |z\rangle_R \quad (18)$$

Appendix B contains all the step-by-step equations, in detail, for the circuit BBM92 with QPE-inspired.

### 5.3. Adversarial Attack Model

To evaluate whether the phase-tracking mechanism preserves the visibility of non-unitary disturbances, an intercept-resend adversarial model was included. Eve executes a strict intercept-resend attack on a defined fraction of the transmitted pulses ( $P_{eve}$ ). She chooses a measurement basis  $\{Z, X\}$  at random, collapses the state, and resends it to Bob. This introduces a non-unitary disturbance that should remain observable in the QBER, since the proposed feedback loop is designed to compensate unitary phase drift rather than adversarial measurement effects.

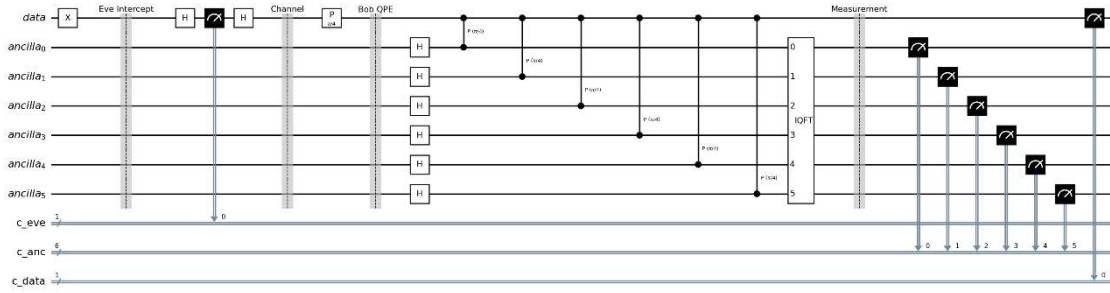


Figure 4 – BB84 QPE PLL with Eavesdropper

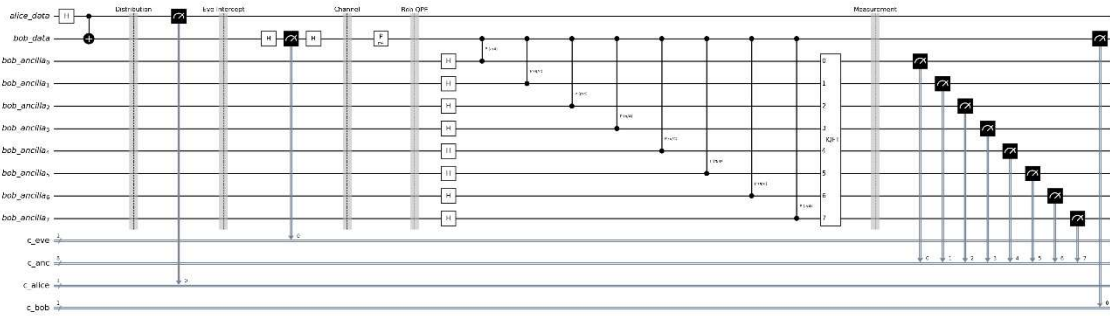


Figure 5 – BBM92 QPE PLL with Eavesdropper

The quantum states analysis following the same idea of the circuit without eavesdropper attack, only added a measurement, simulating an intercept attack.

The present simulations extend the initial proof-of-concept analysis by increasing the number of transmission rounds to  $N = 1000$  and by evaluating two distinct phase-drift regimes. A broader Monte Carlo analysis with multiple random seeds is left for future work.

## 6. RESULTS AND COMPARATIVE ANALYSIS

The performance of the proposed architecture was evaluated under three simulation conditions: **i.** a moderate fiber-like unitary phase-drift regime; **ii.** a high-drift aeronautical phase-noise regime; and **iii.** a limited intercept-resend adversarial scenario.

In the first two regimes, tracked BB84 and BBM92 protocols were compared against their corresponding untracked baselines using QBER and asymptotic secret-key rate as performance metrics. The adversarial scenario was used as a limited test to verify whether non-unitary disturbances remain observable after phase compensation.

### 6.1. Moderate Fiber-Like Phase-Drift Scenario

Figure 6 presents the QBER and asymptotic secret-key rate obtained for BB84 and BBM92 under a moderate fiber-like phase-drift scenario. The simulation uses  $N = 1000$  transmission rounds, random seed 42, drift rate  $\gamma = 0.04$  rad/round, and phase-noise standard deviation ranging from 0 to 0.35 rad.

For both protocols, the untracked baselines remain consistently above the 11% asymptotic threshold, leading to a vanishing secret-key rate across the evaluated noise range. This confirms that uncompensated unitary phase drift is sufficient to suppress key generation under the adopted performance model.

In contrast, the QPE-inspired adaptive tracking framework maintains the QBER below the asymptotic threshold for both BB84 and BBM92 throughout the evaluated interval. In BB84, the tracked QBER remains low even as the phase-noise standard deviation approaches 0.35 rad, preserving a positive secret-key rate over the full simulated range. BBM92 also benefits from the tracking mechanism, although its secret-key rate decreases more sharply at higher noise levels, indicating greater sensitivity of entanglement-based correlations to residual phase-estimation errors.

These results strengthen the evidence that the proposed architecture primarily acts as a unitary phase-drift compensation layer. The separation between the tracked and untracked curves indicates that the QPE-inspired phase-sensing stage and classical feedback loop can substantially reduce phase-induced QBER without requiring full state tomography.

Table I summarizes the observed behavior across the two simulated phase-drift regimes. In both regimes, the untracked baselines remain above the asymptotic QBER threshold and therefore yield zero asymptotic secret-key rate. In contrast, the QPE-inspired tracking configurations remain below the threshold for both BB84 and BBM92, preserving positive key generation across the evaluated noise ranges.

The comparison indicates that the proposed tracking layer is effective in both moderate and high-drift regimes. BB84 exhibits more stable secret-key generation, whereas BBM92 shows stronger degradation at higher noise levels, consistent with the greater sensitivity of entanglement-based correlations to residual phase-estimation errors.

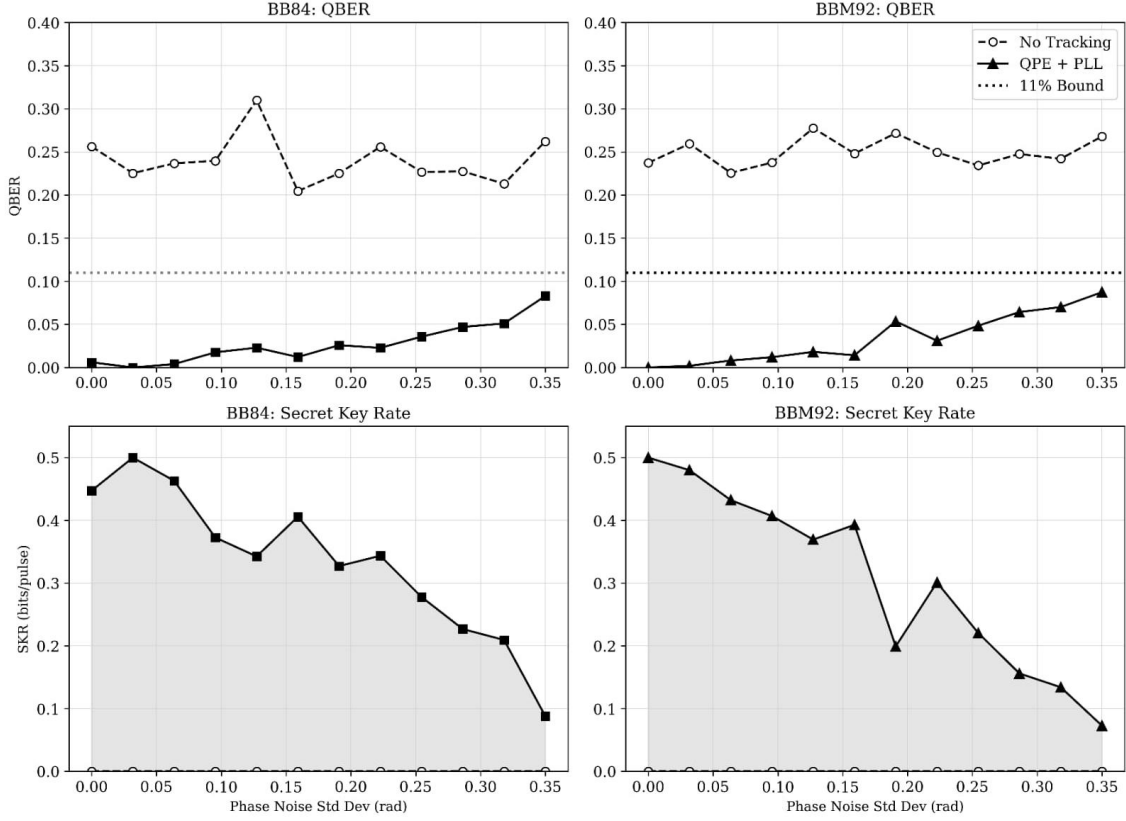


Figure 6. QBER and asymptotic secret-key rate comparison for BB84 and BBM92 under a moderate fiber-like phase-drift scenario. The simulation uses  $N = 1000$  transmission rounds, random seed 42, drift rate  $\gamma = 0.04$  rad/round, and phase-noise standard deviation ranging from 0 to 0.35 rad.

## 6.2. High-Drift Aeronautical Phase-Noise Scenario

Figure 7 evaluates the same adaptive tracking framework under a more dynamically severe phase-noise regime, representative of aeronautical or free-space optical conditions. In this scenario, the deterministic drift rate is increased to  $\gamma = 0.15$  rad/round, while the phase-noise standard deviation ranges from 0.02 to 0.25 rad.

Despite the higher drift rate, the tracked BB84 configuration maintains QBER values well below the 11% asymptotic threshold over the full noise interval. The corresponding secret-key rate remains positive, although it decreases as the phase-noise standard deviation increases. This behavior indicates that the feedback loop can follow substantially faster phase evolution than in the moderate-drift case.

The BBM92 configuration also remains below the QBER threshold in the evaluated interval, but its secret-key rate exhibits stronger degradation as the noise increases. This result is consistent with the greater sensitivity of entanglement-based protocols to residual phase errors and reinforces the need for a higher ancilla-register resolution and a more conservative feedback gain in BBM92.

Overall, the high-drift scenario supports the applicability of the proposed architecture beyond quasi-static fiber-like channels, suggesting potential relevance for dynamic free-space or aeronautical quantum communication links. However, this interpretation remains simulation-based and does not include atmospheric loss, pointing errors, detector noise, or finite-key effects.

*Table 1 - Summary of QBER and asymptotic secret-key rate behavior under moderate fiber-like and high-drift aeronautical phase-noise regimes*

| Scenario                   | Protocol | Tracking         | Drift rate<br>( $\gamma$ ) | Noise range<br>( $\sigma_{\text{ch}}$ ) | QBER<br>behavior   | Secret-Key<br>rate<br>behavior |
|----------------------------|----------|------------------|----------------------------|-----------------------------------------|--------------------|--------------------------------|
| Moderate<br>fiber-like     | BB84     | No               | 0.04                       | 0–0.35                                  | Above<br>threshold | Zero                           |
| Moderate<br>fiber-like     | BB84     | QPE-<br>inspired | 0.04                       | 0–0.35                                  | Below<br>threshold | Positive                       |
| Moderate<br>fiber-like     | BBM92    | No               | 0.04                       | 0–0.35                                  | Above<br>threshold | Zero                           |
| Moderate<br>fiber-like     | BBM92    | QPE-<br>inspired | 0.04                       | 0–0.35                                  | Below<br>threshold | Positive,<br>decreasing        |
| Aeronautical<br>high-drift | BB84     | No               | 0.15                       | 0.02–0.25                               | Above<br>threshold | Zero                           |
| Aeronautical<br>high-drift | BB84     | QPE-<br>inspired | 0.15                       | 0.02–0.25                               | Below<br>threshold | Positive                       |
| Aeronautical<br>high-drift | BBM92    | No               | 0.15                       | 0.02–0.25                               | Above<br>threshold | Zero                           |
| Aeronautical<br>high-drift | BBM92    | QPE-<br>inspired | 0.15                       | 0.02–0.25                               | Below<br>threshold | Positive,<br>decreasing        |

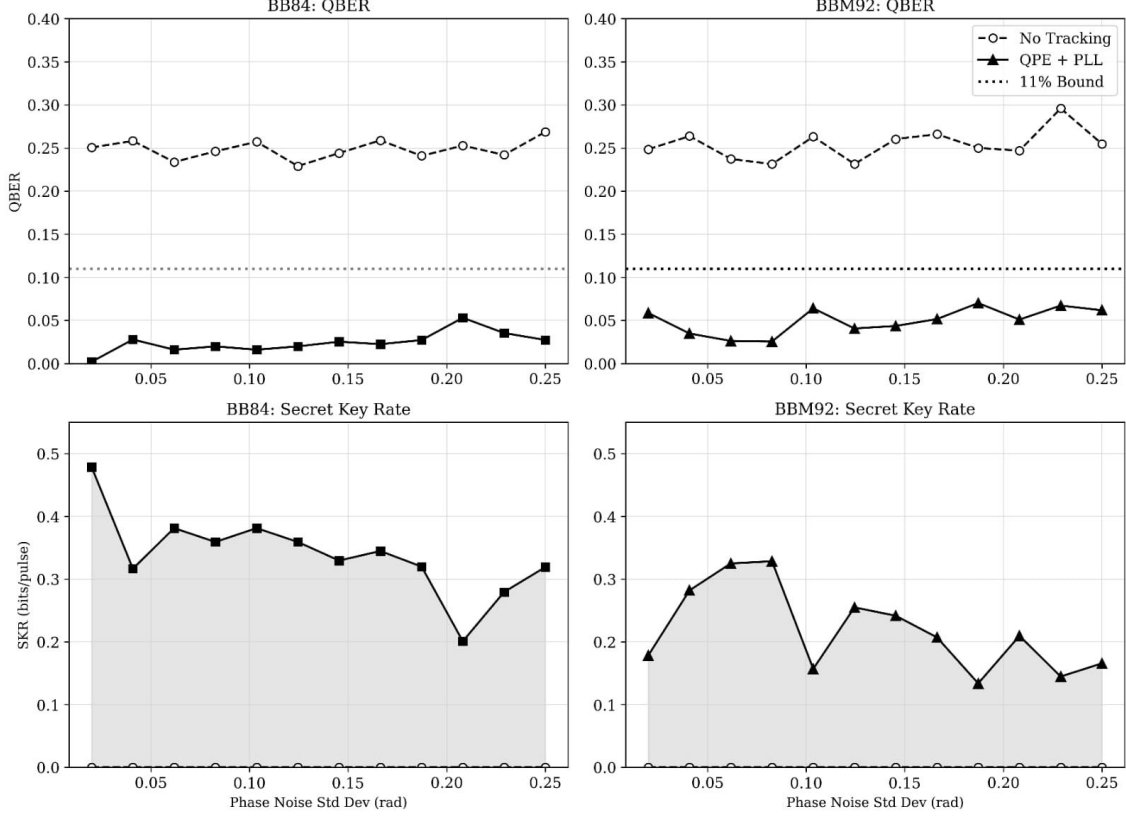


Figure 7. QBER and asymptotic secret-key rate comparison for BB84 and BBM92 under a high-drift aeronautical phase-noise scenario. The simulation uses  $N = 1000$  transmission rounds, random seed 42, drift rate  $\gamma = 0.15$  rad/round, and phase-noise standard deviation ranging from 0.02 to 0.25 rad.

Table II and III show the mean and the standard deviation of the QBER and secret-key rate values comparing the QPE-inspired method with no tracking phase method, from both scenarios, a noisier physical environment and aeronautics regime.

Across both evaluated phase-drift regimes, the proposed QPE-inspired tracking framework reduced the mean QBER by approximately one order of magnitude relative to the corresponding untracked baselines. This reduction enabled positive asymptotic secret-key generation in all tracked configurations, whereas the untracked protocols yielded vanishing secret-key rates throughout the evaluated noise ranges.

### 6.3. Intercept-Resend Adversarial Scenario

To evaluate whether the proposed phase-tracking mechanism preserves the visibility of adversarial disturbances, an intercept-resend scenario was introduced under the same number of transmission rounds and the moderate fiber-like drift configuration. Figures 8 and 9 show the evolution of QBER and asymptotic secret-key rate as Eve's interception probability increases, for BB84 and BBM92 protocols. This test is not intended as a full security analysis, but as a consistency check to verify whether the

proposed compensation mechanism suppresses only unitary phase drift while preserving observable QBER increases caused by non-unitary measurement disturbances.

Table 2 - Quantitative summary for the moderate fiber-like phase-drift regime

| Environment           | Protocol | Method      | QBER Mean | QBER Std Dev | Secret-key Mean (bits/pulse) | Secret-key Std Dev |
|-----------------------|----------|-------------|-----------|--------------|------------------------------|--------------------|
| Fiber physical regime | BB84     | No Tracking | 0.239     | 0.025        | 0                            | 0                  |
|                       |          | QPE + PLL   | 0.027     | 0.022        | 0.336                        | 0.120              |
|                       | BBM92    | No Tracking | 0.250     | 0.016        | 0                            | 0                  |
|                       |          | QPE + PLL   | 0.034     | 0.030        | 0.306                        | 0.130              |

Table 3 - Quantitative summary for the high-drift aeronautical phase-noise regime

| Environment        | Protocol | Method      | QBER Mean | QBER Std Dev | Secret-key Mean (bits/pulse) | Secret-key Std Dev |
|--------------------|----------|-------------|-----------|--------------|------------------------------|--------------------|
| Aeronautics regime | BB84     | No Tracking | 0.248     | 0.012        | 0                            | 0                  |
|                    |          | QPE + PLL   | 0.024     | 0.013        | 0.339                        | 0.077              |
|                    | BBM92    | No Tracking | 0.255     | 0.018        | 0                            | 0                  |
|                    |          | QPE + PLL   | 0.047     | 0.015        | 0.225                        | 0.068              |

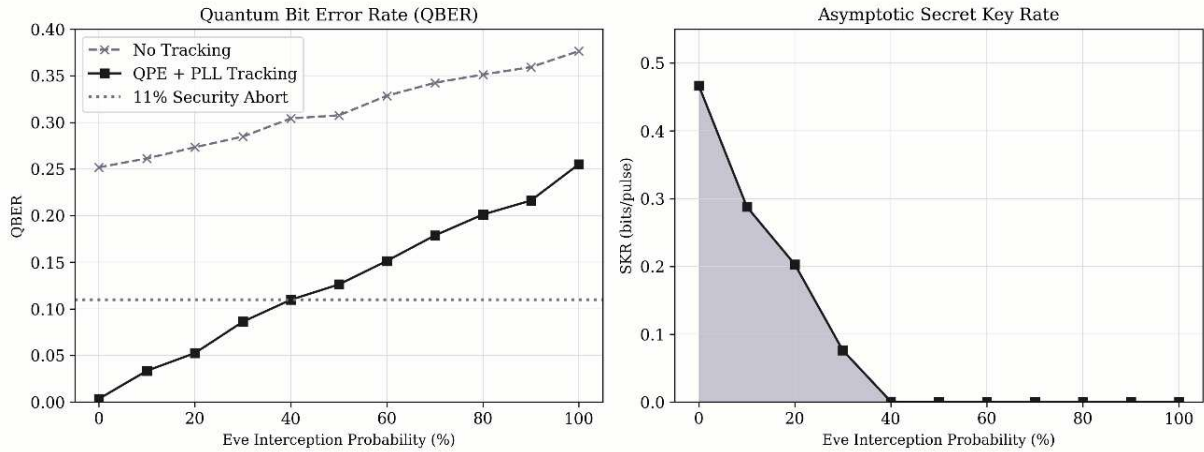


Figure 8 - QBER comparison for BB84 under intercept-resend attack. This adversarial test evaluates whether the phase-tracking layer preserves observable QBER increases associated with non-unitary measurement disturbances.

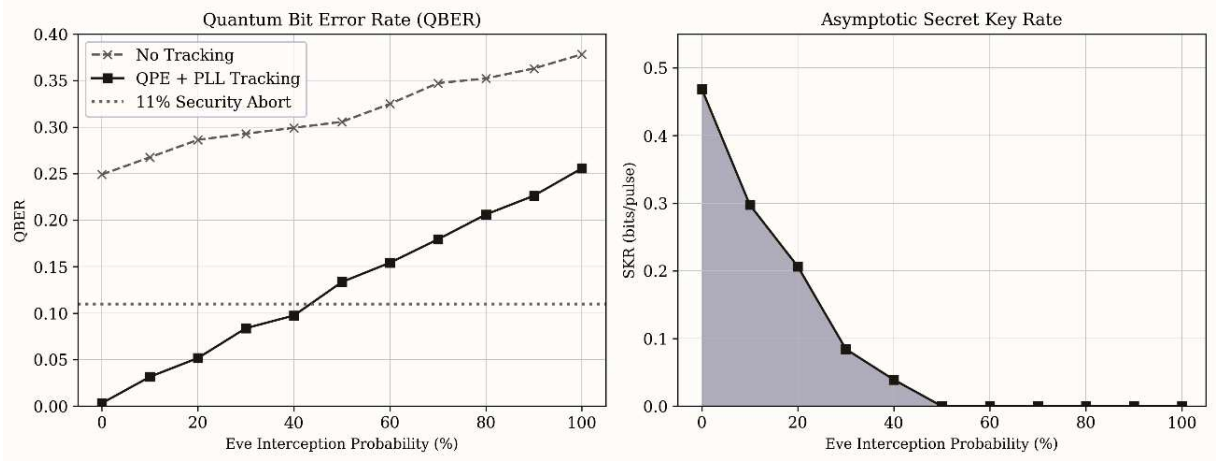


Figure 9 - QBER comparison for BBM92 under intercept-resend attack. This adversarial test evaluates whether the phase-tracking layer preserves observable QBER increases associated with non-unitary measurement disturbances.

For both BB84 and BBM92, the untracked baselines remain above the 11% asymptotic threshold across the evaluated interception range. In contrast, the QPE-inspired tracking configuration reduces the environmental contribution to QBER, allowing the adversarial disturbance to be observed more clearly as Eve's interception probability increases. The tracked configuration remains below the asymptotic threshold only for low-to-moderate interception probabilities and exceeds it as the adversarial disturbance becomes dominant.

These results should be interpreted as a consistency check rather than a complete security analysis. The proposed framework compensates unitary channel drift but does not remove the non-unitary disturbance introduced by intercept-resend measurements. Therefore, the phase-tracking layer can improve operational robustness against environmental phase noise while preserving the QBER signature associated with adversarial measurements within the adopted simulation model.

#### 6.4. Resource Overhead and Hardware Feasibility

While the proposed QPE-inspired hybrid tracking architecture demonstrates QBER reduction in simulation, its practical deployment would depend on the physical feasibility of the receiver-side quantum and classical processing stages.

It is important to note that the present work focuses on algorithmic feasibility and simulation-based validation. No hardware implementation was performed in this work, and the resource estimates presented in this section should therefore be interpreted as preliminary indicators of practical deployment complexity.

The standard IQFT algorithm requires a circuit depth of  $O(n^2)$  and relies heavily on precise two-qubit CP operations:

- *BB84 Requirements:* The 6-ancilla configuration requires 15 CP gates and 6 H gates per calibration round.
- *BBM92 Requirements:* The 8-ancilla configuration necessitates 28 CP gates and 8 H gates.

For NISQ devices, executing 28 sequential CP gates introduces intrinsic gate errors that could rival the environmental channel noise the system is attempting to correct. Consequently, for strictly near-term deployments, lighter directional Classical Phase Estimation (CPE) methods utilizing single probe qubits may be preferable despite their lower asymptotic precision.

Compared with full quantum state tomography, the proposed approach is intended to reduce measurement overhead by extracting phase information rather than reconstructing the complete quantum state.

As quantum networks transition from NISQ to early fault-tolerant regimes with integrated error correction, the ability to obtain low-depth discretized phase estimates using 6 to 8 ancilla qubits may support scalable receiver-side phase tracking for long-haul quantum communication links.

*The resource estimates reported here are intended primarily as comparative indicators of algorithmic complexity. Since the present work focuses on simulation-based validation of a QPE-inspired phase-tracking strategy, the reported values should not be interpreted as optimized hardware requirements for a practical deployment.*

## 7. CONCLUSION AND FUTURE WORK

This paper presented a QPE-inspired adaptive phase-tracking framework for discrete-variable quantum key distribution under unitary channel drift. The proposed approach combines ancilla-assisted phase sensing with a classical feedback mechanism to compensate accumulated phase rotations before quantum-state measurement.

State-vector simulations with  $N = 1000$  transmission rounds indicate that the proposed framework reduces QBER and preserves positive asymptotic secret-key rates relative to conventional untracked BB84 and BBM92 baselines. Under a moderate fiber-like phase-drift regime with  $\gamma = 0.04$  rad/round and  $\sigma_{ch}$  up to 0.35 rad, both tracked protocols remained below the 11% asymptotic threshold, whereas the untracked baselines remained above it. Under a high-drift aeronautical regime with  $\gamma = 0.15$  rad/round, the framework also maintained positive key generation across the evaluated noise range, although BBM92 exhibited stronger degradation at higher noise levels.

Additional simulations incorporating intercept-resend attacks indicate that the proposed tracking layer reduces the unitary environmental contribution to QBER while preserving the observable QBER increase associated with adversarial measurements. The tracked configuration remains compatible with positive asymptotic key generation only under low-to-moderate interception probabilities and fails once the total QBER exceeds the adopted threshold. Therefore, these results should be interpreted as an adversarial consistency check, not as a replacement for a complete QKD security proof.

The principal contribution of this work is therefore not a new security proof, but a communication-oriented phase-estimation strategy inspired by quantum phase estimation concepts. The results demonstrate that low-depth, QPE-inspired adaptive tracking may represent a promising direction for improving the operational robustness of DV-QKD systems under dynamic phase-noise conditions.

### 7.1. Future Work

Future development of this architecture will proceed along three primary engineering tracks:

1. *Hardware-in-the-Loop Emulation:* Implementing the classical PLL on a Field-Programmable Gate Array (FPGA) to evaluate the real-time latency limits of the feedback loop. High-speed hardware execution is required to ensure the predictive equations do not become stale during X-basis data bursts.
2. *Integration with Decoy-State Protocols:* The current adversarial model is limited to single-photon intercept-resend attacks. Integrating the QPE feedback loop with intensity-modulated decoy states is necessary to evaluate the architecture's resilience against comprehensive PNS attacks in severely attenuated fiber channels.
3. *Extended Monte Carlo Validation and Gain Optimization:* Future work will evaluate the framework over multiple random seeds, larger transmission ensembles, feedback-gain sweeps, and ancilla-register configurations to quantify statistical confidence intervals and identify optimal operating regions for BB84 and BBM92.
4. *Extension to Additional QKD Architectures and Network Initialization Strategies:* Future work will investigate the applicability of the proposed QPE-inspired tracking framework to alternative quantum communication protocols, including distributed phase-reference schemes such as Coherent One-Way (COW). In addition, advanced network initialization strategies will be explored to reduce acquisition latency during link establishment, including the use of

quantum-assisted calibration and phase-estimation routines capable of providing faster convergence under severe channel drift conditions.

## REFERENCES

- [1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," \*Proceedings of IEEE International Conference on Computers, Systems and Signal Processing\*, 1984.
- [2] F. Burt, K. -C. Chen and K. K. Leung, "Entanglement-Efficient Distribution of Quantum Circuits Over Large-Scale Quantum Networks," 2025 IEEE International Conference on Quantum Computing and Engineering (QCE), Albuquerque, NM, USA, 2025, pp. 1111-1122, Doi: 10.1109/QCE65121.2025.00125.
- [3] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," \*Physical Review Letters\*, vol. 68, no. 5, p. 557, 1992. [4] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," \*Physical Review Letters\*, vol. 85, no. 2, p. 441, 2000.
- [5] N. V. Nardelli, L. K. Shalm, M. D. Mazurek and T. M. Fortier, "Enabling Phase-Stable Quantum Protocols Over Optical Fiber Networks," 2024 Conference on Lasers and Electro-Optics (CLEO), Charlotte, NC, USA, 2024, pp. 1-2.
- [6] T. Ismail, A. H. Sabeeh and N. Alshaer, "Challenges and Applications of Integrated mmWave/FSO QKD-based Communication Systems for Secure and High-Capacity Networks," 2025 25th Anniversary International Conference on Transparent Optical Networks (ICTON), Barcelona, Spain, 2025, pp. 1-6, Doi: 10.1109/ICTON67126.2025.11125333.
- [7] W. Zita and M. Malkawi, "Quantum-Safe Countermeasures: Mitigating Detector-Blinding Attacks in Quantum Key Distribution Systems," 2026 14th International Symposium on Digital Forensics and Security (ISDFS), Boston, MA, USA, 2026, pp. 1-6, Doi: 10.1109/ISDFS69419.2026.11458942.
- [8] Yichen Zhang, Yiming Bian, Zhengyu Li, Song Yu, Hong Guo. Continuous-variable quantum key distribution system: past, present, and future. *Appl. Phys. Rev.* 11, 011318 (2024). <https://doi.org/10.1063/5.0179566>.
- [9] P. W. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, 2000. <https://doi.org/10.1103/PhysRevLett.85.441>
- [10] B. Mallick et al., "Multi-Channel Multi-Protocol Quantum Key Distribution System for Secure Image Transmission in Healthcare," in *IEEE Access*, vol. 13, pp. 62476-62505, 2025, Doi: 10.1109/ACCESS.2025.3558294.
- [11] Aitor Brazaola-Vicario et al. "Quantum key distribution: a survey on current vulnerability trends and potential implementation risks". *Opt. Continuum* 3, 1438-1460 (2024).
- [12] Hongkang Ni, Haoya Li, Lexing Ying. On low-depth algorithms for quantum phase estimation. *Quantum* 7, 1165 (2023). <https://doi.org/10.22331/q-2023-11-06-1165>.
- [13] Md Mostoba Rafid et al. Quantum Computing Applications in High-Speed Signal Processing for EEE Systems. *International Journal of Engineering Business and Management*. October 2024. DOI:10.22161/ijebm.8.4.7.
- [15] Qiskit framework. <https://pypi.org/project/qiskit-aer/>. Accessed 05/04/26.

## APPENDIX A – BB84 Derivation:

The Initial full state is:

$$|\psi_0\rangle = |0\rangle_d \otimes |000000\rangle_a \quad (1)$$

Apply  $X$  to the data qubit, since  $X|0\rangle = |1\rangle$ :

$$|\psi_1\rangle = X_d |\psi_0\rangle \quad (2)$$

$$|\psi_1\rangle = |1\rangle_d \otimes |000000\rangle_a \quad (3)$$

Now apply  $P(\pi/4)$  to the data qubit and since the data qubit is  $|1\rangle$ :

$$|\psi_2\rangle = P(\pi/4)_d |\psi_1\rangle \quad (4)$$

$$P(\pi/4)|1\rangle = e^{i\pi/4}|1\rangle \quad (5)$$

$$|\psi_2\rangle = e^{i\pi/4}|1\rangle_d \otimes |000000\rangle_a \quad (6)$$

Apply  $H$  to all 6 ancillas, where each ancilla starts in  $|0\rangle$ , so after a Hadamard ( $H$ ). Therefore the 6-ancilla register becomes:

$$(H^{\otimes 6})|000000\rangle = \frac{1}{\sqrt{2^6}} \sum_{y=0}^{63} |y\rangle = \frac{1}{8} \sum_{y=0}^{63} |y\rangle \quad (7)$$

So, the total state is:

$$|\psi_3\rangle = e^{i\pi/4}|1\rangle_d \otimes \frac{1}{8} \sum_{y=0}^{63} |y\rangle_a \quad (8)$$

The total phase added by all six CP gates is:

$$e^{i\frac{\pi}{4}(a_0+a_1+a_2+a_3+a_4+a_5)} \quad (9)$$

So, after all 6 CP gates:

$$|\psi_4\rangle = \frac{1}{8} \sum_{a \in \{0,1\}^6} e^{i\frac{\pi}{4}w(a)} |a\rangle_a \otimes |1\rangle_d \quad (10)$$

where:

$$w(a) = a_0 + a_1 + a_2 + a_3 + a_4 + a_5 \quad (11)$$

Because each ancilla receives the same phase pattern, the ancilla register can also be written as a tensor product:

$$|\psi_4\rangle = \bigotimes_{k=0}^5 \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}} \otimes |1\rangle_d \quad (12)$$

So, each ancilla state after its H + CP pair is:

$$|a_k^{(\text{after CP})}\rangle = \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}} \quad (13)$$

Now the IQFT is applied to the 6-qubit ancilla register:

$$QFT^{-1} |y\rangle = \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} e^{-2\pi i y z / N} |z\rangle \quad (14)$$

Thus, if:

$$|\phi\rangle_a = \frac{1}{8} \sum_{y=0}^{63} c_y |y\rangle \quad (15)$$

Then after IQFT:

$$QFT^{-1} |\phi\rangle_a = \sum_{z=0}^{63} \alpha_z |z\rangle \quad (16)$$

With amplitudes:

$$\alpha_z = \frac{1}{64} \sum_{y=0}^{63} c_y e^{-2\pi i y z / 64} \quad (17)$$

Because every ancilla has the same phase gate  $CP(\pi/4)$ , we have:

$$c_y = e^{i\frac{\pi}{4}w(y)} \quad (18)$$

So, the ancilla output after IQFT is:

$$|\psi_5\rangle = \sum_{z=0}^{63} \alpha_z |z\rangle_a \otimes |1\rangle_d \quad (19)$$

Because the pre-IQFT ancilla state is a tensor product, the amplitude can be factorized:

$$\alpha_z = \frac{1}{64} \prod_{k=0}^5 \left( 1 + e^{i\pi/4} e^{-2\pi i z 2^k / 64} \right) \quad (20)$$

Therefore, the measurement probability of ancilla output  $z$  is:

$$p(z) = |\alpha_z|^2 = \frac{1}{64^2} \prod_{k=0}^5 |1 + e^{i\pi/4} e^{-2\pi i z 2^k / 64}|^2 \quad (21)$$

Using:

$$|1 + e^{i\theta}|^2 = 4\cos^2(\theta/2) \quad (22)$$

## APPENDIX B – BBM92 Derivation:

The Initial full state is:

$$|\Psi_0\rangle = |0\rangle_A |0\rangle_B |00000000\rangle_R \quad (23)$$

Applying H gate to Alice's qubit:

$$|\Psi_1\rangle = (H_A \otimes I_B \otimes I_R) |\Psi_0\rangle \quad (24)$$

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |1\rangle_A |0\rangle_B) \otimes |00000000\rangle_R \quad (25)$$

Applying CNOT gate from Alice to Bob

$$|\Psi_2\rangle = (\text{CNOT}_{A \rightarrow B} \otimes I_R) |\Psi_1\rangle \quad (26)$$

$$|0\rangle_A |0\rangle_B \mapsto |0\rangle_A |0\rangle_B \quad (27)$$

$$|1\rangle_A |0\rangle_B \mapsto |1\rangle_A |1\rangle_B \quad (28)$$

Therefore (following Bell's state):

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}} (|00\rangle_{AB} + |11\rangle_{AB}) \otimes |00000000\rangle_R \quad (29)$$

Applying H gates to Bob's 8 ancillas:

$$H^{\otimes 8} |00000000\rangle = \frac{1}{\sqrt{2^8}} \sum_{y=0}^{255} |y\rangle = \frac{1}{16} \sum_{y=0}^{255} |y\rangle \quad (30)$$

If Bob's data qubit is  $|0\rangle_B$ , then no CP gate contributes any phase. So, the ancilla register remains:

$$\frac{1}{16} \sum_{y=0}^{255} |y\rangle_R \quad (31)$$

$$|\Psi_{A=0}^{(3)}\rangle = |0\rangle_A |0\rangle_B \otimes \frac{1}{16} \sum_{y=0}^{255} |y\rangle_R \quad (32)$$

Now every ancilla bit equal to 1 contributes a phase  $e^{i\pi/4}$ . For an ancilla basis string:

$$|r_0 r_1 r_2 r_3 r_4 r_5 r_6 r_7\rangle_R \quad (33)$$

The total phase is:

$$e^{i\frac{\pi}{4}(r_0+r_1+r_2+r_3+r_4+r_5+r_6+r_7)} \quad (34)$$

Then the ancilla state becomes:

$$|\Psi_{A=1}^{(3)}\rangle = |1\rangle_A |1\rangle_B \otimes \frac{1}{16} \sum_{r \in \{0,1\}^8} e^{i\frac{\pi}{4}w(r)} |r\rangle_R \quad (35)$$

Before IQFT, the ancilla state is the uniform superposition:

$$\frac{1}{16} \sum_{y=0}^{255} |y\rangle \quad (36)$$

This is exactly the QFT of  $|0\rangle$ , so IQFT maps it back to  $|0\rangle$ :

$$QFT^{-1} \left( \frac{1}{16} \sum_{y=0}^{255} |y\rangle \right) = |00000000\rangle \quad (37)$$

Therefore:

$$|\Psi_{A=0}^{(4)}\rangle = |0\rangle_A |0\rangle_B |00000000\rangle_R \quad (38)$$

Now the ancilla state after IQFT is:

$$|\Psi_{A=1}^{(4)}\rangle = |1\rangle_A |1\rangle_B \otimes \sum_{z=0}^{255} \alpha_z |z\rangle_R \quad (39)$$

With amplitudes:

$$\alpha_z = \frac{1}{256} \sum_{y=0}^{255} e^{i\frac{\pi}{4}w(y)} e^{-2\pi i y z / 256} \quad (40)$$