MDPI

*Article*

# Adaptive Real-Time Modulation for Enhanced Resilience to Adversarial Noise in Continuous-Variable Quantum Communication

**Jose R. Rosas-Bustos [1,2,3,*], Jesse Van Griensven Thé [1,2,3], Roydon Andrew Fraser [1,3], Mark Pecen [3], Nadeem Said [1], Sebastian Ratto Valderrama [4], Alexander Truskovsky [5] and Andy Thanos [6]**

[1] Department of MME, University of Waterloo, Waterloo, ON N2L 3G1, Canada
[2] LAKES Environmental Research Inc., Waterloo, ON N2L 3L3, Canada
[3] Applied Quantum Technologies (AQT) Initiative, Columbia, MD 21046, USA
[4] Department of ECE, University of Waterloo, Waterloo, ON N2L 3G1, Canada
[5] EigenQ, Inc., Columbia, MD 21046, USA
[6] Cisco Systems, Inc., San Jose, CA 95134, USA
* Correspondence: jrosasbu@uwaterloo.ca

**Abstract**

Adversarial noise poses a considerable challenge to continuous-variable quantum communication (CVQC) systems, as it enables attackers to either extract sensitive information or disrupt quantum states. This paper presents a dynamic and adaptive modulation framework that utilizes real-time feedback to address three types of adversarial noise: reconnaissance, exploratory, and denial-of-service (DoS) attacks. By dynamically adjusting quantum parameters, such as phase ($\theta$) and squeezing ($r$), based on live feedback, this approach offers a robust solution for preserving quantum state stability against evolving threats. Through simulations and experimental validation using Xanadu's X8_01 photonic quantum processor, we illustrate that static modulation methods are inadequate in countering dynamic adversarial noise. Our findings highlight the superiority of adaptive modulation, which significantly improves resilience against energy deviations caused by adversarial noise, paving the way for more secure CVQC systems.

**Keywords:** Adversarial Noise, Adaptive Modulation, Real-Time Feedback, Continuous-Variable Quantum Communication, Quantum State Stability, Quantum Error Mitigation, Quantum Network Security, Phase and Squeezing Control, Quantum Communication Resilience, Photonic Quantum Processor

## 1. Introduction

Adversarial noise presents a sophisticated and intentional form of interference in quantum communication systems, exploiting system vulnerabilities to either extract sensitive information or disrupt the communication process. While environmental noise typically results from unpredictable fluctuations in the surrounding environment, adversarial noise represents a targeted threat, aimed at degrading system performance or breaching security [1]. This paper redefines adversarial noise as a novel category of quantum communication threat, including specific attacks such as reconnaissance, exploratory, and denial-of-service (DoS) attacks. Unlike environmental noise, adversarial noise evolves dynamically, is difficult to detect, and requires advanced countermeasures due to its intentional nature and unique behavioural patterns.

Received:
Revised:
Accepted:
Published:

**Copyright:** © 2026 by the authors. Submitted to *J. Cybersecur. Priv.* for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license.

Continuous-Variable Quantum Communication (CVQC) plays an essential role in the landscape of Quantum Information Processing (QIP), enabling secure communication through the encoding of quantum information in the quadratures of light, such as phase and amplitude. This makes CVQC highly compatible with current optical infrastructure and foundational protocols like Quantum Key Distribution (QKD) [2–4]. Despite advancements in QIP, CVQC systems remain vulnerable to both environmental and, critically, adversarial noise, which can compromise quantum state integrity and the security of transmitted information [5–7]. Addressing adversarial threats in CVQC is crucial for the reliability of QKD and future quantum networks [8].

Traditional static modulation techniques, designed to counteract environmental noise, are not equipped to handle the evolving and adaptive nature of adversarial noise. Such techniques assume a static or predictable noise profile, which fails in the face of attacks that adapt to system defences [9]. For instance, reconnaissance attacks may covertly gather information on a quantum system's parameters, while exploratory and DoS attacks can gradually degrade or completely halt communication. Existing studies, including those on optical jamming [10,11], have primarily examined isolated attack types and thus do not address the broader, complex nature of adversarial noise. This gap highlights the need for an adaptive countermeasure framework specifically tailored for dynamic, adversarial threats.

To address this challenge, we propose a real-time adaptive modulation framework that dynamically adjusts key quantum parameters, such as phase ($\theta$) and squeezing ($r$), in response to detected adversarial conditions. Traditional static squeezing techniques, which reduce uncertainty in one quadrature while increasing it in the conjugate quadrature, are insufficient for the unpredictable and evolving threats posed by adversarial noise. By contrast, dynamic modulation leverages real-time feedback to continuously adjust these parameters, helping to maintain quantum coherence and stability [12].

In this paper, we model three distinct types of adversarial noise and propose targeted, adaptive countermeasures utilizing real-time feedback. Our framework demonstrates the potential for dynamically modulating both phase and squeezing parameters to mitigate energy deviations caused by adversarial attacks. Through a combination of theoretical modelling, simulations, and experimental validation on Xanadu's X8_01 photonic quantum processor [13], we demonstrate that static modulation techniques are inadequate for countering adversarial noise. Our findings suggest that incorporating phase modulation with real-time squeezing adjustments significantly enhances system resilience against adversarial interference, offering a viable solution for secure and robust CVQC systems.

## 2. Adversarial Noise Modelling

In continuous-variable quantum systems, quantum information can be encoded in the quadratures $\hat{x}$ (position) and $\hat{p}$ (momentum) of qumodes. These quadratures are fundamental to representing quantum states in continuous-variable quantum communication, particularly in protocols like Quantum Key Distribution (QKD) [14]. Adversarial noise in this context refers to intentional perturbations introduced into these quadratures, aimed at disrupting or extracting information from the quantum states. We represent adversarial noise as transformations in the quadratures:

$$\hat{x}' = \hat{x} + f_x(\hat{x}, \hat{p}), \quad \hat{p}' = \hat{p} + f_p(\hat{x}, \hat{p}),$$

where $f_x(\hat{x}, \hat{p})$ and $f_p(\hat{x}, \hat{p})$ are functions describing the specific form and intensity of noise based on the type of adversarial attack. Below, we provide detailed models for each form of adversarial noise.

https://doi.org/10.3390/jcp1010000

### 2.1. Reconnaissance Noise

Reconnaissance noise consists of small, carefully controlled perturbations, introduced with the aim of subtly probing and gathering information about a quantum system's parameters without causing detectable disturbances. This form of noise is especially concerning in quantum cryptographic protocols like Quantum Key Distribution (QKD), where any leakage of information can compromise security. Reconnaissance noise leverages imperceptible fluctuations, effectively bypassing typical detection methods, and may take advantage of the inherent vulnerabilities linked to Hidden Variable Theories (HVTs) and the Heisenberg Uncertainty Principle (HUP) [15].

We model reconnaissance noise as small, additive Gaussian perturbations to the quadratures of the continuous-variable quantum state:

$$\hat{x}' = \hat{x} + \epsilon_x, \quad \hat{p}' = \hat{p} + \epsilon_p,$$

Where $\epsilon_x, \epsilon_p \sim \mathcal{N}(0, \sigma^2_{\text{recon}})$ are random variables drawn from a Gaussian distribution with small variance $\sigma^2_{\text{recon}}$. These minimal fluctuations allow adversaries to extract data on the system's internal parameters while maintaining energy deviations low enough to evade standard detection mechanisms.

Rosas et al. (2024) highlight how the interaction between Bell Inequalities (BIs) and HVTs, when observed through the lens of HUP, introduces regions, or *vicinities of uncertainty*, where quantum and classical predictions align. In these regions, the variance introduced by reconnaissance noise remains within the permissible bounds defined by HUP, making it exceedingly challenging to detect. These vicinities create a potential loophole, allowing adversaries to exploit overlap points between Quantum Mechanics (QM) and HVTs predictions, subtly gaining information over time without alerting detection protocols [15].

Moreover, reconnaissance noise in this context poses a unique challenge for QKD protocols, especially in configurations where measurement settings are aligned. When measurement vectors are configured in ways that approach these overlaps, as identified by Rosas et al., the reconnaissance noise can become even more effective. By carefully tuning the noise within these aligned configurations, attackers may uncover patterns in the measurements that reflect the internal states of the system. This alignment, when within HUP vicinities, enables a form of "quantum reconnaissance" where information is gathered without triggering security alerts.

#### 2.1.1. Practical Implications for Quantum Key Distribution (QKD) Protocols

Quantum key distribution protocols face challenges in realistic noisy environments, particularly under adversarial noise conditions that can compromise system resilience. Past studies have examined these practical challenges, underscoring the importance of noise-resilient designs in QKD [16].

The vulnerabilities identified by Rosas et al. underscore the risks of reconnaissance noise in QKD, particularly in real-world implementations. Due to inherent imperfections such as noise and decoherence in quantum hardware, practical QKD systems often struggle to maintain ideal conditions (e.g., keeping Clauser-Horne-Shimony-Holt (CHSH) inequality parameter $S > 2$ to confirm quantum entanglement). Reconnaissance noise exploits these imperfections, potentially generating misleading $S$-values that challenge the robustness of entanglement validation. This creates an environment where undetected, low-intensity reconnaissance attacks can extract information over time, undermining the foundational security of QKD protocols.

#### 2.1.2. Addressing the Threat of Reconnaissance Noise

Given these insights, it becomes evident that reconnaissance noise poses a persistent threat that could slowly erode the security of QKD systems. Traditional static countermeasures are inadequate to detect or respond to these gradual, near-threshold perturbations. Instead, advanced detection methods, such as real-time adaptive feedback and dynamic modulation, are required to identify and counteract these subtle fluctuations. Real-time feedback mechanisms have been a focus of study in quantum measurement and control, as they enable dynamic responses to noise in quantum systems. Such mechanisms have been explored in-depth for their capacity to stabilize quantum states against fluctuations [17]. Integrating these methods into QKD protocols can help mitigate the vulnerabilities exposed by reconnaissance noise and the convergence points between QM and HVTs predictions, ensuring that critical security measures remain intact despite the sophisticated nature of adversarial threats.

### *2.2. Exploratory Noise*

Exploratory noise is designed to apply moderate perturbations to the quantum system, allowing an adversary to probe its resilience and potentially expose vulnerabilities. Unlike reconnaissance noise, which relies on subtle changes to remain undetected, exploratory noise introduces noticeable disruptions that test the system's ability to maintain stability under varying conditions. This noise type typically combines both displacement and squeezing operations to alter the system's quadratures, observing how these adjustments influence the system's response. By analyzing the system's resilience to exploratory noise, an adversary can uncover patterns in its response, which may later be exploited in more severe attacks if weaknesses are identified.

We model exploratory noise as a combination of squeezing and displacement operations applied to the position and momentum quadratures $\hat{x}$ and $\hat{p}$:

$$\hat{x}' = \hat{x} \cdot e^{-r_{\text{exp}}} + \delta_x, \quad \hat{p}' = \hat{p} \cdot e^{r_{\text{exp}}} + \delta_p,$$

Where:

- $r_{\text{exp}}$ represents the level of adversarial squeezing. Squeezing modifies the uncertainty distribution in the quadratures, reducing uncertainty in one quadrature (e.g., position) while increasing it in the conjugate quadrature (e.g., momentum). This operation leverages the Heisenberg Uncertainty Principle to manipulate the system's state, forcing it to compensate for the adversarial squeezing.
- $\delta_x$ and $\delta_p$ are random displacement terms with moderate variance, chosen to be large enough to influence the quantum state but not so large as to completely disrupt it. These terms introduce shifts in the position and momentum quadratures, further destabilizing the state.

Exploratory noise leverages the fact that quantum states in continuous-variable systems, such as squeezed states, are sensitive to perturbations in their quadrature distributions. The squeezing operation $e^{-r_{\text{exp}}}$ affects the uncertainty in the $\hat{x}$-quadrature, while $e^{r_{\text{exp}}}$ affects the uncertainty in the $\hat{p}$-quadrature. By applying these operations asymmetrically, exploratory noise induces an imbalance in the quadrature variances:

$$\sigma_x' = \sigma_x \cdot e^{-2r_{\text{exp}}}, \quad \sigma_p' = \sigma_p \cdot e^{2r_{\text{exp}}},$$

where $\sigma_x$ and $\sigma_p$ represent the original standard deviations of the quadratures in the absence of noise. The factor $e^{\pm 2r_{\text{exp}}}$ thus amplifies the difference in uncertainties between the quadratures, stressing the system's capacity for noise resilience.

#### 2.2.1. Impact of Exploratory Noise on System Stability

The application of exploratory noise has several implications for the stability of the quantum system:

1. **Imbalance in Quadrature Uncertainties.** By introducing squeezing asymmetrically, exploratory noise creates a disparity between the uncertainties in $\hat{x}$ and $\hat{p}$. This imbalance forces the system to adjust its internal state in an attempt to re-establish stability, which can expose potential vulnerabilities in the system's error-correction or modulation mechanisms.
2. **Stress on Adaptive Modulation Mechanisms.** Systems that rely on dynamic or real-time modulation may struggle to respond effectively to the rapid fluctuations induced by exploratory noise. For instance, if the system uses adaptive feedback to maintain a balanced quadrature distribution, exploratory noise can introduce feedback delays or misalignments, revealing weaknesses in the control architecture.
3. **Response Patterns and Vulnerability Mapping.** The adversary can analyze the system's response patterns to the exploratory noise perturbations, mapping regions of vulnerability where the system's resilience is lowest. Such mapping enables an adversary to identify specific configurations or states that the system is less equipped to handle, laying the groundwork for more targeted attacks in the future.

#### 2.2.2. Exploiting Squeezed States in Exploratory Noise

Squeezed states, commonly used in quantum communication systems to optimize information encoding and reduce noise in specific quadratures, are particularly susceptible to exploratory noise. When adversarial squeezing aligns with the system's squeezing configuration, exploratory noise can enhance the system's sensitivity to specific types of perturbations, thereby amplifying the adversary's ability to extract information or destabilize the system.

For example, if the system is configured to squeeze the $\hat{x}$-quadrature to minimize noise in that dimension, exploratory noise that applies additional squeezing to $\hat{x}$ may further reduce its uncertainty. However, this comes at the cost of increased uncertainty in the conjugate $\hat{p}$-quadrature, which may induce an imbalance in the system's overall stability. The adversary can observe the system's adaptive responses to this targeted imbalance, leveraging it to gain insights into the system's modulation parameters, noise thresholds, and feedback limits.

#### 2.2.3. Representation of Exploratory Noise Impact

The impact of exploratory noise on the system's state can be quantified by examining the induced energy deviation $\Delta E_{\text{exp}}$, which measures the deviation of the perturbed state's energy relative to the unperturbed system:

$$\Delta E_{\text{exp}} = \langle \hat{H}_{\text{pert}} \rangle - \langle \hat{H} \rangle,$$

where $\langle \hat{H}_{\text{pert}} \rangle$ represents the expected energy of the system under exploratory noise, and $\langle \hat{H} \rangle$ represents the energy without noise. By monitoring changes in $\Delta E_{\text{exp}}$, the adversary can assess the energy sensitivity of the system to exploratory noise, identifying thresholds where the system's compensatory mechanisms are weakest.

Exploratory noise serves as a probing tool, allowing adversaries to detect weaknesses in the quantum system's noise resilience. Through moderate squeezing and displacement, exploratory noise uncovers response patterns and areas of vulnerability, which can inform the design of subsequent, more aggressive attacks. Countering exploratory noise requires advanced adaptive modulation techniques that dynamically adjust to asymmetric pertur-

bations across quadratures, maintaining system stability even under deliberate, moderate noise intrusions.

### *2.3. Denial-of-Service (DoS) Noise*

Denial-of-Service (DoS) noise represents a severe, high-intensity attack designed to overwhelm a quantum communication system by introducing extreme levels of noise. Unlike reconnaissance or exploratory noise, which operate subtly to extract information or probe system weaknesses, DoS noise aims to disrupt communication entirely, making reliable information transfer impossible. The objective of a DoS attack is to saturate the communication channel with excessive perturbations, effectively drowning out the legitimate quantum signals. This form of attack is particularly damaging to continuous-variable quantum communication (CVQC) systems, as it targets the stability and coherence of the quantum states used for encoding information.

We model the effect of DoS noise on the position ($\hat{x}$) and momentum ($\hat{p}$) quadratures as follows:

$$\hat{x}' = \hat{x} + \eta_x \cdot \hat{x}, \quad \hat{p}' = \hat{p} + \eta_p \cdot \hat{p},$$

Where:

- $\eta_x, \eta_p \gg 1$ are large scaling factors, typically chosen to be significantly greater than unity, which amplify the original quadrature values. These factors introduce substantial, multiplicative noise to both quadratures, leading to severe distortions in the quantum state.
- The terms $\eta_x \cdot \hat{x}$ and $\eta_p \cdot \hat{p}$ represent noise components that are proportional to the initial values of $\hat{x}$ and $\hat{p}$, leading to exponential scaling in the quadrature distributions.

The large scaling factors $\eta_x$ and $\eta_p$ cause significant perturbations that overwhelm the quantum state's coherence, disrupting the carefully controlled superposition and entanglement properties essential for quantum communication. As a result, DoS noise leads to high energy deviations and, in severe cases, complete breakdown of the quantum channel.

#### 2.3.1. Impact of DoS Noise on Quantum State Coherence

DoS noise introduces large fluctuations that not only increase the uncertainty in the quadrature measurements but also degrade the coherence of the quantum state. The coherence loss can be quantified by examining the increase in variances:

$$\sigma_x' = \sigma_x(1 + \eta_x), \quad \sigma_p' = \sigma_p(1 + \eta_p),$$

Where $\sigma_x$ and $\sigma_p$ are the standard deviations of the position and momentum quadratures in the absence of noise. Since $\eta_x, \eta_p \gg 1$, the variances $\sigma_x'^2$ and $\sigma_p'^2$ become much larger than their original values, leading to significant energy deviations in the system. This degradation in the quadrature distributions disrupts the state's stability and coherence, making it increasingly challenging for the receiver to decode information accurately.

Additionally, the extreme nature of DoS noise typically causes the Wigner function, a phase-space representation of the quantum state, to spread out, losing its Gaussian form and becoming highly distorted. This transformation in the Wigner function indicates a breakdown of the state's purity, rendering the quantum state unsuitable for reliable communication.

#### 2.3.2. Energy Deviation Induced by DoS Noise

The impact of DoS noise can be further analyzed by calculating the energy deviation $\Delta E_{\text{DoS}}$ induced in the system. The energy deviation quantifies the difference between

the perturbed state's energy and the minimum energy $E_{\min}$ achievable in a noiseless environment:

$$\Delta E_{\text{DoS}} = \langle \hat{H}_{\text{pert}} \rangle - E_{\min},$$

Where $\hat{H}_{\text{pert}}$ is the Hamiltonian of the system in the presence of DoS noise. Given the significant scaling factors $\eta_x$ and $\eta_p$, $\Delta E_{\text{DoS}}$ becomes large, indicating that the perturbed state has high energy fluctuations. In practical terms, this increase in energy deviation leads to excessive heating of the quantum state, making it virtually impossible to maintain coherence and stability under DoS noise conditions.

#### 2.3.3. Detection and Challenges of DoS Noise

Due to its high intensity, DoS noise is often easier to detect than reconnaissance or exploratory noise. Large fluctuations in quadrature values or significant deviations in expected energy can serve as immediate indicators of a DoS attack. However, the primary challenge with DoS noise lies in its ability to disrupt communication rapidly, often before detection and countermeasures can be deployed effectively. This attack renders quantum error correction and standard noise mitigation techniques insufficient, as the level of noise far exceeds the system's typical operating thresholds.

DoS noise creates a high-risk scenario where:

1. **Immediate Communication Disruption.** The excessive noise introduced by DoS attacks can immediately disrupt quantum key distribution (QKD) protocols, preventing the establishment of secure keys and halting data transfer.
2. **Loss of Quantum Entanglement.** The intense noise causes the quantum states to lose their entangled properties, a critical component for secure communication in QKD and other quantum protocols.
3. **Irreversible State Degradation.** The energy deviation caused by DoS noise often leads to irreversible degradation of the quantum state, requiring a complete reset of the communication channel.

#### 2.3.4. Model of Resilience to DoS Noise

To analyze the resilience of a quantum system to DoS noise, we consider a threshold energy deviation $\Delta E_{\text{th}}$ beyond which communication becomes unreliable:

$$\Delta E_{\text{DoS}} \gg \Delta E_{\text{th}},$$

Where $\Delta E_{\text{th}}$ represents the maximum energy deviation that the system can tolerate while maintaining coherent communication. For most quantum communication systems, $\Delta E_{\text{th}}$ is calibrated based on typical noise levels and system parameters, but DoS noise far exceeds this threshold, leading to immediate failure of the communication protocol.

Quantifying the resilience to DoS noise involves evaluating the noise tolerance ratio $R_{\text{DoS}}$:

$$R_{\text{DoS}} = \frac{\Delta E_{\text{DoS}}}{\Delta E_{\text{th}}}.$$

A high $R_{\text{DoS}} \gg 1$ indicates that the system's threshold is vastly exceeded, confirming the inadequacy of traditional countermeasures against DoS noise.

#### 2.3.5. Countermeasures for DoS Noise

Mitigating DoS noise requires advanced countermeasures beyond standard error correction techniques. Some potential strategies include:

- **Dynamic Power Scaling.** Reducing the system's sensitivity to incoming signals during suspected DoS attacks by dynamically scaling down the response to high-intensity signals.
- **Adaptive Modulation.** Adjusting the phase and squeezing parameters dynamically to minimize the impact of noise, although this remains challenging under DoS conditions due to the noise's intensity.
- **Early Detection Mechanisms.** Implementing early warning systems based on rapid energy deviation measurements, allowing the system to temporarily halt operations in response to significant fluctuations until stability is restored.

While these countermeasures may offer some resilience, the effectiveness of any mitigation strategy is limited when faced with the extreme intensity of DoS noise. Thus, the primary defense remains early detection and the ability to suspend communication rapidly to prevent total system failure.

In summary, DoS noise presents one of the most severe challenges to continuous-variable quantum communication systems due to its high-intensity nature and potential to cause immediate communication breakdown. Effective countermeasures require rapid detection and responsive modulation techniques, highlighting the need for future research focused on developing robust quantum systems capable of withstanding such extreme noise conditions.

### *2.4. Impact of Adversarial Noise on Quantum States*

Adversarial noise affects quantum states in distinct ways, depending on the type and intensity of the noise introduced. Each noise type has unique characteristics that influence the system's energy, coherence, and overall stability, impacting the reliability and security of continuous-variable quantum communication (CVQC) systems.

#### 2.4.1. Energy Deviation and Coherence Loss

To quantify the impact of adversarial noise on a quantum state, we define the energy deviation $\Delta E$, which measures the difference between the expected energy of the perturbed quantum state and the minimum achievable energy $E_{\min}$ in the absence of noise:

$$\Delta E = \langle \hat{H} \rangle - E_{\min},$$

where $\hat{H}$ is the Hamiltonian of the system, and $E_{\min}$ represents the ground-state energy level in the noiseless state. The energy deviation $\Delta E$ serves as a metric for the degree of perturbation introduced by each noise type. Different adversarial noise types yield varying values for $\Delta E$, reflecting their intensity and impact on the system.

- **Reconnaissance Noise.** Due to its low-intensity nature, reconnaissance noise produces a minimal $\Delta E$ value, close to zero, as it primarily introduces small, undetectable fluctuations. This minimal energy deviation allows reconnaissance noise to bypass standard detection mechanisms, posing a subtle but continuous threat to data security.
- **Exploratory Noise.** Moderate disruptions from exploratory noise result in noticeable increases in $\Delta E$. The controlled application of displacement and squeezing operations distorts the quadrature distributions, leading to observable energy deviations. The extent of $\Delta E$ under exploratory noise conditions depends on the level of squeezing and displacement applied. A higher $\Delta E$ indicates greater susceptibility to this type of noise, suggesting that the system's noise resilience could be further tested and potentially exploited.
- **Denial-of-Service (DoS) Noise.** As the most intense form of adversarial noise, DoS noise produces the highest $\Delta E$ values. The substantial scaling factors $\eta_x$ and $\eta_p$ in

DoS noise result in drastic increases in energy deviation, often exceeding the system's operating tolerance. The large $\Delta E$ not only signifies a high level of perturbation but also correlates with rapid coherence loss and state degradation, making recovery difficult or impossible without resetting the system.

#### 2.4.2. Coherence Loss and State Purity under Adversarial Noise

Beyond energy deviation, coherence loss and purity degradation are critical indicators of the impact of adversarial noise on quantum states. Each type of noise affects coherence differently, impacting the system's ability to maintain reliable communication.

- **Coherence under Reconnaissance Noise.** Reconnaissance noise may operate within the Heisenberg Uncertainty Principle's permissible bounds, introducing fluctuations that minimally disturb coherence. While the state's purity remains high, repeated, undetected reconnaissance noise can cumulatively reveal information about system parameters, gradually compromising security.
- **Coherence under Exploratory Noise.** Exploratory noise applies moderate squeezing and displacement, leading to uneven distributions in the quadrature uncertainties. This imbalance challenges the coherence of the quantum state, causing the Wigner function to slightly deviate from its ideal Gaussian form. The resulting purity degradation, although moderate, indicates the system's reduced ability to maintain stable communication under exploratory noise.
- **Coherence under DoS Noise.** DoS noise introduces extreme perturbations that rapidly degrade coherence, spreading the Wigner function significantly in phase space. This extreme distortion leads to a loss of state purity, transforming the quantum state into a highly mixed state that is incompatible with reliable communication. The rapid coherence loss under DoS noise conditions effectively disrupts entanglement and other quantum correlations essential for secure communication protocols like Quantum Key Distribution (QKD).

### *2.5. General Modulation Framework*

The adaptive modulation framework we propose relies on a feedback loop that continuously monitors the quantum state and adjusts the parameters $\theta$ (phase-space rotation angle) and $r$ (squeezing parameter) in real-time. This system aims to minimize the energy deviation $\Delta E$ caused by adversarial noise by dynamically controlling both the phase-space rotation and squeezing of the qumodes. The general form of this modulation, which describes the transformed position and momentum quadratures, is represented as:

$$\hat{x}_{\theta,r} = \hat{x} \cdot e^{-r} \cos(\theta) - \hat{p} \cdot e^{r} \sin(\theta), \quad \hat{p}_{\theta,r} = \hat{x} \cdot e^{-r} \sin(\theta) + \hat{p} \cdot e^{r} \cos(\theta),$$

Where each term in the equations has a specific role in adapting the system's state:

- $\hat{x}$ and $\hat{p}$: These represent the original position and momentum quadratures of the quantum state. Quadratures are fundamental properties in continuous-variable quantum systems, corresponding to measurable components of the quantum state (analogous to position and momentum in classical mechanics). In this framework, these quadratures are modified to mitigate the impact of noise.
- $e^{-r}$ and $e^{r}$: These exponential terms incorporate the squeezing parameter $r$, which adjusts the uncertainty in the quadratures. Squeezing reduces uncertainty in one quadrature (e.g., $\hat{x}$) while increasing it in the conjugate quadrature (e.g., $\hat{p}$), thereby redistributing noise. $e^{-r}$ applies squeezing to $\hat{x}$, reducing its uncertainty, while $e^{r}$ applies anti-squeezing to $\hat{p}$, increasing its uncertainty. This controlled squeezing modulation helps counteract noise-induced imbalances in the quadrature distributions.

- $\cos(\theta)$ and $\sin(\theta)$: These trigonometric terms incorporate the rotation angle $\theta$, which determines the phase-space rotation applied to the quadratures. By adjusting $\theta$, the system can align with or oppose the direction of incoming noise. The $\cos(\theta)$ and $\sin(\theta)$ terms enable the transformation of the quadratures by rotating the phase space, allowing the state to "reorient" in response to noise. This phase-space rotation effectively reduces the system's sensitivity to perturbations in specific directions.
- $\theta$: The phase-space rotation angle $\theta$ is dynamically adjusted based on real-time feedback, allowing the system to counteract phase-related noise components. By tuning $\theta$, the system can optimize its orientation in phase space, mitigating the impact of noise that shifts the phase of the quadrature distributions.
- $r$: The squeezing parameter $r$ modulates the level of squeezing applied to the state. Dynamic adjustment of $r$ allows the system to redistribute uncertainty between the quadratures in real-time, making the state more resilient to noise that disproportionately affects one quadrature over the other.

In this modulation framework, the combined adjustments of $\theta$ and $r$ allow the system to adapt flexibly to different noise types and intensities, enhancing resilience against adversarial interference. The modulation terms $e^{-r}$, $e^{r}$, $\cos(\theta)$, and $\sin(\theta)$ work in conjunction to transform the position and momentum quadratures, maintaining the stability and coherence of the quantum state even in the presence of fluctuating noise. Through real-time updates of these parameters, the feedback loop can continuously counteract adversarial noise, preserving the integrity and security of continuous-variable quantum communication.

### *2.6. Countering Reconnaissance Noise*

Reconnaissance noise introduces subtle, low-intensity perturbations that are challenging to detect yet capable of leaking sensitive information. This form of noise typically operates at levels close to the system's detection threshold, allowing an adversary to gradually gather information about the quantum system's parameters without triggering conventional security mechanisms. To mitigate the risks associated with reconnaissance noise, a finely tuned phase modulation approach is essential, aiming to reduce the sensitivity of the quantum state to these minor disturbances.

The key to countering reconnaissance noise lies in the system's ability to continuously monitor the energy deviation $\Delta E$, which serves as an indicator of the extent to which the quantum state has been perturbed. By dynamically adjusting the phase-space rotation angle $\theta$, the system can align the quantum state with the incoming noise direction, minimizing the impact of the perturbations and thereby reducing the potential for information leakage. The optimal modulation strategy for reconnaissance noise is represented as:

$$\theta_{\text{optimal}} = \arg\min_{\theta}(\Delta E(\theta)),$$

where each term in this expression has a specific role:

- $\theta$: Represents the phase-space rotation angle of the quantum state. Adjusting $\theta$ changes the orientation of the state in phase space, aligning it in such a way as to minimize sensitivity to the perturbations introduced by reconnaissance noise.
- $\Delta E(\theta)$: The energy deviation as a function of $\theta$. This quantity measures how much the energy of the quantum state deviates from its baseline (unperturbed) energy when the state is rotated by an angle $\theta$ in response to noise. A smaller $\Delta E(\theta)$ indicates that the state has been less affected by reconnaissance noise at that particular angle.

- $\arg\min_\theta$: Denotes the angle $\theta$ that minimizes $\Delta E(\theta)$. The goal is to find this optimal angle, $\theta_{\text{optimal}}$, at which the energy deviation reaches its lowest possible value, thus ensuring minimal disturbance to the quantum state.

This expression indicates that the system actively searches for the angle $\theta_{\text{optimal}}$ that minimizes energy deviation. By achieving this minimum, the system ensures that the quantum state remains as undisturbed as possible in the presence of reconnaissance noise, thereby limiting the noise's potential to extract information.

In this modulation strategy, the squeezing parameter $r$ is held constant because reconnaissance noise typically introduces only minor fluctuations that do not necessitate adjustments in squeezing. By focusing modulation efforts exclusively on the phase angle $\theta$, the system can precisely align the quantum state with the direction of the noise perturbations, effectively dampening their impact. This targeted approach allows the system to defend against reconnaissance noise efficiently, minimizing information leakage while preserving the integrity of the quantum state.

#### 2.6.1. Dynamic Phase Alignment for Enhanced Security

To further enhance resilience against reconnaissance noise, the phase alignment is continuously updated based on real-time feedback. This dynamic process involves:

1. **Real-time measurement of energy deviation.** The system continuously measures $\Delta E$ to detect any changes in the quantum state that may indicate the presence of reconnaissance noise.
2. **Adaptive phase adjustment.** Upon detecting a deviation, the system adjusts $\theta$ incrementally towards $\theta_{\text{optimal}}$ in a manner that counteracts the specific characteristics of the detected perturbation.
3. **Feedback-based recalibration.** As reconnaissance noise may vary slightly over time, the feedback loop recalibrates $\theta$ continuously to maintain minimal $\Delta E$ despite small fluctuations in the noise profile.

This dynamic alignment not only mitigates the impact of reconnaissance noise but also reduces the system's susceptibility to gradual information leakage. Since reconnaissance noise often leverages cumulative, low-intensity fluctuations, the adaptive modulation of $\theta$ serves as a preventive measure, limiting the adversary's ability to extract valuable data from the quantum state.

#### 2.6.2. Preserving Coherence while Countering Reconnaissance Noise

One of the primary challenges in countering reconnaissance noise is to suppress information leakage without significantly disturbing the quantum state's coherence. By modulating only the phase angle $\theta$, the system maintains the original state's coherence and purity, ensuring that quantum information remains intact. This approach is particularly advantageous in quantum communication protocols, where maintaining high coherence is essential for reliable data transmission.

Thus, by dynamically aligning $\theta$ with the perturbations introduced by reconnaissance noise, the system effectively dampens these low-level disturbances, achieving a robust defence against this subtle form of adversarial interference. This technique enhances the overall security of the quantum communication system by preventing gradual, undetected data leakage while preserving the integrity of the quantum state.

### *2.7. Countering Exploratory Noise*

Exploratory noise introduces moderate perturbations to the quantum system, often combining displacement and squeezing operations to probe the system's resilience and identify potential vulnerabilities. This type of noise intentionally disrupts the system more

noticeably than reconnaissance noise, testing its stability and revealing weaknesses. To effectively counter exploratory noise, it is necessary to dynamically adjust both the phase-space rotation angle $\theta$ and the squeezing parameter $r$ in real time. These adjustments help the system maintain coherence and reduce sensitivity to exploratory attacks.

When exploratory noise is detected, the feedback system continuously monitors deviations in the quantum state, adjusting the squeezing parameter $r$ to counter the adversarial squeezing and modifying the rotation angle $\theta$ to compensate for any phase shifts resulting from displacement components of the noise. This dual modulation strategy is designed to minimize the energy deviation $\Delta E$, preserving the stability of the quantum state under the influence of exploratory noise. The modulation strategy for exploratory noise can be expressed as:

$$r_{\text{optimal}} = \log\left(\frac{1}{r_{\text{noise}}}\right), \quad \theta_{\text{optimal}} = \theta + \Delta\theta_{\text{noise}},$$

Where each term in this expression has a specific role:

- $r_{\text{optimal}}$: Represents the optimal squeezing adjustment to counteract the squeezing introduced by exploratory noise. By adjusting the system's squeezing parameter $r$ to match the inverse of the adversarial squeezing (as captured by $r_{\text{noise}}$), the system reduces the noise's impact on quadrature uncertainty.
- $r_{\text{noise}}$: The squeezing factor introduced by exploratory noise, which affects the quadrature uncertainties of the quantum state. By inverting this factor, the system mitigates the squeezing effect and maintains balanced quadrature distributions.
- $\theta_{\text{optimal}}$: The optimal phase-space rotation angle that compensates for phase shifts introduced by displacement components in exploratory noise. Adjusting $\theta$ in response to $\Delta\theta_{\text{noise}}$ ensures that the quantum state realigns in phase space, reducing sensitivity to displacement effects.
- $\Delta\theta_{\text{noise}}$: The phase shift caused by displacement components of the exploratory noise. This value indicates the degree to which the noise shifts the phase of the quantum state, necessitating compensatory adjustments in $\theta$.

By modulating $r$ to counteract adversarial squeezing and adjusting $\theta$ to align the quantum state in phase space, the system reduces the overall energy deviation $\Delta E$ and preserves coherence. This real-time modulation effectively stabilizes the system against exploratory noise, preventing adversaries from mapping out response patterns or identifying vulnerabilities that could be exploited in future attacks.

#### 2.7.1. Feedback Loop Complexity for Exploratory Noise

Countering exploratory noise requires a more sophisticated feedback loop than that needed for reconnaissance noise. This feedback system must continuously detect both phase deviations and the level of squeezing imposed by the noise. Specifically, the feedback loop operates as follows:

1. **Detection of Quantum State Deviation.** The system first measures deviations in the quantum state, identifying perturbations in quadrature distributions caused by exploratory noise.
2. **Quantification of Squeezing and Phase Shift.** The feedback system evaluates the squeezing factor $r_{\text{noise}}$ and phase shift $\Delta\theta_{\text{noise}}$ introduced by the noise. These values inform the required adjustments to $r$ and $\theta$.
3. **Real-Time Adjustment of $r$ and $\theta$.** Based on the detected noise parameters, the feedback system modulates $r$ to neutralize the imposed squeezing and adjusts $\theta$ to realign the quantum state in phase space. These adjustments are applied dynamically to minimize energy deviation.

4. **Continuous Monitoring and Adjustment.** The feedback loop continuously monitors the system, making real-time adjustments to $r$ and $\theta$ as exploratory noise fluctuates. This ensures that the system remains resilient, preventing the adversary from mapping any consistent vulnerabilities.

The dual adjustments of $r$ and $\theta$ ensure that the system remains resistant to exploratory noise, significantly reducing the risk of adversarial vulnerability mapping. This approach not only mitigates the immediate impact of exploratory noise but also strengthens the system's robustness against potential follow-up attacks.

### *2.8. Countering Denial-of-Service (DoS) Noise*

Denial-of-Service (DoS) noise represents one of the most severe forms of adversarial attacks, characterized by its high-intensity perturbations that saturate the quantum communication channel with extreme noise levels. The objective of a DoS attack is to destabilize the quantum state to such a degree that reliable communication becomes impossible. Due to its intensity, DoS noise introduces large, unpredictable fluctuations in the quadratures, significantly increasing energy deviation and impairing coherence. Countering this type of noise requires an aggressive modulation approach to stabilize the system by dynamically adjusting both the phase-space rotation angle $\theta$ and the squeezing parameter $r$ in real-time.

In response to DoS noise, the feedback system continuously monitors large deviations in the quadrature values $\hat{x}$ and $\hat{p}$, detecting shifts in the position and momentum distributions caused by the excessive noise. Based on this real-time monitoring, the system dynamically adjusts both the phase angle $\theta$ and the squeezing parameter $r$ to restore coherence and minimize energy deviations. The modulation strategy to counteract DoS noise is represented as:

$$r_{\text{optimal}} = \frac{1}{\eta_x}, \quad \theta_{\text{optimal}} = \frac{1}{\eta_p},$$

Where each term serves a specific role in the countermeasure framework:

- $r_{\text{optimal}}$: Represents the optimal squeezing parameter to counteract the intense squeezing effect introduced by the DoS noise in the $\hat{x}$-quadrature. Here, $\eta_x$ is a scaling factor related to the magnitude of the noise in the $\hat{x}$ direction. By setting $r$ inversely proportional to $\eta_x$, the system reduces its sensitivity to large displacements in the $\hat{x}$-quadrature, preventing the qumode from becoming overly stretched and maintaining more balanced quadrature distributions.
- $\theta_{\text{optimal}}$: Represents the optimal phase angle for counteracting phase shifts caused by DoS noise in the $\hat{p}$-quadrature. Similarly, $\eta_p$ is a scaling factor associated with the noise intensity in the $\hat{p}$-quadrature. Adjusting $\theta$ in inverse proportion to $\eta_p$ realigns the quantum state within phase space, minimizing the disruption to the quantum state's phase distribution.

These optimal settings help the system counterbalance the intense perturbations induced by DoS noise, stabilizing the quantum state by suppressing energy deviations and preserving coherence.

#### 2.8.1. Adaptive Thresholds for Modulation Parameters

Given the high-intensity nature of DoS noise, the modulation process requires setting adaptive thresholds for $r$ and $\theta$ to avoid overcompensation. Overcompensating in response to extreme fluctuations could further destabilize the quantum state, amplifying energy deviation instead of reducing it. By implementing thresholds for $r$ and $\theta$, the system maintains control over the modulation process, ensuring that adjustments remain within a range conducive to stability. These thresholds are dynamically tuned based on the noise

intensity detected in real-time, allowing the system to handle various levels of noise severity without risking overshoot or instability.

$$r_{\text{threshold}} = \max\left(r_{\text{optimal}}, r_{\max}\right), \quad \theta_{\text{threshold}} = \max\left(\theta_{\text{optimal}}, \theta_{\max}\right),$$

Where $r_{\max}$ and $\theta_{\max}$ are predefined upper bounds for modulation under extreme conditions. These values are calibrated to ensure that the modulation parameters remain effective against noise without reaching destabilizing extremes.

#### 2.8.2. High-Frequency Feedback Loop

To effectively counteract DoS noise, the feedback system must operate at a higher frequency than it would for lower-intensity noise types. DoS noise typically fluctuates rapidly, with large, transient peaks that can overwhelm the quantum state if not promptly mitigated. Therefore, the feedback loop for DoS countermeasures is designed to detect and respond to fluctuations in real-time, adjusting $\theta$ and $r$ swiftly to keep the energy deviation $\Delta E$ within acceptable limits. This high-frequency feedback loop follows a rapid sequence of operations:

1. **Detect Noise Level.** Continuously measure the quadrature values $\hat{x}$ and $\hat{p}$, calculating the instantaneous energy deviation $\Delta E$ to detect spikes indicative of DoS noise.
2. **Calculate Optimal Modulation.** Use the current values of $\eta_x$ and $\eta_p$ to determine $r_{\text{optimal}}$ and $\theta_{\text{optimal}}$ for immediate modulation.
3. **Apply Threshold-Adjusted Modulation.** Adjust $r$ and $\theta$ based on the calculated optimal values while respecting the thresholds $r_{\text{threshold}}$ and $\theta_{\text{threshold}}$ to avoid overcompensation.
4. **Continuous Monitoring and Adjustment.** Continuously repeat these steps to address fluctuating noise levels, ensuring stability by maintaining the modulation at high frequency.

#### 2.8.3. Ensuring System Resilience under DoS Conditions

Implementing this high-frequency feedback loop and adaptive modulation allows the system to respond promptly to DoS noise, preserving the stability and coherence of the quantum state. This approach not only minimizes the immediate impact of DoS attacks but also helps the system withstand prolonged exposure to high-intensity noise. By maintaining modulation parameters within optimal ranges and avoiding overcompensation, the system achieves a balanced response that supports secure and stable communication even under adversarial DoS conditions.

Countering DoS noise requires an aggressive, high-frequency modulation strategy with carefully managed thresholds for $r$ and $\theta$. This approach effectively restores stability and coherence to the quantum state, minimizing energy deviations and ensuring that the system can continue functioning under extreme noise conditions.

### *2.9. Real-Time Feedback Mechanism*

A critical component of the proposed countermeasures is the real-time feedback mechanism, which enables continuous monitoring and precise adjustment of $\theta$ (phase-space rotation angle) and $r$ (squeezing parameter) based on the prevailing noise profile. This feedback mechanism is essential in adapting to fluctuating and unpredictable noise, particularly in scenarios involving adversarial interference. By constantly evaluating the energy deviation $\Delta E$, the system can detect deviations introduced by noise and react promptly by updating modulation parameters. This approach helps maintain the stability and coherence of the quantum states, which are vital for secure communication.

The real-time feedback process consists of the following sequential steps:

1. **State Measurement.** Measure the current state of the qumodes by assessing quadrature values, $\hat{x}$ (position) and $\hat{p}$ (momentum), to detect noise-induced deviations. This step provides immediate insights into the state of the system, indicating any adverse effects caused by external noise.
2. **Energy Deviation Computation.** Calculate the energy deviation $\Delta E = \langle \hat{H} \rangle - E_{\min}$, where $\langle \hat{H} \rangle$ is the measured Hamiltonian (system's total energy in the presence of noise), and $E_{\min}$ represents the minimum achievable energy in a noiseless environment. $\Delta E$ serves as a metric to quantify how much the noise perturbs the quantum state, with larger values indicating more substantial interference.
3. **Modulation Adjustment.** Based on the computed $\Delta E$ and the detected noise profile, dynamically adjust $\theta$ and $r$ to minimize the energy deviation. This step uses tailored modulation strategies that differ depending on the type of adversarial noise (e.g., reconnaissance, exploratory, or DoS). For instance, reconnaissance noise may only require phase adjustments ($\theta$), while DoS noise typically requires adjustments in both $\theta$ and $r$ due to its high intensity.
4. **Continuous Adaptation.** The process continuously repeats, with the feedback loop monitoring, computing, adjusting, and re-evaluating in real-time. This continuous operation is necessary to maintain optimal performance, as noise conditions are expected to evolve over time.

This real-time feedback loop is crucial for responding to the dynamic and unpredictable nature of adversarial noise. By constantly measuring $\Delta E$ and updating $\theta$ and $r$, the system can mitigate the impacts of noise, preserving coherence and stability in quantum communication channels. To counteract high-intensity noise, particularly under DoS conditions, the feedback mechanism must be both rapid and precise, as even minor delays in adjustment could result in significant degradation of quantum state fidelity.

#### 2.9.1. Implementation Considerations for Real-Time Feedback

Practical implementation of a real-time feedback mechanism involves several critical considerations, including high-speed data processing, precise measurement accuracy, and the ability to predict noise trends for anticipatory adjustments. Implementing these requirements ensures that the feedback mechanism effectively counteracts noise while remaining efficient and adaptable.

- **High-Speed Processing.** The feedback mechanism requires a fast data-processing system capable of handling continuous measurement and modulation updates. This is particularly relevant in DoS noise scenarios, where the noise profile may fluctuate rapidly, demanding real-time adjustments. A high-speed processing capability enables the feedback system to respond immediately to incoming data, maintaining the stability of the quantum states.
- **Accurate State Measurement.** Quantum state measurement, particularly through techniques like homodyne detection, allows precise monitoring of the quadrature values $\hat{x}$ and $\hat{p}$. Homodyne detection provides real-time insights into the quantum state's position and momentum, which are crucial for identifying perturbations and guiding modulation adjustments. High measurement accuracy ensures that the feedback mechanism bases adjustments on reliable data, reducing the risk of overcompensation or under-adjustment.
- **Adaptive Algorithms for Noise Prediction.** Incorporating adaptive algorithms that predict noise trends can improve the feedback loop's responsiveness. Algorithms that leverage predictive modelling or machine learning can analyze historical noise patterns, enabling anticipatory adjustments to $\theta$ and $r$ before significant deviations

occur. This preemptive approach reduces reliance solely on reactive adjustments, enhancing the system's ability to maintain stability under various noise conditions.

- **Algorithm Efficiency and Minimization of Latency.** For high-intensity noise types such as DoS, latency in the feedback mechanism could lead to significant state degradation. Optimizing the feedback algorithm to minimize processing delays is essential for high-frequency adjustments, ensuring that modulation parameters are updated in near real-time. Efficient algorithms enable the feedback mechanism to continuously counteract noise, preserving the coherence of the quantum state.

An efficient real-time feedback loop enhances the system's ability to maintain secure and stable quantum communication, ensuring resilience against various adversarial noise types. Additionally, exploring more advanced feedback algorithms, such as those based on machine learning, could allow the system to autonomously adapt to complex and evolving noise profiles, further improving adaptability and response time.

The adaptive modulation strategy described in this section provides a robust framework for countering adversarial noise in quantum communication systems. By combining continuous adjustments to $\theta$ and $r$ with real-time feedback, the proposed approach ensures resilience against reconnaissance, exploratory, and DoS noise, preserving the integrity and security of quantum states in continuous-variable quantum communication systems.

## 3. Methods

In this section, we outline the simulation and experimental methodologies used to investigate the feasibility of adaptive modulation as a countermeasure for adversarial noise in continuous-variable quantum communication systems. Our proposed approach involves dynamically adjusting phase-space rotation angles ($\theta$) and squeezing parameters ($r$) to mitigate noise, minimize energy deviation, and maintain quantum state fidelity. However, due to hardware constraints, our experimental implementation was limited to adjusting only the phase-space rotation angle ($\theta$) without real-time feedback or dynamic squeezing adjustments.

The theoretical framework developed in previous sections provides a basis for optimizing phase and squeezing adjustments in response to different types of adversarial noise, including reconnaissance, exploratory, and denial-of-service (DoS) attacks. Our simulations utilize these insights via Xanadu's *Strawberry Fields* platform to evaluate the effectiveness of phase-first modulation strategies. Subsequently, we conduct experimental validation on Xanadu's X8_01 photonic quantum processor, focusing specifically on phase modulation under heavy noise conditions due to the device's limitations.

### *3.1. Theoretical Framework*

#### 3.1.1. Adversarial Noise Modulation of Qumodes

Qumodes, as continuous-variable quantum states, are highly susceptible to adversarial noise attacks, including reconnaissance, exploratory, and DoS attacks. Each form of adversarial noise presents unique challenges to quantum coherence and state fidelity. Our theoretical analysis indicates that dynamically adjusting both the qumode's squeezing parameter $r$ and phase-space rotation angle $\theta$ could mitigate these effects. In our framework, modulation is designed to operate based on real-time feedback from the noise profile in the communication channel [14,18].

We developed analytical models that simulate qumode responses under various adversarial noise conditions, focusing on performance metrics such as energy deviation and purity. The framework employs a phase-first modulation strategy as the primary defense mechanism, with potential squeezing adjustments to further reduce energy deviations if needed [2,19].

#### 3.1.2. Phase-First and Squeezing Modulation

Our **Phase-first modulation strategy** prioritizes adjustments to the phase-space rotation angle ($\theta$) before modifying the squeezing parameter ($r$) in response to adversarial noise. This approach is based on a theoretical model that links energy deviation $\Delta E$ with the adversarial noise profile. For severe adversarial noise, such as DoS attacks, combining adjustments to both $\theta$ and $r$ is theoretically essential to maintain quantum state stability [13,18].

The derived formulas in our theoretical model serve as a basis for optimizing $r$ and $\theta$ based on the noise type and intensity. These theoretical results are further detailed in the results section, where we demonstrate how these modulation strategies effectively reduce energy deviation and enhance system resilience under adversarial conditions.

### *3.2. Simulation Methodology*

#### 3.2.1. Simulation Setup

Simulations were conducted using the *Strawberry Fields* library with the *fock* backend on Xanadu's platform [13]. These simulations model the impact of DoS attacks on continuous-variable quantum communication systems, specifically evaluating the effects of phase-first modulation and theoretical squeezing adjustments under adversarial noise. The simulation methodology followed these steps:

1. **Initial Qumode Preparation** - The qumodes were initialized in both the **vacuum state** and **squeezed states** to serve as baseline conditions. The vacuum state, with minimal energy deviation, and squeezed states, introducing predefined squeezing $r$, formed the basis for subsequent modulation strategies [7].
2. **Adversarial Noise Modeling** - A DoS adversarial noise model was introduced to simulate high-intensity interference, primarily affecting the $p$-quadrature. The noise profile was designed to mimic significant interference (up to 80%) encountered in adversarial scenarios [18,20].
3. **Phase and Squeezing Modulation** - After introducing noise, the qumodes underwent phase-first modulation, adjusting $\theta$ to mitigate the effects of adversarial noise. Squeezing adjustments $r$ were also evaluated theoretically to further reduce energy deviation and stabilize the qumode's state [13]. This combined modulation strategy was tested across various noise intensities.

- **Energy Deviation** - Energy deviation served as the primary metric for assessing qumode resilience to adversarial noise. It reflects variance across qumode quadratures (both $x$ and $p$) and indicates the extent of noise impact on the system [13,18].
- **Wigner Function Analysis** - Wigner function plots visualized the effects of adversarial noise and the applied modulation on qumode states, offering insight into the state distribution in phase space. Smoother Wigner contours indicated improved state stability, confirming the effectiveness of modulation strategies [14].

Simulation results, benchmarked against control groups of non-modulated qumodes, indicated that phase-first modulation combined with squeezing could reduce energy deviation by 35% to 50%, depending on the noise type and intensity. These findings support both our theoretical predictions and experimental observations.

### *3.3. Experimental Methodology*

#### 3.3.1. Experimental Design

To validate our theoretical predictions, we conducted real quantum experiments on Xanadu's X8_01 photonic quantum processor. Given hardware constraints, the experiments were limited to phase modulation and its impact on energy deviation under heavy adver-

sarial noise. The primary goal was to identify optimal phase angles $\theta$ that minimize energy deviation without employing real-time feedback or squeezing modulation. Despite these limitations, the experiments offer valuable insights into phase-first modulation strategies.

#### 3.3.2. Experimental Procedure

The experimental procedure followed these steps:

1. **Qumode Initialization** - The qumodes were initialized in the **vacuum state** on the X8_01 platform [7], setting a neutral phase-space configuration as a baseline.
2. **Phase Modulation under Heavy Adversarial Noise** - Phase modulations were applied across a range of angles under heavy noise conditions, from $-\pi$ to $\pi$ in 10-degree increments. This process allowed us to assess energy deviation across different phase angles. Due to platform limitations, no squeezing operations were applied.
3. **Energy Deviation Measurement** - Energy deviation was measured before and after applying noise for both modulated and non-modulated states. Results were plotted against phase angles, showing that optimal energy deviation did not always align with classical phase values such as $\pi/2$ or $\pi/4$. Instead, results emphasized the need for dynamic phase optimization under noise conditions.

#### 3.3.3. Data Collection and Analysis

Data were collected over multiple runs to account for hardware variability. Analysis focused on identifying energy deviation trends relative to phase modulation under adversarial noise. As shown in Figure 3, the findings confirmed that phase-first modulation significantly reduces energy deviation compared to non-modulated qumodes, particularly under heavy noise conditions. These results closely align with theoretical predictions, highlighting the effectiveness of adaptive phase modulation in practical quantum communication systems.

## 4. Results

This section presents the findings from our theoretical models, simulations, and experimental validation, collectively demonstrating the potential of adaptive modulation strategies for mitigating adversarial noise in continuous-variable quantum communication. Our primary investigation focused on phase modulation, with theoretical exploration into squeezing, to reduce energy deviation under adversarial conditions, particularly denial-of-service (DoS) noise. Due to hardware constraints, experimental validation was limited to phase-only modulation without real-time feedback or dynamic squeezing adjustments.

The results indicate that phase-first modulation strategies, where the phase-space rotation angle $\theta$ is adjusted dynamically, can improve the stability of quantum states against adversarial noise. Simulations and experiments both support the conclusion that optimized phase modulation enhances resilience to noise, even under heavy interference.

The following subsections provide a detailed analysis of these results, incorporating theoretical insights into adversarial noise, observed trends from simulations, and findings from experimental testing on Xanadu's X8_01 photonic quantum processor.

### *4.1. Simulation Results*

The 2D and 3D Wigner function plots in Figures 1 and 2 illustrate the effects of our adaptive modulation framework in mitigating the impact of DoS noise on continuous-variable qumodes. The initial vacuum state (A) shows a symmetric Gaussian profile, serving as a baseline. When DoS noise is applied (B), the Wigner function becomes significantly distorted, particularly in the $p$-quadrature, indicating a substantial loss of coherence.

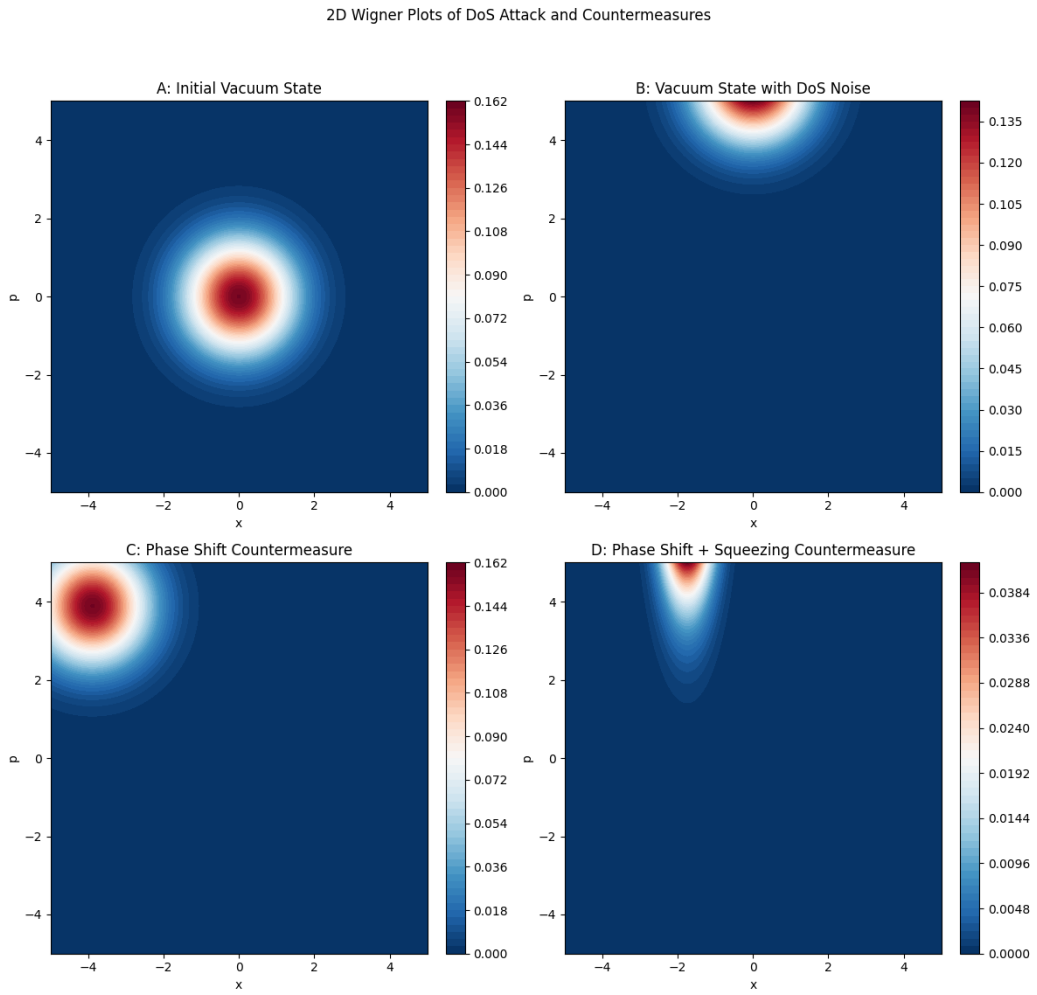


**Figure 1.** 2D Wigner function plots for various qumode states under DoS noise and countermeasures. (A) Initial vacuum state, (B) vacuum state with DoS noise showing significant distortion, (C) phase shift countermeasure applied, and (D) phase shift + squeezing countermeasure, showing reduced noise impact.

Applying a phase shift countermeasure (C) reduces this distortion, with more localized contours in the 2D plot and a concentrated peak in the 3D plot. When both phase shift and squeezing are applied (D) in the simulation, the Wigner function shows an even higher degree of localization, suggesting that in theory, phase modulation complemented by squeezing could further enhance resilience to noise.

These visual results support our approach, showing that phase modulation—and theoretically, the addition of squeezing—can improve quantum state stability under adversarial noise. The figures underscore several key points:

1. **2D and 3D Wigner Plot Insights.** Both 2D and 3D Wigner functions highlight the effectiveness of countermeasures, with the 3D plots particularly emphasizing changes in peak coherence, reflecting a more stable state distribution.
2. **Impact of DoS Noise.** The flattened and elongated Wigner distribution under DoS noise reveals the vulnerability of non-modulated states to interference, supporting the necessity of active noise mitigation.
3. **Countermeasure Effectiveness.** The combination of phase shift and squeezing in simulations shows reduced spread and restored symmetry in the Wigner function, indicating that this dual approach could theoretically offer robust noise resilience.

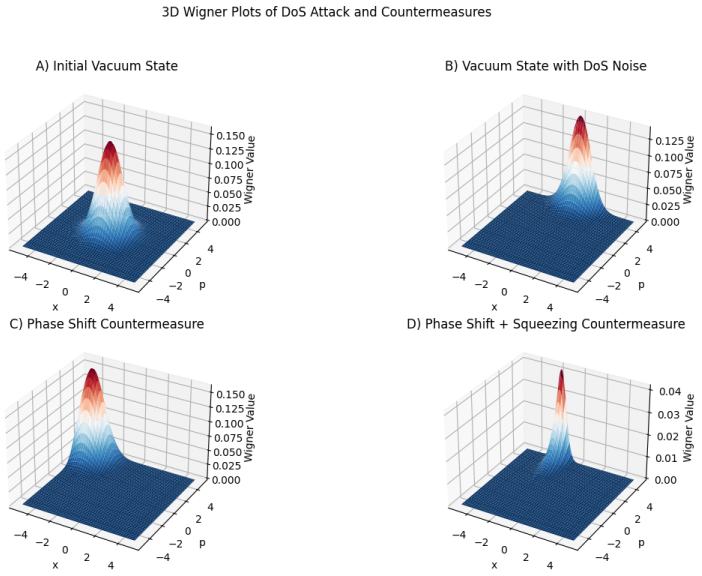


**Figure 2.** 3D Wigner function plots for various qumode states under DoS noise and countermeasures. (A) Initial vacuum state, (B) vacuum state with DoS noise, showing significant distortion, (C) phase shift countermeasure applied, and (D) phase shift + squeezing countermeasure, highlighting the changes in peak coherence and distribution.

These results demonstrate that adaptive modulation strategies, particularly phase modulation combined with squeezing (in theory), can mitigate the spread and distortion caused by adversarial noise, supporting the potential of real-time modulation for continuous-variable quantum states.

### *4.2. Experimental Results*

The experimental results on Xanadu's X8_01 photonic quantum processor further validate our modulation framework, focusing on energy deviation as a function of phase angle $\theta$ under heavy adversarial noise. Due to hardware limitations, the experiments were restricted to phase modulation without real-time feedback or squeezing adjustments. Nevertheless, these experiments provide valuable insights into the effectiveness of phase-first modulation.

Key findings from the experiments include:

1. **Energy Deviation as a Function of Phase Modulation.** Figure 3 shows that energy deviation varies across phase angles, confirming that optimized phase modulation is essential for minimizing noise-induced deviation. Notably, classical phase values like $\pi/2$ and $\pi/4$ were found suboptimal, highlighting the need for dynamic phase adjustment.
2. **Adversarial Noise Impact.** The application of heavy noise significantly increased energy deviation for non-modulated states. Phase-modulated states, however, exhibited reduced energy deviation at specific phase values, aligning with our simulation predictions and confirming the necessity of adaptive phase modulation.
3. **Consistency with Simulation Results.** The experimental data align closely with simulation results, reinforcing the effectiveness of phase-first modulation strategies. This consistency suggests that the phase modulation methodology is feasible even under limited hardware capabilities, supporting further investigation of real-time adaptive modulation.
4. **Experimental Limitations.** Although real-time modulation and squeezing operations were not feasible due to platform constraints, phase-only modulation successfully

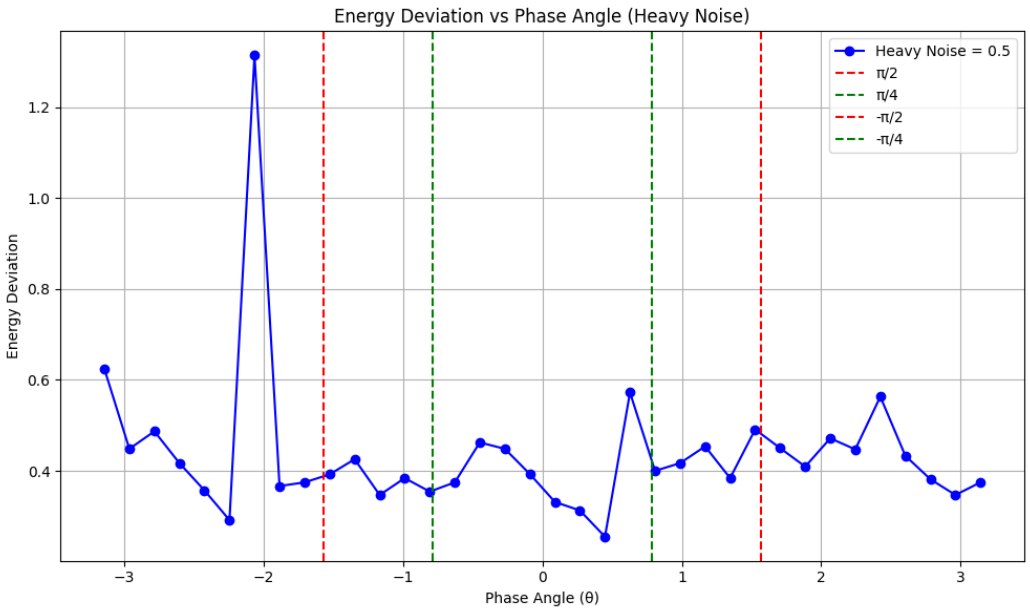


**Figure 3.** Energy deviation as a function of phase angle $\theta$ under heavy noise, performed on Xanadu's X8_01 photonic quantum processor. The results demonstrate that optimized phase modulation is crucial to minimizing energy deviation, as classical values such as $\pi/2$ and $\pi/4$ were suboptimal under these conditions.

reduced energy deviation under adversarial noise. These findings demonstrate the practicality of adaptive phase modulation even in simplified experimental setups, encouraging future work with advanced hardware for real-time feedback and dynamic squeezing.

These experimental findings emphasize the importance of adaptive phase modulation for quantum communication systems. Despite hardware limitations, phase modulation alone significantly mitigates noise-induced energy deviation, enhancing quantum state stability. Future work should extend these techniques using advanced hardware with real-time feedback and squeezing adjustments to maximize system resilience.

## 5. Discussion and Conclusion

### *5.1. Interpretation of Key Results*

Our experimental results support the efficacy of phase-first modulation in enhancing the resilience of qumodes against adversarial noise. In contrast to previous approaches, which predominantly focused on squeezing or static modulation, our findings reveal that phase modulation alone can lead to substantial reductions in energy deviation. Specifically, under heavy adversarial noise conditions, dynamic phase adjustments significantly minimized energy deviation, further emphasizing the importance of real-time feedback mechanisms for optimal performance.

A key insight from our experiments is the discovery that modulating the phase angle $\theta$ across a range (from $-\pi$ to $\pi$) revealed non-intuitive phase angles where energy deviation was minimized. These results challenge conventional approaches that use fixed phase values such as $\frac{\pi}{2}$ or $\frac{\pi}{4}$. This demonstrates the necessity of dynamic adaptation in practical implementations, particularly in noisy and adversarial environments. Our experiments on Xanadu's X8_01 photonic processor confirmed the effectiveness of phase-first modulation in countering even strong adversarial noise, highlighting its potential for real-world quantum communication systems.

### 5.2. Comparison with Existing Research

Our findings complement and expand upon previous research in quantum communication and noise mitigation. While prior studies have extensively explored static squeezing configurations to reduce noise sensitivity [21], our work demonstrates that phase-first modulation can serve as a powerful alternative or complementary approach. For instance, in Quantum Key Distribution (QKD) systems, where noise resilience is crucial, our results suggest that real-time phase modulation could play a critical role in maintaining system integrity under adversarial conditions [22].

Quantum error correction (QEC) has long been a cornerstone of noise mitigation in quantum systems, with methods like stabilizer codes providing foundational error resilience [23]. While QEC is highly effective for environmental noise, adaptive modulation may serve as an effective, lightweight alternative or supplement for real-time countermeasures against adversarial noise.

While advancements in noise-resilient QKD continue to progress, including efforts to mitigate noise-induced security risks, our adaptive modulation framework could provide an additional safeguard against active, targeted attacks on quantum states [16].

This study also aligns with the broader goal of developing noise-resilient quantum systems, particularly under adversarial conditions. However, unlike traditional approaches that primarily rely on static or predefined configurations, our dynamic modulation strategy emphasizes the need for adaptability. As quantum networks and communication protocols evolve, the incorporation of phase-first modulation can offer an additional layer of security and stability in the face of adversarial attacks [24].

### 5.3. Broader Implications for Quantum Information Processing

The success of phase-first modulation in reducing energy deviation has broader implications for both quantum communication and quantum computing. In quantum communication, dynamic phase modulation can significantly enhance the robustness of quantum states during transmission, particularly in noisy or adversarial environments. This method could be instrumental in the development of future quantum internet infrastructures, where adaptive feedback mechanisms optimize phase angles in real-time, improving both key generation rates and entanglement distribution in QKD systems.

As the field progresses towards fault-tolerant quantum computing, adaptive modulation could complement error correction frameworks, helping to alleviate the computational overhead associated with QEC [25].

In quantum computing, especially in fault-tolerant architectures, phase-first modulation can contribute to maintaining qumode coherence in the presence of environmental or adversarial noise. As quantum processors become more complex, dynamic modulation strategies like the one proposed in this work can help reduce the computational burden on error correction frameworks, potentially increasing both system efficiency and overall fault tolerance.

### 5.4. Limitations

While the experimental results are promising, the study is limited by the constraints of the hardware platform used. The X8_01 photonic quantum processor employed in our experiments supports phase modulation but lacks the capacity for real-time squeezing adjustments, limiting our ability to explore the full range of modulation strategies. Additionally, our experiments focused on single-mode qumodes, meaning that further research is required to investigate how these strategies scale in multi-mode or distributed quantum networks.

Another limitation is the absence of real-time feedback mechanisms. Although our post-experiment adjustments demonstrated significant reductions in energy deviation, the integration of real-time adaptive modulation could further improve the system's ability to counteract noise dynamically. Future research will require more advanced hardware platforms capable of supporting real-time modulation strategies.

### *5.5. Future Directions*

Building on the promising results of phase-first modulation, future research should focus on several key areas:

1. **Scaling the framework** - Extending phase-first modulation strategies to multi-mode quantum systems and distributed quantum networks will be critical for assessing their robustness in more complex adversarial scenarios.
2. **Real-time feedback** - The integration of real-time feedback systems is an essential next step. Adaptive modulation that reacts dynamically to changing noise conditions could greatly enhance the noise resilience of quantum communication systems.
3. **Machine Learning** - Integrating machine learning or quantum machine learning, into adaptive modulation could enhance predictive noise mitigation. Recent studies have demonstrated that reinforcement learning and neural networks can dynamically adjust quantum systems under noise [26,27]. Leveraging these tools may allow our framework to preemptively adapt to adversarial noise.
4. **Exploring additional adversarial noise models** - While this study focused on reconnaissance and denial-of-service (DoS) attacks, future research should explore more sophisticated adversarial models to fully understand the limits and potential of the proposed modulation framework.
5. **Integration with quantum error correction** - Incorporating phase-first modulation into quantum error correction frameworks could mitigate decoherence and other noise-induced errors, particularly in fault-tolerant quantum computing systems.

This work has established a foundation for future advancements in noise-resilient quantum communication and computation. As quantum technologies continue to evolve, the need for dynamic, adaptive modulation strategies like phase-first modulation will become increasingly critical in ensuring the stability and security of quantum systems.

**Author Contributions:** Conceptualization, J.R.R.B.; methodology, J.R.R.B. and J.V.G.T.; investigation, J.R.R.B.; validation, J.V.G.T., R.A.F., and M.P.; formal analysis, J.R.R.B.; writing, original draft, J.R.R.B.; writing, review and editing, J.V.G.T., R.A.F., M.P., N.S., S.R.V., A.T. and A.T; supervision, R.A.F.

**Funding:** This research was funded by the Natural Sciences and Engineering Research Council of Canada (NSERC), Discovery Grants Program and by LAKES Environmental Research Inc., Canada.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Data available from the corresponding author upon reasonable request.

**Acknowledgments:**

The authors thank Xanadu for providing access to experimental platforms used in this research.

We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC), RGPIN-2023-04513.
Cette recherche a été financée par le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG), RGPIN-2023-04513.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| CVQC | Continuous-Variable Quantum Communication |
| CV | Continuous Variable |
| QIP | Quantum Information Processing |
| DoS | Denial of Service |

## Appendix A Experimental Setup

This section describes the experimental setup used in Section 3.3, outlining how we performed the experimental validation of adversarial noise mitigation using Xanadu's hardware.

### *Appendix A.1 Hardware Configuration*

Experiments were conducted on Xanadu's X8_01 photonic quantum processor, which supports Gaussian operations, including squeezing, phase-space rotations, and beam splitting [13]. The primary objective of the experimental validation was to evaluate how phase-first modulation mitigates adversarial noise by dynamically adjusting the phase-space rotation $\theta$ under heavy noise conditions. Due to platform constraints, squeezing operations were not applied, and the focus was solely on phase modulation to reduce energy deviation.

The experimental hardware allowed us to simulate adversarial noise models but limited real-time feedback. Thus, post-noise adjustments were made based on pre-measured energy deviation trends.

### *Appendix A.2 Qumode Preparation*

The qumodes were initialized in the **vacuum state**, serving as the baseline for adversarial noise testing:

- **Vacuum State** - Initialized without photons, squeezing, or phase-space rotation, the vacuum state is highly sensitive to noise, providing an ideal scenario to test phase-first modulation for noise mitigation [19].

In this setup, the phase-first modulation strategy focused on adjusting the phase-space rotation $\theta$ in response to adversarial noise while ensuring that the energy deviation remained minimized.

### *Appendix A.3 Adversarial Noise Injection*

Adversarial noise models were applied to test the system's resilience to different types of quantum noise:

- **Heavy Noise** - Significant noise perturbations were introduced to simulate worst-case scenarios, where the goal is to overwhelm the qumode's stability. The noise was modelled as high-amplitude random phase shifts. The objective was to test whether optimal phase modulation could restore stability post-noise.

The modulation framework explored a range of phase angles $\theta$ from $-\pi$ to $\pi$, identifying angles that minimized energy deviation after noise injection. Unlike real-time noise compensation, phase modulation was adjusted post-noise based on pre-obtained energy deviation data.

*Appendix A.4 Measurement Procedure*

To quantify the effectiveness of the modulation framework, the following measurements were recorded:

1. **Initial energy deviation** - Recorded for the qumodes in the vacuum state before applying adversarial noise.
2. **Energy deviation after heavy noise without modulation** - This established the baseline impact of adversarial noise on the system without applying any modulation.
3. **Energy deviation after modulation** - Phase modulation was applied across different values of $\theta$ to minimize the energy deviation. This helped identify the phase angles that achieved the best noise resilience [9].

Experimental results were gathered over several trials, and energy deviation was measured as the primary metric to evaluate the modulation framework's performance.

*Appendix A.5 Experimental Limitations*

The experimental setup faced certain constraints:

1. **Real-time feedback and adaptation** - Real-time adaptive feedback was not feasible due to hardware limitations. Instead, phase modulation was applied after noise injection based on pre-collected data.
2. **Squeezing operations** - Due to platform constraints, squeezing operations could not be performed. Thus, the experiments focused exclusively on phase modulation as the primary noise mitigation strategy.

Despite these limitations, the experimental setup successfully demonstrated that phase-first modulation effectively reduces energy deviation under heavy noise, confirming the feasibility of this approach for real-world quantum communication systems.

## References


1. Gangopadhyay, S.; Wang, T.; Mashatan, A.; Ghose, S. Controlled quantum teleportation in the presence of an adversary. *Physical Review A* **2022**, *106*, 052433. Publisher: American Physical Society, https://doi.org/10.1103/PhysRevA.106.052433.
2. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Advances in Optics and Photonics* **2020**, *12*, 1012–1236. Publisher: Optica Publishing Group, https://doi.org/10.1364/AOP.361502.
3. Wehner, S.; Elkouss, D.; Hanson, R. Quantum internet: A vision for the road ahead. *Science* **2018**, *362*, eaam9288. https://doi.org/10.1126/science.aam9288.
4. Pironio, S.; Acín, A.; Massar, S.; De La Giroday, A.B.; Matsukevich, D.N.; Maunz, P.; Olmschenk, S.; Hayes, D.; Luo, L.; Manning, T.A.; et al. Random numbers certified by Bell's theorem. *Nature* **2010**, *464*, 1021–1024. https://doi.org/10.1038/nature09008.
5. Lipka-Bartosik, P.; Diotallevi, G.F.; Bakhshinezhad, P. Fundamental Limits on Anomalous Energy Flows in Correlated Quantum Systems. *Physical Review Letters* **2024**, *132*, 140402. https://doi.org/10.1103/PhysRevLett.132.140402.
6. Micadei, K.; Peterson, J.P.S.; Souza, A.M.; Sarthour, R.S.; Oliveira, I.S.; Landi, G.T.; Batalhão, T.B.; Serra, R.M.; Lutz, E. Reversing the direction of heat flow using quantum correlations. *Nature Communications* **2019**, *10*, 2456. https://doi.org/10.1038/s41467-019-10333-7.
7. Su, X.; Zhao, Y.; Hao, S.; Jia, X.; Xie, C.; Peng, K. Experimental preparation of eight-partite cluster state for photonic qumodes. *Optics letters* **2012**, *37*, 5178–5180. Place: United States Publisher: The Optical Society, https://doi.org/10.1364/OL.37.005178.
8. Hu, X.M.; Zhang, C.; Guo, Y.; Wang, F.X.; Xing, W.B.; Huang, C.X.; Liu, B.H.; Huang, Y.F.; Li, C.F.; Guo, G.C.; et al. Pathways for Entanglement-Based Quantum Communication in the Face of High Noise. *Physical Review Letters* **2021**, *127*, 110505. Publisher: American Physical Society, https://doi.org/10.1103/PhysRevLett.127.110505.

9. Crockett, B.; Romero Cortés, L.; Maram, R.; Azaña, J. Optical signal denoising through temporal passive amplification. *Optica* **2022**, *9*, 130. https://doi.org/10.1364/OPTICA.428727.
10. Simmons, C.; Noblet, Y.; Castillo, A.T.; Donaldson, R. An investigation of jamming in free-space quantum key distribution. In Proceedings of the Quantum Technology: Driving Commercialisation of an Enabling Science III. SPIE, 2023, Vol. 12335, pp. 84–91. https://doi.org/10.1117/12.2644866.
11. Brassard, G.; Nayak, A.; Tapp, A.; Touchette, D.; Unger, F. Noisy Interactive Quantum Communication. *SIAM Journal on Computing* **2019**, *48*, 1147–1195. Publisher: Society for Industrial and Applied Mathematics, https://doi.org/10.1137/16M109867X.
12. Kuang, R.; Perepechaenko, M. Quantum encryption with quantum permutation pad in IBMQ systems. *EPJ Quantum Technology* **2022**, *9*, 1–26. Number: 1 Publisher: SpringerOpen, https://doi.org/10.1140/epjqt/s40507-022-00145-y.
13. Killoran, N.; Izaac, J.; Quesada, N.; Bergholm, V.; Amy, M.; Weedbrook, C. Strawberry Fields: A Software Platform for Photonic Quantum Computing. *Quantum* **2019**, *3*, 129. Publisher: Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften, https://doi.org/10.22331/q-2019-03-11-129.
14. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Reviews of Modern Physics* **2012**, *84*, 621–669. Publisher: American Physical Society, https://doi.org/10.1103/RevModPhys.84.621.
15. Rosas-Bustos, J.R.; Thé, J.V.G.; Frayser, R. Unveiling Hidden Vulnerabilities in Quantum Systems by Expanding Attack Vectors through Heisenberg's Uncertainty Principle, 2024. https://doi.org/10.21203/rs.3.rs-4979824/v1.
16. Diamanti, E.; Lo, H.K.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Information* **2016**, *2*, 1–12. Publisher: Nature Publishing Group, https://doi.org/10.1038/npjqi.2016.25.
17. Wiseman, H.M.; Milburn, G.J. *Quantum Measurement and Control*; Cambridge University Press: Cambridge, 2009. https://doi.org/10.1017/CBO9780511813948.
18. Pfister, O. Continuous-variable quantum computing in the quantum optical frequency comb. *Journal of physics. B, Atomic, molecular, and optical physics* **2020**, *53*, 12001–. Publisher: IOP Publishing, https://doi.org/10.1088/1361-6455/ab526f.
19. Yang, Z.; Jahanbozorgi, M.; Jeong, D.; Sun, S.; Pfister, O.; Lee, H.; Yi, X. A squeezed quantum microcomb on a chip. *Nature Communications* **2021**, *12*, 4781. https://doi.org/10.1038/s41467-021-25054-z.
20. Mao, Y.; Huang, W.; Zhong, H.; Wang, Y.; Qin, H.; Guo, Y.; Huang, D. Detecting quantum attacks: a machine learning based defense strategy for practical continuous-variable quantum key distribution. *New journal of physics* **2020**, *22*, 83073–. Place: Bristol Publisher: IOP Publishing, https://doi.org/10.1088/1367-2630/aba8d4.
21. Huang, W.; Liang, X.; Zhu, B.; Yan, Y.; Yuan, C.H.; Zhang, W.; Chen, L. Protection of Noise Squeezing in a Quantum Interferometer with Optimal Resource Allocation. *Physical Review Letters* **2023**, *130*, 073601. Publisher: American Physical Society, https://doi.org/10.1103/PhysRevLett.130.073601.
22. Shao, Y.; Wang, H.; Pi, Y.; Huang, W.; Li, Y.; Liu, J.; Yang, J.; Zhang, Y.; Xu, B. Phase noise model for continuous-variable quantum key distribution using a local local oscillator. *Physical Review A* **2021**, *104*, 032608. Publisher: American Physical Society, https://doi.org/10.1103/PhysRevA.104.032608.
23. Terhal, B.M. Quantum error correction for quantum memories. *Reviews of Modern Physics* **2015**, *87*, 307–346. Publisher: American Physical Society, https://doi.org/10.1103/RevModPhys.87.307.
24. Sohr, P.; Ecker, S.; Bulla, L.; Bohmann, M.; Ursin, R. Overcoming noise limitations in quantum key distribution with quantum privacy amplification. *Physical Review Applied* **2024**, *22*, 024059. Publisher: American Physical Society, https://doi.org/10.1103/PhysRevApplied.22.024059.
25. Preskill, J. Quantum Computing in the NISQ era and beyond. *Quantum* **2018**, *2*, 79. https://doi.org/10.22331/q-2018-08-06-79.

26. Bukov, M.; Day, A.G.; Sels, D.; Weinberg, P.; Polkovnikov, A.; Mehta, P. Reinforcement Learning in Different Phases of Quantum Control. *Physical Review X* **2018**, *8*, 031086. Publisher: American Physical Society, https://doi.org/10.1103/PhysRevX.8.031086.
27. Carleo, G.; Troyer, M. Solving the quantum many-body problem with artificial neural networks. *Science* **2017**, *355*, 602–606. Publisher: American Association for the Advancement of Science, https://doi.org/10.1126/science.aag2302.

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