

Article

Not peer-reviewed version

Entropy of the Quantum-Classical Interface: A Potential Metric for Security

[Sarah Chehade](#)^{*}, [Joel A. Dawson](#), [Stacy Prowell](#), [And Ali Passian](#)

Posted Date: 20 February 2025

doi: 10.20944/preprints202502.1598.v1

Keywords: Entropy; quantum security; quantum-classical interface; entropic measures; quantum information theory; classical information theory



Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Article

Entropy of the Quantum-Classical Interface: A Potential Metric for Security

Sarah Chehade^{1,2,*} , Joel A. Dawson^{3,4} , Stacy Prowell^{3,4}  and Ali Passian^{1,2} 

¹ Quantum Information Science Section, Oak Ridge National Laboratory

² Computational Sciences and Engineering Division, Oak Ridge National Laboratory

³ Resilient Cyber-Physical Systems Section, Oak Ridge National Laboratory, Oak Ridge

⁴ Cyber Resilience and Intellegence Division, Oak Ridge National Laboratory

* Correspondence: chehades@ornl.gov

Abstract: The quantum-classical interface (QCI) i.e., the boundary where quantum and classical systems interact, introduces unique security challenges and potential vulnerabilities within quantum technologies. This position paper explores the use of entropy as one metric to monitor and secure information transfer across the QCI. We propose an initial QCI security framework, outlining criteria by which entropy-based measures contribute to detecting deviations and potential threats to quantum system integrity. By presenting these theoretical constructs, we aim to catalyze further investigation and discussion, establishing a basis for empirical validations and future development of practical quantum security strategies.

Keywords: entropy; quantum security; quantum-classical interface; risk assessment; entropic measures; quantum information theory; classical information theory

1. Introduction

¹ The rapid advancement of quantum technologies has highlighted the significance of the quantum-classical interface (QCI), a critical “node” where quantum and classical systems interact and communicate. While the QCI is essential to harnessing the power of quantum technologies, it also introduces unique security vulnerabilities. Historically, the boundary between quantum and classical realms has remained distinct and largely unexplored. As hybrid quantum-classical systems become more prevalent, traditional notions of information and security warrant closer examination, given that quantum information fundamentally differs from its classical counterpart, a disparity that introduces complex challenges in securing the information flux across the QCI. In particular, entropy quantifies uncertainty, which is crucial in security applications. Different entropy measures ensure various security aspects such as average uncertainty, conditional uncertainty, and distinguishability.

Central to our position paper is the introduction of entropy as a metric for QCI security. We aim to explore how entropy, as a measure of uncertainty, can help quantify information exchange between quantum and classical domains, revealing potential vulnerabilities and guiding protective strategies. To fully realize this approach, it is of key importance to map the intricacies of quantum systems, their interaction with classical control mechanisms, and the impact of quantum measurements [1] and external perturbations [2]. Our aim is to stimulate methods that quantify the information interchange between the quantum and classical spheres, offering information on possible vulnerabilities and charting pathways for protection of quantum devices.

¹ This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The Department of Energy will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (<http://energy.gov/downloads/doe-public-access-plan>).

The study of the quantum-classical interface (QCI) and hybrid quantum-classical systems remains open, lacking a universally accepted framework. This manuscript does not claim to provide a definitive formulation but rather presents a structured perspective to inspire further exploration. While many studies focus on the structural and dynamical consistency of hybrid systems [3–7], our motivation stems from security concerns—specifically, whether the QCI introduces vulnerabilities that can be quantified using entropy-based methods. Given the challenges of hybrid dynamics, alternative formulations may be more suitable in different contexts [3,7]. We argue that alongside fundamental studies, security implications must be considered, especially in applications involving quantum sensors, cryptography, or hybrid control. By refining interface conditions and leveraging entropy, we offer a perspective that may guide both theoretical and experimental investigations into security risks in hybrid systems. Ultimately, this work aims to stimulate further discussion and refinement rather than propose a final or exhaustive framework.

Our presentation is organized as follows: In Section 2, we discuss classical, quantum, and quantum-classical interfaces and present a formal definition of the QCI. Section 3 highlights all the proposed entropic functions that evaluate QCI while Section 4 proposes the use of complementary metrics that are common anomaly detectors. Section 5 outlines reasonable criteria for QCI security and highlights known classical counterparts. We end this position paper with a discussion in Section 6 and concluding remarks in Section 7.

2. Preliminaries

2.1. Formalization of an Interface

In the QCI context, we define an *interface* as a condition under which the states of the two systems are coupled or connected to various degrees of strength. Let $u_1(\mathbf{p}_1)$ and $u_2(\mathbf{p}_2)$ represent the states of System 1 and System 2, respectively. Here, u_1 lies in a classical phase space if System 1 is classical, and u_2 lies in a quantum Hilbert space if System 2 is quantum. Thus, the states u_i can be functions, vectors, or operators, depending on the nature of the system. The variables \mathbf{p}_1 and \mathbf{p}_2 represent the parameters specific to each system. For example, they could parameterize the state but do not define their evolution. To characterize the interaction between u_1 and u_2 over the parameters \mathbf{p}_1 and \mathbf{p}_2 , we define a coupling function $\mathcal{K}(u_1, u_2; \mathbf{p}_1, \mathbf{p}_2)$. Namely, the *interface condition* can then be expressed as an equation or constraint that satisfies $\mathcal{K}(u_1, u_2; \mathbf{p}_1, \mathbf{p}_2) = 0$ (or within a bounded tolerance). We then define a general interface equation:

$$\mathcal{K}(u_1(\mathbf{p}_1), u_2(\mathbf{p}_2)) = f(u_1(\mathbf{p}_1)) - g(u_2(\mathbf{p}_2)) = 0, \quad (1)$$

where f and g are transformations or mappings that bring the states u_1 and u_2 into a common interaction space (e.g., converting quantum states to classical observables or vice versa).

In a control interface, the classical system often acts as an external controller, which modifies the quantum observable. To introduce a functional dependence in the transformation maps, such that the quantum state transformation depends on the classical states, we require

$$\mathcal{K}(u_1(\mathbf{p}_1), u_2(\mathbf{p}_2)) = f(u_1(\mathbf{p}_1), u_2(\mathbf{p}_2)) - g(u_2(\mathbf{p}_2)) = 0. \quad (2)$$

This modification allows a classical state $u_1(\mathbf{p}_1)$ to influence the transformation function f , rather than assuming a fixed changed.

If the systems evolve over time, the coupling depends on time t :

$$\mathcal{K}(u_1(\mathbf{p}_1), u_2(\mathbf{p}_2), t) = 0, \quad (3)$$

which represents dynamic coupling, such as energy exchange or information transfer, where \mathcal{K} changes over time based on the state evolution of each system.

Example 1. If u_1 is a quantum state $|\psi\rangle$ and u_2 is a classical observable x , then we define an interface by the expectation value:

$$\mathcal{K}(u_1, u_2; \mathbf{p}_1, \mathbf{p}_2) = \langle \psi | \hat{O} | \psi \rangle - x(\mathbf{p}_2) = 0, \quad (4)$$

where \hat{O} is a quantum operator whose expectation value matches the value of the classical observable x after the measurement (x acting on the phase space). This coupling creates a link between the quantum and classical systems. In this example, x is the passivable state variable representing an observed quantity in the system.

This level of formal representation suffices for our objectives in the rest of this manuscript, and Figure 1 depicts the workflow of our QCI representation.

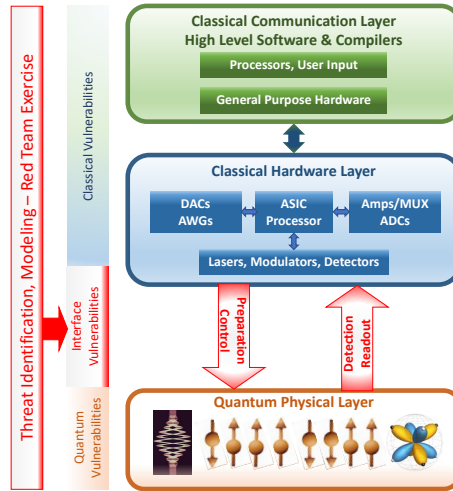


Figure 1. High-level depiction of a physical QCI in the context of a larger quantum information hardware stack. The conversion of classical physical states into discrete physical qubits - and vice versa - is enabled by hardware that, in effect, responds to control inputs encoded in logical bits or qubits.

2.2. Interface from a Hamiltonian

Writing the interface equation in terms of Hamiltonians ensures that the evolution respects the underlying symmetries and conservation laws and many hybrid quantum-classical models naturally arise from a Hamiltonian framework. To do this, we introduce the quantum Hamiltonian H_q , governing the quantum subsystem and the classical Hamiltonian H_c , governing the classical subsystem. The coupling term between the quantum and classical components can be incorporated into a total Hamiltonian H_{tot} defined as the total Hamiltonian of a generic QCI:

$$H_{\text{tot}}(q, p, \hat{O}) = H_c(q, p) + H_q(\hat{O}) + H_{\text{int}}(q, p, \hat{O}), \quad (5)$$

where $H_{\text{int}}(q, p, \hat{O})$ mediates the interaction between the two subsystems. By considering the Hamiltonian equations of motion, we can develop an interface condition:

$$\mathcal{C}(q, p, \hat{O}) = -\frac{\partial H_{\text{int}}}{\partial q} - \left\langle \frac{\delta H_{\text{int}}}{\delta \hat{O}} \right\rangle = 0. \quad (6)$$

That is, the classical subsystem is influenced by the quantum expectation values while maintaining consistency with the quantum commutator evolution. The first term $-\frac{\partial H_{\text{int}}}{\partial q}$, represents the force exerted by the interaction Hamiltonian on the classical system. The second term $\left\langle \frac{\delta H_{\text{int}}}{\delta \hat{O}} \right\rangle$, captures the quantum back-action on the classical system, where the variation with respect to \hat{O} determines how the quantum state influences the evolution of the classical degrees of freedom. The functional derivative appears because H_{int} generally depends on quantum observables, which are operator-valued quantities, requiring a variational treatment to correctly describe their effect on the classical

equations of motion. This term ensures that the expectation value of quantum fluctuations modifies the classical dynamics in a self-consistent manner, preserving the hybrid system's stability.

A key aspect of the interaction is the proper coupling of classical and quantum components. The classical variables influence the quantum system "parametrically," appearing as externally controlled parameters in $H_q + H_{\text{int}}$, while the quantum system influences the classical dynamics through expectation values in the classical equations of motion. This avoids mathematical inconsistencies yielding a physically valid quantum-classical hybrid system.

Furthermore, H_{int} introduces an intrinsic feedback mechanism. For example, the term $\lambda q \hat{\sigma}_x$ leads to continuous bidirectional coupling: the classical displacement q modifies the quantum Hamiltonian, altering quantum evolution, while the quantum expectation $\langle \hat{\sigma}_x \rangle$ contributes to the classical force, modifying the oscillator's motion. In principle, delayed feedback could be introduced by incorporating memory-dependent terms such as $H_{\text{int}}(q(t - \tau), p(t - \tau), \hat{\sigma}_x)$, leading to non-Markovian corrections.

2.3. Classical Interfaces and Security

In the classical domain, such as computing and communication systems, security at the classical-classical interface, where two distinct classical systems interact, has been extensively studied and developed in both the physical [8] and computational domains [9,10].

Understood as a physical exchange, a classical-classical interface is an exchange of signals or energy between two systems that can be modeled using the tools and intuitions of classical physics. Explicitly, we would say that these signals are reproducible to an arbitrary degree of precision, that measurement of these signals is *non-destructive*, and that any observed non-deterministic dynamics are the result of incomplete knowledge about the system. The attribute of security, then, pertains to measurable, deterministic properties of the signal exchange, and efforts by attackers or defenders to disrupt or maintain these properties. This covers a wide field of study, from traditional jamming to sensor spoofing and side-channel techniques.

While the term is "classical computation" is still somewhat informal, we define a "classical computer" as one that is implementable through a combination of classical states exhibiting deterministic behavior. A classical computer reflects classical physics in its operational logic and behavior. Ideally, it is deterministic, fully traceable, and arbitrarily precise. (In a digital system, *arbitrary precision* is mediated by the allocation of discrete resources, i.e., bits, processor cycles, etc.) Any ideal interface between two such systems will exhibit similar features, as will the semantics of any symbols exchanged via such an interface.

Because these interfaces convey signals that encode semantically-meaningful statements, classical-classical interface security emphasizes techniques that prevent the malicious reading, destruction, or editing of these statements or their constituent symbols. To do this, security teams rely on well-established cryptographic methods to encrypt messages, detect tampering, and verify message properties and authorship [9]. Even with cryptographic protocols, classical-classical interfaces are vulnerable to certain attacks that exploit the boundaries between systems. For instance, man-in-the-middle attacks, command injection, and protocol and serialization exploitation can all occur during data exchanges between two classical systems, emphasizing the rather plain fact that any shared boundary introduces potential security weaknesses [11]. This understanding of classical-classical interface security offers a valuable perspective when addressing the complexities of the QCI, where traditional methods are insufficient and new security paradigms such as entropy-based measures are required.

2.4. Quantum-Classical Interface (QCI)

To formally define the QCI, we wish to consider a general and abstract way to mathematically formulate the QCI. We introduce entropic measures as core mathematical tools to capture information dynamics across QCI, essential in characterizing how information transforms and potentially degrades when transitioning between quantum and classical systems. Beginning with the systems and states

of QCI, let \mathcal{Q} denote the set of quantum states, i.e., a quantum system, with respect to its underlying Hilbert space \mathcal{H} :

$$\mathcal{Q} = \{|\psi\rangle \in \mathcal{H} : [|\psi\rangle] = \{e^{i\theta} |\psi\rangle\} \text{ and } \|\psi\rangle\| = 1\}, \quad (7)$$

where $[|\psi\rangle]$ denotes defines an equivalence class of vectors differing only by a global phase factor $e^{i\theta}$, which ensures phase invariance. Let \mathcal{C} denote the set of classical states, i.e., the set of all probability distributions, with respect to its underlying phase space \mathcal{P} , which represents all possible configurations of the system:

$$\mathcal{C} = \{x : \mathcal{P} \rightarrow [0, 1] : \int_{\mathcal{P}} x d\mu = 1\}, \quad (8)$$

where $d\mu$ is a measure on \mathcal{P} , x typically represents a probability density over \mathcal{P} , and we assume the condition that $x \geq 0$, and $\int_{\mathcal{P}} x d\mu = 1$ ensures that x is indeed a valid probability distribution.

Transformations between the systems are defined via operators. i.e., $T_{QC} : \mathcal{H} \rightarrow \mathcal{P}$, corresponds to the quantum to classical transformation such that $x = T_{QC}(|\psi\rangle)$. Similarly, $T_{CQ} : \mathcal{P} \rightarrow \mathcal{H}$, corresponds to the classical to quantum transformation such that $|\psi\rangle = T_{CQ}(x)$ ². To describe the dynamics of the QCI, we require an operator \mathcal{L}_{QCI} that acts on the combined state of the quantum and classical system. While \mathcal{L}_{QCI} takes a specific form for a given physical scenario, here we suffice that it captures a measurement interaction (including the subsequent classical outcome).

As a conceptual framework to capture how classical systems (and their evolution) can influence and be influenced by quantum systems, at the interface where the two meet, i.e., the QCI, we introduce the unitary evolution operator $U(t)$ for the quantum system, and let $F(t)$ denote the time evolution of the classical system. At the QCI, the dynamics is given by:

$$U(t)|\psi\rangle = F(t) \circ \mathcal{L}_{QCI} \circ T_{CQ}(x), \quad (9)$$

where $T_{CQ}(x)$ describes the transformation of some classical state x into a quantum state, that is, the process of embedding classical information into the quantum domain. Subsequently, the QCI can further influence or transform this quantum state (via the linear operator \mathcal{L}_{QCI}). Thereafter, the quantum state undergoes its intrinsic time-evolution influenced by its interaction with the classical system via $F(t)$ so that the final evolved quantum state can be produced by the left-hand side.

A key aspect of the QCI is the process of measurement [1], where a quantum state collapses to a particular outcome, modeled as:

$$P_m|\psi\rangle = \delta_m(x)T_{QC}(|\psi\rangle), \quad (10)$$

where P_m is the projection operator for a measurement outcome m and a corresponding classical indicator function $\delta_m(x)$. Thus, when a quantum state $|\psi\rangle$ undergoes a measurement resulting in outcome m , it can be represented or interpreted classically as x through the transformation T_{QC} .

In practice, projective measurements are difficult to implement on hardware due to noise. To address this challenge, we adopt quantum instruments—a general framework that extends the concept of projective measurements to account for realistic, potentially noisy measurement processes, as well as the system's evolution after measurement. A quantum instrument is mathematically a collection of completely positive trace-non-increasing maps $\{\mathcal{E}_k\}$ on the set of density operators $\mathcal{D}(\mathcal{H})$ of a Hilbert space \mathcal{H} satisfying

$$\sum_k \mathcal{E}_k(\rho) = \mathcal{E}(\rho), \quad (11)$$

where \mathcal{E} is a completely positive trace-preserving map. Each \mathcal{E}_k represents a possible outcome indexed by k and it determines the post-measurement state conditioned on the outcome k . Intuitively, quantum instruments proved a mathematically rigorous way to describe realistic measurements incorporating

² In practice, when we identify quantum states with density matrices, the T_{CQ} operator takes a vector x and maps it to the matrix whose diagonal entries are precisely the vector x . Conversely, the T_{QC} operator takes the density operator, and throws away all the non-diagonal entries leaving just a classical vector.

noise and decoherence, post-measurement dynamics, i.e., how the quantum state evolves after an outcome is observed, and open quantum systems, which model interactions between quantum systems coupled to its environment.

The intrinsic complexities arising from the coexistence of quantum and classical domains in QCI includes decoherence [12], which we have not discussed. However, interactions with a classical environment, is a pivotal aspect at this interface. These interactions with the environment can often challenge the preservation of quantum properties. An example might be a qubit interfacing with a classical reading device, highlighting the bidirectional influence of both systems. The task of reliably bridging quantum and classical systems is challenging with the added difficulty of doing so within a set of security measures and constraints which underscores the significance of our discussions. Furthermore, we also consider not only the measurement interactions but also other interactions at the QCI, such as quantum-classical correlations or the challenges arising from the measurement process and classical readout. This also extends to coupling with external forces. Having defined the basic dynamics of the QCI, we now proceed with examining the QCI entropy.

2.5. A QCI Example: Classical and Quantum Langevin Equations

To better guide our QCI discussions, we utilize a classical and a quantum system, each governed by their respective Langevin equations [13–17]. A QCI is formed through coupling conditions that link these systems and facilitate interaction, see Equation (3). We first consider a classical system characterized by the position $x(t)$ and velocity $v(t)$ of a particle immersed in a thermal bath. The classical Langevin equation is:

$$m \frac{dv(t)}{dt} = -\gamma v(t) + F_e(t) + \eta(t), \quad (12)$$

where m is the particle's mass, γ represents dissipation due to the environment, $F_e(t)$ is an external deterministic force applied to the system, and $\eta(t)$ is a random force modeling thermal noise, with properties $\langle \eta(t) \rangle = 0$ and $\langle \eta(t)\eta(t') \rangle = 2D\delta(t-t')$, for a noise strength D . The state of the system is represented by $u_1(\mathbf{p}_1) = (x(t), v(t))$, with \mathbf{p}_1 encompassing parameters such as m, γ .

Next we consider a quantum system described by the operator $\hat{a}(t)$ (e.g., the annihilation operator for a quantum harmonic oscillator) interacting with a quantum environment. The quantum Langevin equation [15] is:

$$\frac{d\hat{a}(t)}{dt} = -i\omega\hat{a}(t) - \Gamma\hat{a}(t) + \hat{\zeta}(t), \quad (13)$$

where ω is the natural frequency of the quantum oscillator, Γ is the damping rate characterizing energy dissipation, and $\hat{\zeta}(t)$ is a noise operator from the environment modeled as a quantum noise source with $\langle \hat{\zeta}(t) \rangle = 0$ and commutation relations $[\hat{\zeta}(t), \hat{\zeta}^\dagger(t')] = \delta(t-t')$. The quantum state of the system is represented by $u_2(\mathbf{p}_2) = \hat{a}(t)$, with \mathbf{p}_2 containing parameters such as ω, Γ , and properties of the quantum noise $\hat{\zeta}(t)$.

The QCI is established by coupling conditions that link the states of the classical and quantum systems, for example, as follows. The external force $F_e(t)$ in the classical Langevin equation is assumed to be influenced by the quantum system's observable $\langle \hat{a}(t) + \hat{a}^\dagger(t) \rangle$ (e.g., describing the oscillation amplitude of the quantum state). This creates the coupling condition:

$$F_e(t) \sim g \langle \hat{a}(t) + \hat{a}^\dagger(t) \rangle, \quad (14)$$

where g is a coupling constant. Similarly, the quantum-classical noise operator $\hat{\zeta}(t)$ can be assumed to be influenced by the classical term $v(t)$:

$$\hat{\zeta}(t) = \hat{\zeta}_0(t) + hv(t), \quad (15)$$

where $\hat{\xi}_0(t)$ is the intrinsic quantum noise operator and h is a coupling constant. Such a coupling could be due to back-action, where the classical system affects the quantum noise. Combining these interactions, we define the interface condition:

$$\mathcal{K}(u_1, u_2; \mathbf{p}_1, \mathbf{p}_2) = \left(F_e(t) - g\langle \hat{a}(t) + \hat{a}^\dagger(t) \rangle, \hat{\xi}(t) - (\hat{\xi}_0(t) + hv(t)) \right) = 0, \quad (16)$$

which describes the coupling between the classical and quantum systems, establishing a QCI. Note that our formal interface defined via \mathcal{K} is to capture the presence or absence of interactions at the QCI. When $\mathcal{K} = 0$ includes non-zero coupling terms, it indicates active interaction and potential for information exchange. When the coupling terms are zero, the systems are independent, and no interaction occurs, and $\mathcal{K} = 0$ leads to separate, uncoupled dynamics.

3. Entropic Approach to QCI Security

Quantum systems can be susceptible to quantum attacks (e.g., quantum eavesdropping in QKD [18]) or classical attacks on their classical components. The QCI, serving as the junction where quantum and classical signals are transduced and thus information representation exchanges occur pose security challenges which is countered by monitoring the entropy at the QCI, offering a way to characterize potential information leaks.

3.1. Classical Entropy

Classical information theory invokes entropy to quantify and analyze uncertainty and information in various communication systems. For system \mathcal{C} , the measure of uncertainty for a discrete random variable X with possible outcomes $\{x_i\}_i$ from a finite alphabet \mathcal{X} and corresponding probability distribution $\{p_i\}_i = \{p(x_i)\}_i$, the realization that x_i occurs, is given by the Shannon entropy defined as:

$$H(X) := - \sum_{i=1}^n p(x_i) \log p(x_i), \quad (17)$$

with the base of the logarithm taken to be 2 to measure $H(X)$ in bits. For more information about the Shannon entropy, its applications, and its mathematical characteristics, see Chapter 10 in [19].

Example 2. From the example in Section 2.5, recall the classical system is a particle in a thermal bath described by the Langevin equation. If the system reaches thermal equilibrium, the probability distribution $P(u_1)$ follows a Boltzmann-Gibbs distribution.

$$P(u_1) = \frac{1}{Z} \exp\left(-\frac{E(x, v)}{k_B T}\right), \quad (18)$$

where T is the temperature, k_B is the Boltzmann's constant, $E(x, v) = \frac{1}{2}(mv^2 + kx^2)$ is the total energy of the system, $Z = \frac{2\pi k_B T}{\sqrt{km}}$ is the normalization factor. To simplify the calculations, we divide phase space into small bins so that the classical state $u_1 = (x, v)$. Thus, each probability is $p(x_i) \propto \exp\left(-\frac{E(x, v)}{k_B T}\right)$. With this, one could calculate the Shannon entropy as in Equation (17).

3.2. Quantum Entropy

In the case of \mathcal{Q} , the von Neumann entropy S , similarly describes the concept and quantification of uncertainty or the 'entropy' associated with the quantum state or its density representation, ρ , of the quantum system. Its definition is analogous to the Shannon entropy for \mathcal{C} :

$$S(\rho) = -\text{Tr}(\rho \log \rho), \quad (19)$$

with the logarithm in base 2 to express $S(\rho)$ in bits. For more information about the Shannon entropy, its applications, and its mathematical characteristics, see Chapter 11 in [19].

Example 3. The quantum system above is also harmonic oscillator coupled to a thermal bath at temperature T . The density operator in thermal equilibrium is

$$\rho = \frac{1}{Z} \exp\left(-\frac{\hat{H}}{k_B T}\right), \quad (20)$$

where $\hat{H} = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2})$ is the Hamiltonian.

3.3. QCI Entropy

At the QCI, entropy features both quantum and classical elements, providing an “interfacial” measure of uncertainty. The QCI system, denoted as ρ_{QC} (a tensor product of quantum and classical states), and its entropy S_{QC} captures the collective uncertainty of both domains. This encompasses not only the individual uncertainties of Q and C but also the correlations and coherence established at the interface. Consequently, QCI entropy can be interpreted in two complementary ways: (1) as the total entropy of the joint system, and (2) as a composite entropy that dissects individual contributions and interactions between quantum and classical subsystems. More formally, consider the following quantum-classical ensemble:

$$\left\{ p_C(x), \rho_Q^x \otimes |x\rangle \langle x|_C \right\}_{x \in \mathcal{C}},$$

where the first system (Q) is quantum, and the second system (C) is classical. The correlation between the quantum and classical state is represented by associating the classical state $|x\rangle$ with each quantum density operator ρ_Q^x . Here, $\{|x\rangle\}_{x \in \mathcal{C}}$ forms an orthonormal basis for the classical subsystem. The bipartite state of the quantum-classical system is expressed as:

$$\rho_{QC} = \sum_{x \in \mathcal{C}} \rho_Q^x \otimes p_C(x) |x\rangle \langle x|_C.$$

In this setup, the classical states C are perfectly distinguishable. In this case, the joint entropy is given by

$$S(\rho_{QC}) = H(C) + \sum_{x \in \mathcal{C}} p_C(x) S(\rho_Q^x), \quad (21)$$

where $H(C)$ is the classical entropy of a random variable \mathcal{C} , $p_C(x)$ is in terms of the measurement outcomes, namely $p_C(x) = \text{Tr}(\rho_Q M_x)$, for a given positive-operator valued measure associated with the classical variable x . Equation (21) quantifies the total uncertainty or lack of information about the combined quantum-classical system, however it does not indicate which part of the system the uncertainty is coming from. For this, we use a mutual information measure:

$$I(Q : C) := S(\rho_Q) + H(C) - S(\rho_{QC}). \quad (22)$$

Mutual information quantifies the dependency or correlation between Q and C . Unlike the joint entropy, which globally measures uncertainty, the mutual information focuses on the shared content between subsystems, and thus highlights how the classical subsystem ‘leaks’ information into or about the quantum system and vice versa.

3.4. Information Flow at QCI

Information flow refers to how data moves within a system, between systems, or across different security domains. When a quantum system is measured, as described by a set of positive operator valued measures $\{M_i\}$, the probability of outcome i is:

$$p(i) = \text{Tr}(M_i^\dagger M_i \rho). \quad (23)$$

This transformation from ρ to $p(i)$ represents the QCI. The entropy across this boundary, i.e., transformation between classical and quantum systems or vice versa, can be viewed as a change in information

when transitioning from a quantum to a classical system. This change is typically represented by a change in entropy. The choice of entropic function here depends on the domain interest and is chosen from the mentioned entropic functions in this section. Furthermore, the QCI acts as a bridge for information exchange between \mathcal{Q} and \mathcal{C} .

3.4.1. Quantum-to-Classical ($\mathcal{H} \rightarrow \mathcal{P}$)

In the quantum context, information flow primarily pertains to the measurement process: a measured quantum state yields a specific outcome that can be recorded classically. Through this flow, the transition is facilitated by T_{QC} , which deciphers the result of quantum computation or quantum systems' evolution.

3.4.2. Classical-to-Quantum ($\mathcal{P} \rightarrow \mathcal{H}$)

Conversely, this flow direction involves quantum state prep based on classical data or instructions, e.g., during the initialization of quantum systems, where classical data might be encoded into a quantum form, represented by the transformation T_{CQ} .

3.4.3. Interplay at QCI

At the QCI, quantum and classical states coexist and interact simultaneously. For instance, while a quantum algorithm runs, classical controls might adjust parameters based on intermediate quantum states. In this discussion, such intertwined dynamics, necessitates a comprehensive understanding of information management and exchange at the QCI, is to ensure reliable operation.

3.5. Inferring Information Flow Using Entropy at the QCI

One primary concern at the QCI is decoherence [12], where quantum information is lost to its environment, which is typically classical in nature. This loss is not just a transfer of information but an unwanted leakage that may change entropy S_{QC} . When the quantum system interacts with an external environment (i.e., an open quantum system) or when noise is present, the system undergoes decoherence. This leads to an evolution in its state, resulting in a new density matrix, ρ' , often determined using quantum master equations. The change in entropy due to such interactions can be quantified by the relative entropy:

$$S(\rho||\rho') := \text{Tr}(\rho \log \rho - \rho \log \rho'). \quad (24)$$

Although $S(\rho||\rho')$ itself does not reveal the direction of information flow, the change in entropy can provide useful metrics. In particular, relative entropy is useful for quantifying how much the system has deviated from its original state ρ to its decohered state ρ' . When $S(\rho||\rho')$ is closer to 0, it signifies very little change from ρ to ρ' . Conversely, if $S(\rho||\rho')$ is large, it indicates that major change in the system has occurred. A decline in $S(\rho||\rho')$ post-measurement points toward a quantum-to-classical information flow. Such measurements involve classical control signals, used to either manipulate or initialize quantum states. If a classical control steers the quantum system into a more certain (less mixed) state, this transition might represent information flow from the classical domain to the quantum one. A scenario closely related to this is quantum feedback [2,20]: a quantum system is measured, the outcome (now classical) is processed, and then a classical control signal is relayed back to influence the quantum system, suggesting a cyclical information flow: first from quantum to classical (through measurement), and then from classical back to quantum (via control).

3.6. Quantum Phenomena and Their Influence on QCI Entropy

Consider a quantum state $|\psi\rangle$ of \mathcal{Q} in a d -dimensional Hilbert space:

$$|\psi\rangle = \sum_{i=1}^d c_i |i\rangle, \quad (25)$$

where $|c_i|^2$ represents the probability of finding the system in state $|i\rangle$, where each is orthogonal to one another. In general, the entropy S , of a state is give by

$$S = - \sum_{i=1}^d |c_i|^2 \log_2 |c_i|^2, \quad (26)$$

that is, superposition's inherent uncertainty contributes to the entropy of quantum states.

For example, consider the Bell state (a canonical example of an entangled state for two qubits):

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad (27)$$

for which, entropy takes on a particularly intriguing role. The joint system, described by the Bell state for instance, exhibits zero entropy when considered as a whole. However, when considering each qubit (or subsystem) separately, the entropy is maximized. As quantum states decohere, they tend to evolve into mixed states. A pure quantum state has a well-defined entropy based on its superposition coefficients. As decoherence progresses, the off-diagonal elements of the system's density matrix decrease, leading to an increase in entropy until the system is fully decohered.

An entropy-based security framework for the QCI should establish conditions where entropy fluctuations indicate vulnerabilities. A formal theorem or statistical threshold can enable anomaly detection by flagging significant deviations from a baseline. Such thresholds would depend on the applications and materials used. Practical hybrid quantum-classical systems, including quantum computing, QKD, and quantum sensors, provide testbeds for studying entropy dynamics [21,22]. Moreover, security assessments must account for adversarial strategies like side-channel exploitation, covert entropy leaks, and decoherence injection to distinguish genuine threats from environmental noise [23,24]. Such concepts would require additional investigations for assessments and standardization.

4. Other Metrics

In our modular approach, the presented entropy-based metric could be broadened by aligning it with elements from the statistical estimation theory such as the Fisher information and the Cramér-Rao bound [25–27] leading to a higher degree of conceptual and quantitative assessment of the QCI's sensitivity to attacks or anomalies. Adding a statistical layer helps define the boundaries within which entropy or mutual information can be meaningfully detected at the QCI. By establishing thresholds for detectable entropy or mutual information, the statistical layer defines where quantum effects are distinguishable from classical contributions, clarifying the operational boundaries of the QCI.

To formally discuss parameter estimation in both classical and quantum settings, we define both the classical and quantum Fisher Information and the corresponding Cramér-Rao Bounds [27,28]. For a random variable X with probability density function $p(X|\theta)$ that depends on an unknown parameter θ , the *classical Fisher information* $\mathcal{I}(\theta)$ is defined as:

$$\mathcal{I}(\theta) := \mathbb{E} \left[\left(\frac{\partial}{\partial \theta} \ln p(X|\theta) \right)^2 \middle| \theta \right],$$

where $\ln p(X|\theta)$ is the logarithm of the likelihood function, $\frac{\partial}{\partial \theta} \ln p(X|\theta)$ is the score function, which measures the sensitivity of the likelihood to changes in θ , and $\mathbb{E}[\cdot|\theta]$ denotes the expectation taken with respect to the distribution $p(X|\theta)$. Note that $\mathcal{I}(\theta) \geq 0$ because the term is squared, Moreover, the dependency of θ ensures that $\frac{\partial}{\partial \theta} \ln p(X|\theta)$ is generally non-zero for some values of X . This ensures that $\mathcal{I}(\theta)$ is non-zero and hence well defined.

Classically, the *Cramér-Rao bound* states that for any unbiased estimator $\hat{\theta}$ of θ , the variance of $\hat{\theta}$ is bounded by the reciprocal of the Fisher information:

$$\text{Var}(\hat{\theta}) \geq \frac{1}{\mathcal{I}(\theta)},$$

which indicates that the variance of any unbiased estimator cannot be lower than $\frac{1}{\mathcal{I}(\theta)}$, setting a fundamental limit on estimation precision.

The *quantum Fisher information* $\mathcal{I}_Q(\theta)$ is defined as:

$$\mathcal{I}_Q(\theta) = \text{Tr}(\rho_\theta L_\theta^2),$$

where L_θ is the symmetric logarithmic derivative (SLD) with respect to θ . The SLD is defined implicitly by:

$$\frac{\partial \rho_\theta}{\partial \theta} = \frac{1}{2}(\rho_\theta L_\theta + L_\theta \rho_\theta),$$

where L_θ depends on the state ρ_θ and encodes the sensitivity of the quantum state to changes in θ .

Similarly, the *quantum Cramér-Rao bound* states that for any unbiased estimator $\hat{\theta}$ of the parameter θ based on measurements on the quantum state ρ_θ , the variance is bounded by the reciprocal of the quantum Fisher information:

$$\text{Var}(\hat{\theta}) \geq \frac{1}{\mathcal{I}_Q(\theta)},$$

which represents the ultimate limit on estimation precision imposed by the quantum nature of the system, and it is generally tighter (i.e., more precise) than the classical Cramér-Rao bound for measurements on the quantum state [29].

5. Criteria for QCI Security

Our objective here is to provide a perspective on using entropy changes at the QCI as a potential metric for evaluating security concerns. We use a simple definition of security, namely that the system only does what it is designed to do and nothing more. The idea of using entropic functions to quantify uncertainty allows us to more formally quantify instances in security where ‘more occurs than a given system is expected to do’. Given a quantum system \mathcal{Q} and a classical system \mathcal{C} , interfacing at the QCI, the cumulative entropy across the QCI is given by Equation (21).

The concept that any significant, unexpected change in $S(\rho_{QC})$ could potentially be an initial indication of a security breach or an anomaly is what we aim to elaborate. This concept posits that while individual changes in the entropies of \mathcal{Q} or \mathcal{C} might be expected due to the normal dynamics of each system, it is the combined entropy across the interface that serves as a reliable measure of system integrity. If a theorem can be devised as a theoretical foundation, its practical implications could prove useful.

Real-world quantum systems, when interfacing with classical components, often operate under noisy conditions. In such scenarios, distinguishing between routine entropy fluctuations and potential threats becomes crucial. The question is if it is possible, by setting a hardware agnostic threshold for acceptable entropy changes at the QCI and monitoring $S(\rho_{QC})$, to effectively identify and mitigate potential risks.

Our framework employs entropy measures to identify security criteria at QCI, aimed at spotting and quantifying vulnerabilities in information transfer processes. To initiate, the list of criteria span all possible threats one wishes to monitor for secure information protocols. QCI measures must detect the following:

1. Information leakage detection
2. Anomalies in mutual information at the QCI, indicating unintended data transfer
3. Consistency in entropic dynamics

4. Assessment of relative entropy between expected and observed values (states) reveal unexpected perturbations, suggesting possible security breaches
5. Control entropy decreases via data processing.

6. Discussions

The Quantum-Classical Interface (QCI) theory benefits from a multi-layered approach, balancing granular and comprehensive perspectives to effectively analyze system security.

A granular perspective focuses on expectation values of individual observables, enabling the identification of specific vulnerabilities. By isolating the impact on particular observables, this approach allows for precise troubleshooting, making it ideal for detecting localized disturbances and pinpointing minute vulnerabilities in the system. This approach, however, can sometimes overlook broader, holistic changes in the system that emerge from interactions across multiple observables or collective behavior. Additional complexities arise due to repeated tampering, which if occur at certain intervals might resonate with quantum dynamics, amplifying the effect on potential thresholds.

Conversely, a comprehensive perspective aims to capture the overall state integrity by examining global indicators like entropy changes. By monitoring several entropic functions, the system can encapsulate global disturbances, shifts in information flow, and the influence of substantial perturbations on the system as a whole. A large perturbation, in this context, typically implies a noticeable difference between the tampered and untampered states, informing about potential security breaches and information leakage on a macro scale. However, this broader scope may miss subtle disturbances, especially those confined to specific parts of the system.

In practical applications, a combined use of these perspectives could offer both a global overview and detailed diagnostics. By adapting the approach to fit the system's unique features and security needs, one could maintain a comprehensive understanding of overall system health through entropy measurements while also addressing specific vulnerabilities at the observable level. This combined strategy could provide a versatile and effective framework for managing the diverse security challenges within quantum-classical systems.

7. Conclusions

This position paper introduces an entropy-based framework for understanding and securing the QCI. By outlining essential security criteria and potential vulnerabilities, we aim to catalyze ongoing discussions and encourage empirical studies that will further solidify and expand QCI security strategies in emerging quantum technologies. Our work emphasizes the significant need of a QCI entropy in the broader context of quantum technology development.

Author Contributions: All authors wrote and revised the manuscript.

Funding: This research was supported by the laboratory directed research and development fund at Oak Ridge National Laboratory (ORNL).

Acknowledgments: This research was supported by the laboratory directed research and development fund at Oak Ridge National Laboratory (ORNL). ORNL is managed by UT- Battelle, LLC, for the US DOE under contract DE-AC05-00OR22725. We thank Ryan Bennink at ORNL for discussions and feedback of this initial framework.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DOAJ	Directory of open access journals
ORNL	Oak Ridge National Laboratory
QCI	Quantum-classical interface

References

1. Wiseman, H.M.; Milburn, G.J. *Quantum measurement and control*; Cambridge university press, 2009. <https://doi.org/10.1017/CBO9780511813948>.
2. Cong, S. *Control of quantum systems: theory and methods*; John Wiley & Sons, 2014. <https://doi.org/10.1002/9781118608135>.
3. Elze, H.T. Quantum-classical hybrid dynamics—A summary. *x* **2013**, *x*, *x*.
4. Elze, H.T. *x*. *x* **2013**, *442*, 012007.
5. Dammeier, L.; van Enk, S.J. *x*. *Entropy* **2023**, *25*, 602. <https://doi.org/x>.
6. Dammeier, L.; Werner, R.F. Quantum-Classical Hybrid Systems and their Quasifree Transformations. *Quantum* **2023**, *7*, 1068. <https://doi.org/10.22331/q-2023-07-26-1068>.
7. Koopman, B.O.; von Neumann, J. Dynamical systems of continuous spectra. *Proceedings of the National Academy of Sciences* **1931**, *17*, 315–318. <https://doi.org/10.1073/pnas.17.5.315>.
8. Goldsmith, A. *Wireless communications*; Cambridge university press, 2005. <https://doi.org/10.1017/CBO9780511841224>.
9. Stallings, W. *Cryptography and Network Security: Principles and Practice*, 4th ed.; Pearson, 2016. <https://doi.org/978-0135764039>.
10. Momot, F.; Bratus, S.; Hallberg, S.M.; Patterson, M.L. The Seven Turrets of Babel: A Taxonomy of LangSec Errors and How to Expunge Them. In *Proceedings of the 2016 IEEE Cybersecurity Development (SecDev)*, 2016, pp. 45–52. <https://doi.org/10.1109/SecDev.2016.019>.
11. Anderson, R.J. *Security engineering: a guide to building dependable distributed systems*; John Wiley & Sons, 2010. <https://doi.org/978-1119642787>.
12. Milburn, G. Decoherence and the conditions for the classical control of quantum systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* **2012**, *370*, 4469–4486. <https://doi.org/10.1098/rsta.2011.0487>.
13. Coffey, W.T.; Kalmykov, Y.P.; Waldron, J.T. *The Langevin equation: with applications to stochastic problems in physics, chemistry and electrical engineering*; World Scientific, 2004. <https://doi.org/doi.org/10.1142/8195>.
14. De Oliveira, M.J. Quantum Langevin equation. *Journal of Statistical Mechanics: Theory and Experiment* **2020**, *2020*, 023106. <https://doi.org/10.1088/1742-5468/ab6de2>.
15. Gardiner, C.; Zoller, P. *Quantum noise: a handbook of Markovian and non-Markovian quantum stochastic methods with applications to quantum optics*; Springer Science & Business Media, 2004. <https://doi.org/978-3540223016>.
16. Walls, D.; Milburn, G.J. Quantum Information. In *Quantum Optics*; Springer, 2008; pp. 307–346. <https://doi.org/10.1007/978-3-540-28574-8>.
17. Carmichael, H. *An open systems approach to quantum optics: lectures presented at the Université Libre de Bruxelles, October 28 to November 4, 1991*; Vol. 18, Springer Science & Business Media, 2009. <https://doi.org/doi.org/10.1007/978-3-540-47620-7>.
18. Lee, C.; Sohn, I.; Lee, W. Eavesdropping detection in BB84 quantum key distribution protocols. *IEEE Transactions on Network and Service Management* **2022**, *19*, 2689–2701. <https://doi.org/10.1109/TNSM.2022.3165202>.
19. Wilde, M. *Quantum information theory*; Vol. 1, Cambridge University Press, 2013. <https://doi.org/10.1017/CBO9781139525343>.
20. Petersen, I., Control of Quantum Systems. In *Encyclopedia of Systems and Control*; Springer London: London, 2013; pp. 1–10. https://doi.org/10.1007/978-1-4471-5102-9_147-1.
21. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum Cryptography. *Reviews of Modern Physics* **2002**, *74*, 145–195. <https://doi.org/10.1103/RevModPhys.74.145>.
22. Pirandola, S.; Andersen, U.L.; et al., E.B. Advances in Quantum Cryptography. *Advances in Optics and Photonics* **2020**, *12*, 1012–1236. <https://doi.org/10.1364/AOP.361502>.
23. Xu, F.; Qi, B.; Lo, H.K. Experimental Demonstration of Phase-Remapping Attack in a Practical Quantum Key Distribution System. *New Journal of Physics* **2020**, *12*, 113026. <https://doi.org/10.1088/1367-2630/12/11/113026>.
24. Lo, H.K.; Curty, M.; Tamaki, K. Secure Quantum Key Distribution. *Nature Photonics* **2014**, *8*, 595–604. <https://doi.org/10.1038/nphoton.2014.149>.
25. Steven, M.K. *Fundamentals of Statistical Signal Processing, Volume 1: Estimation Theory*. PTR Prentice-Hall, Englewood Cliffs, NJ **1993**, *10*, 148. <https://doi.org/9780134878409>.
26. Song, Z.; Chen, Y.; Sastry, C.R.; Tas, N.C. *Optimal observation for cyber-physical systems: a fisher-information-matrix-based approach*; Springer Science & Business Media, 2009. <https://doi.org/10.1007/978-1-84882-656-4>.

27. Hall, M.J. Quantum properties of classical Fisher information. *Physical Review A* **2000**, *62*, 012107. <https://doi.org/10.1103/PhysRevA.62.012107>.
28. Petz, D.; Ghinea, C. Introduction to quantum Fisher information. In *Quantum probability and related topics*; World Scientific, 2011; pp. 261–281. https://doi.org/10.1142/9789814338745_0015.
29. Paris, M.G. Quantum estimation for quantum technology. *International Journal of Quantum Information* **2009**, *7*, 125–137. <https://doi.org/10.1142/S0219749909004839>.

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.