Coin.fi Research Team: Arvin Bhangu, Dylan Kawalec

Title:
A Theoretical and Philosophical Recasting of a Global-Sensitivity Quantum One-Time Pad System

Abstract:
We propose a revised theoretical framework for a quantum-based key generation and encryption system—analogous to a Quantum One-Time Pad (QOTP)—that departs from conventional notions of localized eavesdropping detection. In traditional QKD and QOTP architectures, the security often hinges on detecting disturbances introduced by adversaries through local quantum measurements. Here, we eliminate any reliance on localized detection and instead propose a radically holistic, philosophically grounded model. This model assumes that even infinitesimal changes, whether introduced deliberately by an adversary or passively by the natural progression of time, reconfigure the entire quantum-mechanical representation. Through a carefully constructed manifold encoding of information, arranged on a continuum with non-orientable topologies such as a Möbius strip, any microscopic perturbation induces a global transformation of the state's Hamiltonian. This results in a situation where no incremental information leakage is possible and where stable partial knowledge cannot be accumulated over time. The philosophical underpinnings of this approach challenge classical notions of information locality and propose a worldview in which information security is enforced by the very structure of temporal and quantum reality itself.

This theoretical and philosophical reimagining of QOTP security owes conceptual inspiration to established principles of quantum randomness, nonlocality, and the philosophical debates surrounding time and information in quantum theory.

This construction leads to a QOTP scenario offering theoretically perfect secrecy without traditional error-rate-based intrusion detection. Instead, the mere nature of time and quantum non-locality enforces security.

Abstract

We present a quantum-based cryptographic key generation and encryption scheme analogous to a Quantum One-Time Pad (QOTP). Unlike previous approaches that rely on detecting eavesdropping through localized state disturbances or error rates, our approach rests on a global sensitivity principle. Here, the encoding of information into a random manifold and its holographic projections forms a structure so fragile and interdependent that any infinitesimal change—whether introduced by an adversary, caused by quantum uncertainty, or simply arising from the natural

progression of time—results in a complete transformation of the underlying Hamiltonian that defines the system's ground state.

This radical sensitivity implies that there is no stable partial information leakage. Any attempt to gain even a single bit of information without complete knowledge instantly collapses the entire configuration into a new global state, effectively nullifying any incremental approach to compromise the key. We describe axioms that capture this sensitivity principle, lemmas that characterize the uniform unpredictability and global interdependence, and finally a proof demonstrating that the resulting system ensures absolute secrecy and unpredictability of the derived key.

Conceptual Overview

In standard quantum key distribution (QKD) and QOTP approaches, security often hinges on detecting eavesdropping through error rates or state disturbances. In our new system, we remove the explicit concept of "detection" and replace it with a principle of radical global reconfiguration. The key is represented in a quantum manifold's holographic encoding. This manifold is constructed so that the distribution of information across a set of "information continua" is not only non-local but also hypersensitive to any micro-level interaction, including the mere passage of time used as a reference by a Turing machine implementing the protocol.

1. Introduction and Conceptual Foundations

In standard quantum cryptographic protocols, including quantum key distribution (QKD) and its integration into one-time pad schemes, the underlying premise is that eavesdroppers can be detected through specific, localized state anomalies. This detection frequently involves monitoring error rates or subtle state disturbances. Our new theoretical construction diverges fundamentally from that tradition. Instead, we posit that the information is embedded within a quantum manifold whose topology and metric properties are so globally sensitive that no partial measurement or incremental intrusion yields stable information. The philosophical implication here is that the act of observing or even passively waiting while referencing a computational clock inherently and holistically reshapes the manifold's form.

We begin by encoding information into a quantum manifold, denoted by the symbol $\mathcal{M}(t)$, where t represents an absolute time parameter referenced by a Turing machine that implements the protocol. The manifold $\mathcal{M}(t)$ is generated from quantum-random processes, ensuring that each instance in time corresponds to a distinct measure $\mu_t(\mathcal{M})$. The encoded quantum state can be represented as $|\psi\rangle = \Psi(\mathcal{M}(t))$, with $\Psi : \mathcal{M}(t) \to \mathcal{H}$ mapping the manifold's configuration to a state in the Hilbert space $\mathcal{H}$.

Philosophically, this setup abandons the notion that time is a neutral parameter upon which information states can be stably defined. Instead, time itself—represented discretely as increments Δt—becomes a fundamental driver of configuration change. Any temporal progression, $\mathcal{M}(t) \to \mathcal{M}(t + \Delta t)$, modifies not merely the state's phase or a subset of its qubits, but rather induces a wholly new encoding with a transformed Hamiltonian. We write this schematically as

$$H(\mathcal{M}(t)) \xrightarrow{\Delta t} H'(\mathcal{M}(t + \Delta t)),$$

indicating that no continuous, incremental relation exists between the old and new Hamiltonians. From a metaphysical standpoint, this breaks with classical assumptions of continuity and gradualism in knowledge acquisition.

---

2. Axiomatic Assumptions and Nonlocal Topology

We now formalize the central assumptions of this model. The first key axiom is that no stable partial states exist. More formally, there is no local measurement that can yield an incrementally informative outcome without triggering a redefinition of the entire state. Writing this as an axiom:

Axiom 1 (No Stable Partial States): For any given initial state $|\psi\rangle$, any minimal interaction—be it a localized measurement or a mere increment in time Δt—transforms the system into $|\psi'(\Delta t)\rangle$, with the crucial property that $\langle\psi|\psi'(\Delta t)\rangle \approx 0$.

This implies that even a minimal intervention collapses any hypothetical continuity of information. Such global sensitivity can be realized by embedding the information holographically on a continuum with a Möbius-like topology. This topological complexity ensures that changes cannot remain local. Instead, any perturbation reconfigures the entire boundary condition that defines the holographic encoding.

Axiom 2 (Global Hamiltonian Reset): We assume that each microchange alters the Hamiltonian drastically, eliminating any possibility of slowly "probing" the structure. If $H(\mathcal{M}(t))$ defines the system at time t, then after a microscopic change we have a new Hamiltonian $H'(\mathcal{M}(t + \Delta t))$ unrelated in a simple manner to the original. Symbolically:

$$H(\mathcal{M}(t)) \xrightarrow{\text{min. perturbation}} H'(\mathcal{M}(t + \Delta t)).$$

Furthermore, the entropy seed used to generate $\mathcal{M}(t)$ is time-dependent, ensuring that any temporal increment leads to a distribution $\mu_{t+\Delta t}(\mathcal{M})$ uncorrelated with $\mu_t(\mathcal{M})$. This reflects a deeply nonlocal and time-sensitive structure that, in philosophical terms, blends the epistemology of observation with the ontology of time-dependent quantum states.

---

3. Philosophical Implications of Temporal Entropy and Non-Determinism

From a philosophical viewpoint, this approach challenges the classical

notion that one can "wait and see" or "probe gradually." Instead, waiting Δt does not preserve the original problem state; it generates a new one. Any adversary attempting to glean partial information is confronted by a paradox: the very act of attempting to understand the system incrementally, or even to let time pass while contemplating it, reconfigures the system into a fundamentally new scenario.

Since no stable incremental approach is possible, we find that guessing the final state $|\phi\rangle$ at a given time t reduces to a uniform probability over a vast configuration space $\mathcal{S}$. The probability of success for an adversary without full knowledge thus remains at best $1/|\mathcal{S}|$, akin to picking a random state. Mathematically, we write:

$$\Pr(\text{Adversary predicts } |\phi\rangle) \leq 1/|\mathcal{S}|.$$

This result emerges from the principle that any attempt to break down the complexity via partial measurements fails due to the global and instantaneous reconfiguration property.

---

4. Lemmas Supporting Global Sensitivity and Witness Verification

We now state key lemmas that undergird this construction. First, consider the uniform unpredictability lemma:

Lemma 1 (Uniform Unpredictability): Given the axioms of global reset and time-dependent entropy, the final state $|\phi\rangle$ at time t is uniformly unpredictable by any adversary lacking complete initial knowledge.

This lemma is supported by the impossibility of incremental inference. Next, we consider the lemma of global sensitivity:

Lemma 2 (Global Sensitivity to Single Changes): Any single perturbation, including the natural flow of time Δt, induces a near-complete orthogonal transformation of the manifold's encoding. Thus, no sequence of small steps can aggregate partial information without losing the relevance of previously gained data.

Now, consider the verification lemma:

Lemma 3 (Stability of the Witness Condition): The legitimate parties pre-agree on a known deterministic witness condition, often expressed as verifying that $\langle\phi|H_{\text{ref}}|\phi\rangle \leq E_0 + \varepsilon$. In the absence of unauthorized perturbations, $|\phi\rangle$ meets this witness condition. Any unauthorized attempt to observe, measure, or even stall time in an uncontrolled manner will yield a radically different Hamiltonian and hence a failure in the witness test.

---

5. Theoretical and Philosophical Proof of Security

The security of the proposed QOTP-like scheme follows directly from these lemmas and axioms. Any adversary $\mathcal{E}$ aiming to extract a partial key incrementally faces the problem that minor perturbations, including waiting for the next time step, rewrite the state and its Hamiltonian. Because no incremental advantage can be gained, and since the witness verification at the predetermined time ensures a consistent final key for the legit-

imate parties, the adversary's best strategy is reduced to guessing blindly within an immense configuration space.

Formally, if the legitimate receiver obtains a final state $|\phi\rangle$ and checks $\langle\phi|H_{\text{ref}}|\phi\rangle$, they either confirm integrity or detect a departure from the expected ground state energy range. If a departure is found, they simply regenerate the key at a new time $t + \Delta t$, ensuring that adversaries gain no incremental foothold.

This proof relies on a philosophical acceptance that "time waiting" or "small changes" do not preserve partial knowledge. Instead, each attempt to approach the system leads to a holistic and unpredictable metamorphosis of the total quantum scenario. In this sense, the security is woven into the fabric of temporal and spatial quantum structure: knowledge cannot be extracted fragment by fragment, and thus no adversary can break the system down into simpler components.

---

6. Philosophical Reflections

The theoretical framework presented here radically shifts the emphasis from local detection methods to a global and holistic principle of security. By designing a QOTP-like system in which every microscopic change, including the natural progression of time, induces a wholly new Hamiltonian and hence a new global configuration, we ensure that incremental or partial attacks are futile. This approach not only achieves a form of absolute security but also resonates with philosophical themes in quantum mechanics: it suggests that the informational content of a quantum world may be intrinsically nonlocal, non-incremental, and deeply interwoven with the temporal dimension.

Such a system extends the domain of cryptographic thought into the philosophical realm, encouraging us to reconsider the assumptions of stability, continuity, and local accessibility of information. In doing so, it highlights the potential of quantum theory to reshape fundamental concepts of secrecy and knowledge, offering a security model grounded in the impossibility of stable partial measurement and the inexorable influence of time itself.

Key Features:

1. **Random Manifolds as Information Continua:**
   The key is stored as a holographic encoding across multiple strata of a randomly generated quantum manifold. Unlike linear sequences of qubits, these manifolds create a global "continuum" of information where no local region is independent.

2. **Mobius-Loop or Cyclic-Array Structure:**
   The information continuum is arranged in a topologically complex manner (e.g., a Möbius strip or other non-orientable structure). Any change at any point in this structure—spatially or temporally—alters the entire manifold's global topological and metric properties.

3. **Global Hamiltonian Redefinition Under Minimal Changes:**
   A single quantum interaction, a minor change in an input variable, or even the natural progression of time leads to a complete recalculation of the global Hamiltonian describing the state. This ensures that the ground state and all eigenstates rearrange fundamentally, preventing stable partial extraction of information.

4. **Absolute Temporal Sensitivity:**
   The system's reference clock (embodied by a Turing machine) ensures that even a minute time step results in a redefinition of the manifold's encoding. Thus, no observer can "hold" the system static to glean stable partial knowledge; every moment in time yields a distinct global state.

5. **Deterministic Witness in Interaction Ceremony:**
   The final stage of deriving a key involves interpreting the holographic continuum against a known deterministic witness condition. This witness is a specific low-energy eigenstate under the current Hamiltonian. Any attempt (successful or not) to gain partial information changes the Hamiltonian so drastically that the final witness test produces a fundamentally different result, ensuring no incremental advantage to an adversary.

Axioms

Axiom 1 (No Stable Partial States):
For any given encoding $|\psi\rangle$ derived from the manifold $\mathcal{M}$, there exists no local measurement or partial observation that yields stable or incremental information. Formally, any attempt to interact with a subset of the manifold's degrees of freedom, or the mere lapse of a discrete time step Δt, induces a global transformation:

$$|\psi\rangle \xrightarrow{\text{min. change}} |\psi'(\Delta t)\rangle$$

where $|\psi'(\Delta t)\rangle$ is not isomorphic or partially related in a simple way to $|\psi\rangle$.

Axiom 2 (Global Hamiltonian Reset):
The manifold's encoding is defined by a Hamiltonian $H(\mathcal{M}, t)$ that depends on the manifold $\mathcal{M}$ and the global clock time t. Any change in time, or in any microscopic parameter of $\mathcal{M}$, results in:

$$H(\mathcal{M}, t) \xrightarrow{\text{min. perturbation}} H'(\mathcal{M}, t + \Delta t)$$

with $\langle\psi|H(\mathcal{M}, t)|\psi\rangle$ and $\langle\psi'|H'(\mathcal{M}, t + \Delta t)|\psi'\rangle$ having no simple or continuous relationship, ensuring no gradual approach to deciphering $|\psi\rangle$.

Axiom 3 (Topological Nonlocality):
Information is encoded holographically on a continuum arranged in a cyclic or Möbius-like topology. Because of this topological complexity, a single perturbation affects the global boundary conditions, causing a near-complete redistribution of quantum states:

$$\Psi : \mathcal{M} \to \mathcal{H}, \quad \text{is highly nonlocal.}$$

No localized action or partial measurement reveals a stable subset of information.

Axiom 4 (Temporal Entropy Sensitivity):
The entropy seed used for non-determinism is time-dependent. Any increment in time Δt alters the entropy source used to seed the manifold's configuration. Thus, each time step changes the holographic projection:

$$\mathcal{M}(t + \Delta t) \sim \mu_{t+\Delta t}(\mathcal{M})$$

with no overlap in distribution from $\mu_t(\mathcal{M})$.

Axiom 5 (Deterministic Witness Condition):
A known reference Hamiltonian form H_{ref} defines a witness condition. If $|\phi\rangle$ is the intended final state, verifying $\langle\phi|H_{\text{ref}}|\phi\rangle \leq E_0 + \varepsilon$ confirms integrity. Due to Axiom 2, any perturbation (including eavesdropping attempts) changes the Hamiltonian drastically, ensuring that $|\phi\rangle$ no longer satisfies this condition in the same manner.

Lemmas

Lemma 1 (Uniform Unpredictability):
Given the global reset axiom (Axiom 2) and temporal sensitivity (Axiom 4), the final state $|\phi\rangle$ at time t is uniformly unpredictable from the perspective of any adversary who does not know all initial conditions and who cannot maintain a static frame of reference. The probability of correctly guessing $|\phi\rangle$ or any partial feature of it is at best random, akin to uniform distribution over a large state set $\mathcal{S}$.

Proof Sketch:
Because each time step or minor perturbation yields a completely new Hamiltonian with no simple relation to the previous one, no adversary can track or approximate states incrementally. The unpredictability follows from the absence of stable partial information.

Lemma 2 (Global Sensitivity to Single Changes):
Any single change in position, input variable, or the natural progression of time, causes a near-complete change in the global manifold encoding. Formally:

$$|\psi\rangle \xrightarrow{\Delta x, \Delta t} |\psi''\rangle$$

with $\langle \psi'' | \psi \rangle \approx 0$. Thus, an adversary cannot benefit from a series of small measurements or time delays to gradually glean information.

Proof Sketch:
From Axiom 1 and Axiom 3, local actions have global effects. The nonlocal topology ensures any tiny action disrupts the entire encoded structure. Combined with temporal entropy changes (Axiom 4), even letting time pass changes the reference frame entirely.

Lemma 3 (Stable Key Extraction via Witness):
Despite the radical sensitivity, Alice and Bob can pre-agree on a deterministic witness condition associated with a reference Hamiltonian H_{ref}. If $|\phi\rangle$ meets the witness condition, it ensures that no unknown perturbation occurred in a way that yields partial adversarial information.

Proof Sketch:
Because any unknown perturbation would redefine the Hamiltonian drastically (Axiom 2 and 5), the intended witness test at a known time t and known configuration $\mathcal{M}(t)$ is either passed (no unauthorized perturbation changed the structure) or produces a drastically different signature (indicating a null result or failure, prompting regeneration of the key).

Equations and Conditions

1. **Time-Dependent Manifold Selection:**

$$\mathcal{M}(t) \sim \mu_t(\mathcal{M}) \implies |\psi\rangle = \Psi(\mathcal{M}(t))$$

   Each increment Δt induces $\mathcal{M}(t + \Delta t)$ and thus a new map Ψ.

2. **Global Hamiltonian Transformation:**

$$H(\mathcal{M}(t)) \xrightarrow{\Delta t, \Delta x} H'(\mathcal{M}(t + \Delta t))$$

   No incremental relation exists:

$$|\langle \psi | \psi' \rangle| \approx 0 \quad \text{for minimal perturbations.}$$

3. **Witness Condition:**

$$\langle \phi | H_{\text{ref}} | \phi \rangle \leq E_0 + \varepsilon \implies \text{Integrity guaranteed.}$$

   Any perturbation yields no such simple inequality, as $|\phi\rangle$ and H_{ref} relationship collapses.

Main Theorem : Security of the Rosario QOTP

Statement:
Under the given axioms, lemmas, and the introduced global sensitivity principle, the key extracted from the holographic manifold is secure. Any attempt by an adversary $\mathcal{E}$ to gain partial information, even infinitesimal, or any reliance on waiting for time changes without authorization, causes a complete redefinition of the global state and Hamiltonian, destroying any partial advantage and invalidating incremental attacks.

Proof:

1. **No Incremental Information Gain:**
   By Lemma 2 and Axiom 1, no partial measurement or small delay can yield stable partial knowledge. Each interaction resets the system's complexity, making previously gained partial "clues" obsolete.

2. **Uniform Unpredictability:**
   Lemma 1 states unpredictability under dynamic and global state changes. With no incremental approach possible, guessing the final key is at best a uniform random guess over an exponentially large configuration space.

3. **Deterministic Witness for Integrity:**
   Lemma 3 and Axiom 5 ensure that at the predetermined time and configuration, the legitimate parties verify the witness condition. Any deviation caused by adversarial tampering leads to a fundamentally different Hamiltonian reference check result. This ensures that the legitimate parties either obtain a pristine key or are alerted to regenerate one.

4. **Summary:**
   Because no partial or incremental approach works and any attempt to learn even one bit triggers a global change, the adversary gains no advantage. The final key emerges only in a controlled final step that checks the witness condition. Thus, the QOTP key is secure and unpredictably random, granting absolute secrecy.

Summary

In this Rosario QOTP framework:

- We have replaced the notion of detecting eavesdropping via local variance in quantum states with a far stronger condition: any microscopic change (measurement, waiting, perturbation) triggers a wholesale reconfiguration of the entire quantum system.

- Axioms ensure radical global sensitivity, temporal dependence of entropy, and topological nonlocality.
- Lemmas capture unpredictability, the impossibility of incremental information gain, and the role of a deterministic witness in ensuring final integrity.
- The final proof confirms that the key generated this way is secure against any adversary, since no stable partial information extraction is feasible.