Quantum One-Time Pad (QOTP): A Detailed Explanation

The Quantum One-Time Pad (QOTP) is a cryptographic scheme that integrates the principles of quantum mechanics with the classical concept of the one-time pad (OTP). The classical OTP, considered information-theoretically secure, relies on a shared secret key of random bits that is as long as the message itself. When the key is perfectly random, never reused, and kept secret, it provides absolute security—an eavesdropper gains no information about the original message.

However, one major challenge in classical OTP systems is the secure distribution of the random key. If we must send the key over a channel that could be intercepted, we risk its secrecy. Traditionally, this key distribution problem severely limits OTP's practicality. Quantum cryptography, in particular quantum key distribution (QKD), solves this problem by leveraging the laws of quantum mechanics to generate and distribute keys securely. QKD assures that if an eavesdropper tries to intercept the key in transmission, their presence will be detected.

The combination of QKD and OTP leads to the Quantum One-Time Pad, often referred to in general terms as "quantum-based key distribution followed by classical one-time pad encryption." While not always called "QOTP" by name, the concept is that you use a quantum channel to establish a perfectly random, tamper-evident key, and then use that key in a one-time pad encryption of the classical data. The resulting system offers unbreakable encryption, both in theory and in practice, assuming the integrity of the quantum transmission and the secure storage of the resulting key.

Process of Establishing and Using a QOTP:

1. **Quantum Key Distribution (QKD) Setup**:

   - **Preparation of Quantum States**: Alice (the sender) encodes a sequence of random bits (0s and 1s) into quantum states of photons. Each bit can be represented by the polarization of a single photon. Two common polarization schemes are:
     - **Rectilinear basis (+)**: Vertical ($\updownarrow$) to represent a 1 and horizontal ($\leftrightarrow$) to represent a 0.
     - **Diagonal basis ($\times$)**: Diagonal polarization (e.g., $\nearrow$) to represent a 1 and the opposite diagonal (e.g., $\searrow$) to represent a 0.

   Alice chooses for each bit which basis to use (rectilinear or diagonal) at random. Thus, each photon sent encodes a single bit in one of the two possible polarization bases, but Alice doesn't announce which basis she used yet.

2. **Transmission Over a Quantum Channel**:

- Alice sends these photons down a quantum channel (an optical fiber or free-space link) to Bob (the receiver).
- During this transmission, if an eavesdropper (Eve) tries to measure the photons, she will inevitably disturb their quantum states due to the no-cloning theorem and the principle of measurement in quantum mechanics. Any attempt at interception will leave detectable traces (errors in Bob's measurements).

3. **Measurement by the Receiver**:

   - Bob has two detectors, one for each basis (one for + and one for $\times$). For each incoming photon, Bob randomly chooses which detector to use without knowing which basis Alice originally chose.
   - If Bob chooses the same basis that Alice used, he will measure the correct bit with high probability. If he chooses the wrong basis, he risks obtaining a random and potentially incorrect value.

4. **Public Discussion for Basis Reconciliation**:

   - After sending a large number of photons, Alice announces over a classical, insecure channel which basis she used for each photon, but not the resulting bit value.
   - Bob then reveals which basis he *guessed* for each photon.
   - They discard all the measurements where Bob used the wrong basis, because in those cases he cannot be certain of having the correct bit.
   - The remaining subset of their results, where Bob's measurement basis matched Alice's preparation basis, will form a shared, random sequence of bits. This sequence is their secret key.

5. **Error Checking and Privacy Amplification**:

   - Alice and Bob sacrifice a few bits of their key at random for testing. They compare these test bits over the public channel.
   - If the test bits match perfectly (or show only an expected level of error due to noise), they assume no eavesdropping took place.
   - If the error rate is suspiciously high, they discard the entire key and start again, because this indicates potential interception by Eve.
   - If the key is confirmed to be secure, it can be shortened (privacy amplification) and used as a true one-time pad key.

6. **Classical One-Time Pad Encryption**:

- Once Alice and Bob share this verified, random key, Alice can take her plaintext message and XOR it bit-by-bit with the key to produce ciphertext.
- Bob, having the same key, can decrypt by XORing the ciphertext with the identical key, retrieving the original message perfectly.

Because the key is truly random, known only to Alice and Bob, never reused, and cannot be intercepted without detection, the encryption is absolutely secure against any computational attack.

Non-Deterministic States (Superposition and Measurement Uncertainty):

A central concept in quantum mechanics—and a key reason why quantum cryptography is secure—is the non-deterministic nature of quantum states. When a quantum system is not observed, it can exist in a superposition of all possible states simultaneously, and measurement forces it into a single, definite state.

- **Example of a Non-Deterministic (Superposition) State**:
  Consider a single photon that must pass through one of two slits (as in the famous double-slit experiment). If we do not measure which slit it goes through, the photon can be described not as choosing left slit or right slit deterministically, but as existing in a *superposition* of going through both slits at once. This superposition persists until a measurement (an interaction that extracts information about which path the photon took) is made.

  Another common example is the polarization of a photon. Suppose a photon's polarization is aligned vertically ($\updownarrow$). If we measure it using a detector aligned in the same vertical/horizontal basis, we get a deterministic result: vertical polarization. But if we measure it in a diagonal basis ($\times$), the outcome is probabilistic. Before measurement, the photon's polarization can be considered a superposition of two diagonal states: $\nearrow$ and $\searrow$. Each measurement yields one of these outcomes at random, and the act of measuring forces the photon into one diagonal state or the other. Thus, before measurement, the photon is non-deterministically "both $\nearrow$ and $\searrow$" in the quantum sense—though this is an abstract notion and not a classical one.

- **Why Non-Determinism Ensures Security**:
  This fundamental unpredictability means that an eavesdropper cannot reliably obtain full information about the transmitted photons without disturbing them and alerting Alice and Bob. Trying to measure a photon in the "wrong" basis yields a random, non-deterministic outcome that corrupts the original encoding. Quantum theory inherently prevents Eve from extracting the full bit value without introducing detectable errors.

The Quantum One-Time Pad (QOTP) is a method for using quantum mechanics to overcome the traditional key distribution problem, thereby enabling truly secure encryption. Its security rests on the non-deterministic, superposed nature of quantum states, which ensures that any attempt at eavesdropping is both unsuccessful and detectable.

For our QOTP we integrate random manifolds, holographic representations, Markovian "Las Vegas" circuits, static Hamiltonian states, and human interpretation—into a variant of a Quantum One-Time Pad (QOTP) framework.

Conceptual Overview

Traditionally, a QOTP relies on securely generated quantum keys—distributed, for instance, via quantum key distribution—to achieve absolute secrecy. In the standard approach, photons or qubits are prepared in certain bases, transmitted, measured, and refined into a secret key. Now imagine a far more elaborate scenario, one in which the key itself and the process of verifying it are not simply linear sequences of qubits, but are embedded in a rich and evolving mathematical structure: a random manifold that encodes multiple "information continuums" as a holographic data representation.

In this variation, the QOTP key generation and verification is transformed into a procedure that leverages:

1. **Random Manifolds as Information Substrates**
2. **Holographic Encodings of Multiple Data Streams**
3. **Markovian Las Vegas–Style Quantum Circuits for Non-Deterministic Evolution**
4. **Human Interpretation of Manifold Evolutions to Derive Witness States**
5. **Static Hamiltonian Challenges as Verification Steps**

The goal is the same as in a traditional QOTP: to produce a random, secret key that can be used to encrypt a message securely. But now the environment for generating and verifying that key is an intrinsically complex quantum–geometric structure that ensures non-determinism and unpredictability at a fundamental level.

---

1. Random Manifold with Multiple Information Continua

Instead of distributing qubits directly, Alice begins by generating a high-dimensional quantum manifold—a sort of quantum geometric space—whose curvature and topology are defined by random parameters. These parameters are chosen via a quantum-random process, possibly involving

vacuum fluctuations or other quantum entropy sources, ensuring they cannot be predicted by any adversary.

Within this manifold, information is not stored as simple bit strings or qubit sequences. Instead, it is dispersed across multiple "information continua" represented as overlapping holographic projections. Think of these continua as different layers or strata of encoded data, each accessible only via a particular set of quantum measurements.

- **Holographic Encoding:**
  The manifold itself can be thought of as a bulk geometric entity, while the key's information is encoded holographically on a boundary surface. Observers can retrieve information about the interior states by examining the boundary hologram, but doing so without the correct "projection basis" yields meaningless or scrambled results—akin to mismatching polarization bases in standard QKD.

- **Unique Entropy Sources:**
  Each layer of the hologram incorporates entropy drawn from fundamentally quantum processes—spontaneous parametric down-conversion, zero-point energy measurements, or even Bell-basis measurements of entangled pairs. This ensures a profound level of unpredictability in the final structure, mirroring the unpredictability needed in a one-time pad key.

---

2. Distribution Via a Markov "Las Vegas" Quantum Circuit

Once this manifold is prepared, a special type of quantum circuit—a "Markov Las Vegas" circuit—is used to "walk" through the manifold's topological features. A Las Vegas algorithm in classical computing always returns a correct result if it returns one, and never returns a wrong solution; it may just take an uncertain amount of time. Translating this idea into a quantum setting, the "Markov Las Vegas" circuit is a quantum walk over the manifold's state-space:

- **Markovian Non-Determinism:**
  The circuit's evolution depends on stochastic transitions between manifold regions. These transitions are governed by quantum Markov processes, ensuring memoryless, probabilistic state changes. Because these changes are tied to the manifold's random geometry, each "step" of the circuit leads to a non-deterministic partial collapse of possibilities into certain holographic encodings.

- **Maintaining Integrity & Privacy:**
  If an adversary tries to probe the manifold at any point, they induce detectable distortions in the hologram's interference patterns. Just as eavesdropping on photons in QKD introduces detectable errors, tampering with the manifold or its Markovian transitions creates

anomalies in the boundary hologram that Alice and Bob can later detect.

---

3. Evolving Manifold Projection and Human Interpretation

As the Markov Las Vegas circuit iterates, it "scrambles" and "unscrambles" patterns on the holographic boundary. After a sufficient number of iterations, Alice "freezes" the manifold in a particular configuration. This configuration is not a simple list of qubits, but a geometric-holographic pattern. The complexity and non-determinism come from the random walk on the manifold, ensuring that the resulting pattern is unpredictable.

- **Human Interpretation Step:**
  While quantum devices can measure states, a crucial twist in this protocol is that a human cryptanalyst (on the receiving end—Bob's side) must interpret the final manifold configuration. The human looks at the final holographic pattern—imagine a highly abstract visualization, possibly aided by classical computation—and attempts to "decompose" it into a simpler representation. In other words, the human (or a trusted classical algorithm they control) must choose the correct measurement basis or decoding key suggested by the known "construction rules" shared between Alice and Bob.

- **Witness as a Static Hamiltonian State:**
  The final step of verification involves considering the manifold's encoding as a static Hamiltonian problem. The hologram can be mapped to a Hamiltonian whose ground state or particular eigenstate serves as a "witness" that the protocol's evolution was correct and untampered. Finding this witness state is akin to solving a complex but tractable quantum puzzle.

The "challenge" is to confirm that the measured manifold configuration corresponds to the expected static Hamiltonian solution. If Alice and Bob share a known reference model of the Hamiltonian (determined at the outset of the protocol), Bob's human interpreter tries to solve this Hamiltonian or at least verify that the sampled configuration of the hologram corresponds to a low-energy eigenstate.

---

4. Ensuring a Secure Key Extraction

If the witness state checks out—meaning the final configuration aligns with the predetermined Hamiltonian's expected solution—Bob is assured that no adversary has distorted the manifold's evolution. Now the interpreted pattern can be simplified into a cryptographic key. Because of all the intermediate steps—random manifold generation, holographic dispersion, Markov Las Vegas transitions, non-deterministic measurement, and Hamiltonian verification—the final key is as random and unpredictable as in a QOTP, but now embedded in a much richer structure.

- **Non-Deterministic Evolution Guarantees Security:**
  Any attempt by an adversary to intercept or measure the manifold states prematurely collapses certain holographic projections and changes the Hamiltonian solution space. Because this final solution acts as a delicate global witness, the slightest tampering reveals itself as discrepancies in the eigenvalue measurements or correlation patterns.
- **From Complex Pattern to Key:**
  After verification, Bob and Alice agree on a method to extract a final binary key sequence from the confirmed holographic manifold pattern. This key is then used in a one-time pad encryption of messages, just as in a standard QOTP, ensuring absolute secrecy.

In Summary

This variation of a QOTP replaces the straightforward photon-based QKD and linear OTP combination with:

- A **randomly generated manifold** as a geometric "platform" for quantum information.
- A **holographic encoding** of multiple data streams layered within that manifold.
- A **Markov Las Vegas circuit** that randomly evolves the manifold's projections, ensuring inherent non-determinism.
- A **human interpretation step** that decodes the hologram into a static Hamiltonian problem and finds a "witness state," ensuring no tampering occurred.
- The resulting confirmed pattern serves as a highly complex, completely unpredictable key, ready to be used as a one-time pad, mirroring the absolute security of QOTP but through a fantastically more intricate and exotic construction.

We produces a random secret key with properties analogous to a classical one-time pad (OTP), but ensured through quantum principles. Here is how it implements a form of Quantum One-Time Pad (QOTP):

1. **Quantum Origin of Randomness:**
   Traditional QOTP hinges on the idea that the key must be perfectly random and secret. In this new system, the key's randomness comes from the inherently quantum processes used to create a complex manifold and encode information holographically. Quantum effects ensure that any measurement or interaction by an eavesdropper introduces disturbances, thereby guaranteeing that the key remains private and that tampering is detectable.

2. **Non-Deterministic Manifold Generation:**
   Instead of distributing simple qubits (as in standard QKD/QOTP scenarios), the system constructs a quantum manifold whose geometry and topological features are defined by quantum-random parameters. This manifold acts as a higher-dimensional "container" of quantum information. Because it is formed via quantum processes—such as superposition and entanglement—the manifold itself is imbued with the same unpredictability and fragility (sensitivity to observation) that standard QKD relies on.

3. **Holographic Encoding as Quantum Key Distribution:**
   In classical QOTP, the key must be shared secretly between two parties. In standard quantum key distribution, photons are sent directly and measured. In this new approach, the "key" is never just a direct bitstream. Instead, it is represented as a pattern etched into a holographic boundary of the manifold.

   Accessing this holographic information is akin to receiving qubits in a QKD protocol: you must measure it correctly. Misaligned measurements or unapproved attempts to read the hologram scramble the extracted data, resulting in detectable errors. Thus, the holographic representation serves the same function as quantum signals in normal QKD: it allows secure key establishment.

4. **Markov "Las Vegas" Circuit as a Randomizing Process:**
   The key is not simply generated and handed over. It emerges from a stochastic quantum process—a Markovian "Las Vegas" circuit—that evolves the manifold state. This circuit provides a layer of quantum-driven randomness and non-determinism, ensuring the final key pattern cannot be predicted by an adversary.

   Just as in QKD, where random bases are chosen to encrypt bits, this circuit enacts random transitions that guarantee no outsider can deduce the final encoded key. Any unauthorized attempt at observing intermediate states collapses superpositions and changes the manifold's final structure, producing easily detectable anomalies.

5. **Verification via a Static Hamiltonian Witness:**
   In QKD, after the quantum exchange, the parties verify that no eavesdropping has occurred by comparing subsets of data and checking error rates. In this manifold-based system, verification happens by interpreting the final manifold-hologram configuration as a static Hamiltonian problem. By solving or verifying this Hamiltonian's expected solution—akin to checking for "no anomalies"—the legitimate parties confirm that the key has not been tampered with.

   This verification step replaces the classical error-checking in QKD, but serves the same purpose: to ensure that the final shared data (the key) has not been compromised. Any discrepancy signals the

presence of an eavesdropper, prompting the parties to discard the generated key.

6. **Extraction of a One-Time Pad Key:**
   Once the legitimacy of the final configuration is assured, the complex holographic data is distilled into a classical binary string—a sequence of random bits. This sequence is as unpredictable and fresh as the key generated by traditional QKD methods. Because the key emerges from a fully quantum-driven, tamper-evident process, it inherits the perfect secrecy property of a one-time pad when used to encrypt data.

   Just like in a standard QOTP, this final key is never reused. It encrypts a single message once, guaranteeing information-theoretic security. The quantum origin and holographic complexity ensure that no adversary could have gained useful information about it.

In essence:

- The manifold and holographic encoding take the place of directly transmitted quantum states.
- The Markov Las Vegas circuit and human verification step replace the simpler protocols of measuring photon polarizations and discussing measurement bases.
- The final step yields a random, secret key confirmed to be untampered by quantum means.

This process still accomplishes the fundamental goal of QOTP: producing a secure, random key via quantum methods that cannot be intercepted without detection, ensuring that when used as a one-time pad, the encryption is absolutely secure.

The Proofs

these detailed proofs use the given axioms and the stated lemmas to rigorously show that the custom QOTP is secure against any adversary. The key point is that any attempt to gain information induces changes detectable through the Hamiltonian witness or through statistical deviations in measurement outcomes, thereby preserving the integrity and secrecy of the final key.

Proof of Lemma 1 (Unpredictability of Final State)

Restatement of Lemma 1:
Given $|\psi\rangle$ chosen via Ψ and evolved by $\mathcal{C}$ into $|\phi\rangle$, any adversary $\mathcal{E}$ with no prior interaction and no knowledge of the random seed defining $\mathcal{M}$ cannot predict $|\phi\rangle$ with probability greater than $1/|\mathcal{S}|$, where $\mathcal{S} \subset \mathcal{H}$ is the set of likely final states.

Proof:

1. By **Axiom 3 (Holographic Randomness)**, the initial state $|\psi\rangle = \Psi(\mathcal{M})$ is drawn from a distribution induced by $\mu(\mathcal{M})$. This measure μ ensures that $|\psi\rangle$ is essentially uniform over a subset of $\mathcal{H}$.

2. By **Axiom 4 (Markov Las Vegas Randomization)**, the circuit $\mathcal{C}$ acts as a quantum Markovian process on the manifold parameters. Hence, the final state $|\phi\rangle = \mathcal{C}(|\psi\rangle)$ is also distributed (conditioned on no external interference) according to a known uniform measure over $\mathcal{S} \subseteq \mathcal{H}$.

3. Since $\mathcal{E}$ has no knowledge of the seed defining $\mathcal{M}$ or the internal randomization of $\mathcal{C}$, her probability distribution for $|\phi\rangle$ must coincide with this uniform measure. In other words, from $\mathcal{E}$'s perspective, $|\phi\rangle$ could be any element of $\mathcal{S}$ with equal probability.

4. Thus, the best $\mathcal{E}$ can do is guess a particular state $|\phi'\rangle \in \mathcal{S}$. The probability of guessing correctly is $1/|\mathcal{S}|$.

5. Therefore, $\Pr[\mathcal{E} \text{ predicts } |\phi\rangle] \leq 1/|\mathcal{S}|$.

This completes the proof of Lemma 1.

Proof of Lemma 2 (No-Disturbance, No-Information)

Restatement of Lemma 2:
If an eavesdropper $\mathcal{E}$ attempts to measure $|\phi\rangle$ in a basis not aligned with its preparation subspace, the final measurement distribution observed by the authorized parties will deviate from the expected distribution by at least a factor $\eta > 0$.

Proof:

1. Consider that $|\phi\rangle$ is defined in some "correct" measurement scheme $\alpha \in \mathbb{A}$. That is, if the legitimate parties measure $|\phi\rangle$ in basis $\{|\varphi_\alpha\rangle\}$ associated with α, they expect a certain probability distribution P_α over the outcomes.

2. Suppose $\mathcal{E}$ measures $|\phi\rangle$ in a different basis $\{|\varphi_\beta\rangle\}$, with $\beta \neq \alpha$.

3. By **Axiom 2 (Measurement Disturbance)**, measuring a state prepared in one basis with a non-commuting basis introduces a nonzero probability of altering the state. This follows from the general quantum mechanical principle that non-commuting observables do not share eigenbases and that measurement collapses the wavefunction.

4. Formally, if $|\phi\rangle$ was consistent with basis α, a measurement in basis β will, with nonzero probability, project $|\phi\rangle$ into a subspace orthogonal (or partially orthogonal) to $|\varphi_\alpha\rangle$. Let ϵ_0 denote the minimum probability that the distribution of outcomes is altered in a detectable manner.

5. After $\mathcal{E}$'s interference, when the legitimate parties measure in the correct basis α, they will notice a deviation from the expected distribution P_α. This deviation can be bounded below by a positive constant η, which depends on the overlap between the bases and the structure of $|\phi\rangle$.

6. Hence, any attempt by $\mathcal{E}$ to extract information via wrong-basis measurement introduces a distinguishable statistical signature. Thus, no information can be gained without causing disturbance.

This completes the proof of Lemma 2.

Proof of Lemma 3 (Hamiltonian Integrity Check)

Restatement of Lemma 3:
If $|\phi\rangle$ is measured and found to approximate a known Hamiltonian ground state $|\phi_0\rangle$ such that $\langle\phi|H|\phi\rangle \leq E_0 + \varepsilon$, then with high probability no tampering occurred.

Proof:

1. By **Axiom 5 (Static Hamiltonian Witness)**, there exists a Hamiltonian H and a known ground state $|\phi_0\rangle$ (or low-energy state) with energy E_0. The set $\mathcal{G}$ of states that qualify as integrity witnesses are those for which $\langle\phi|H|\phi\rangle \approx E_0$, i.e., differ by no more than ε.

2. Consider that tampering by $\mathcal{E}$ would, with high probability, drive $|\phi\rangle$ out of $\mathcal{G}$. This is because the states consistent with no tampering form a delicate subset of $\mathcal{H}$. Disturbance forces $|\phi\rangle$ into a different configuration, typically raising its expected energy above $E_0 + \varepsilon$.

3. The variational principle in quantum mechanics states that for any arbitrary state $|\chi\rangle$, $\langle\chi|H|\chi\rangle \geq E_0$. If $|\phi\rangle$ closely approximates the ground state energy, it must be close (in Hilbert space norm) to $|\phi_0\rangle$. Significant tampering would shift $|\phi\rangle$ away from $|\phi_0\rangle$, increasing the expected energy.

4. Thus, measuring $|\phi\rangle$ and verifying that $\langle\phi|H|\phi\rangle \leq E_0 + \varepsilon$ provides evidence that $|\phi\rangle$ lies in $\mathcal{G}_\varepsilon$ (the set of states close to $|\phi_0\rangle$) and therefore that no significant tampering has occurred.

This completes the proof of Lemma 3.

Proof of the Main Theorem (Security of the Custom QOTP)

Theorem:
Given the axioms and lemmas, the Custom QOTP derived from a random manifold holographically encoded and verified via a Hamiltonian witness is secure. That is, for any eavesdropper $\mathcal{E}$, the probability of learning the key κ without detection is negligible.

Proof:

1. **Unpredictability of $|\phi\rangle$**:
   From Lemma 1, $\mathcal{E}$ cannot predict the final state $|\phi\rangle$. This ensures that the key $\kappa = K(|\phi\rangle)$ is uniformly random (as stated by the key extraction equation $\Pr(\kappa = s) = 2^{-n}$). Hence, guessing κ without any measurement is equivalent to random guessing, giving negligible advantage.

2. **Detection of Disturbance via Wrong-Basis Measurement**:
   If $\mathcal{E}$ attempts to measure $|\phi\rangle$ to gain information, Lemma 2 ensures that such a measurement in the wrong basis (which $\mathcal{E}$ is forced to attempt due to her ignorance of the correct scheme) introduces a detectable disturbance. The legitimate parties, by checking their expected distribution of outcomes, can spot this disturbance.

3. **Hamiltonian Witness Verification**:
   After $|\phi\rangle$ is established, the legitimate receiver (with the help of the trusted interpreter) verifies that $|\phi\rangle$ lies in the set $\mathcal{G}_\varepsilon$ by measuring $\langle\phi|H|\phi\rangle$. By Lemma 3, any tampering that would have allowed $\mathcal{E}$ to extract information increases the expected energy beyond $E_0 + \varepsilon$. Such an increase reveals the tampering.

4. **No Undetected Information Gain**:
   Combining the above points, $\mathcal{E}$ has two choices: (a) Attempt no measurement and remain ignorant, or (b) Attempt measurement and cause detectable disturbance or energy shift. In both cases, $\mathcal{E}$ cannot gain information about κ without the legitimate parties detecting it.

5. **Conclusion**:
   The key κ is therefore secure. Its security rests on the uniform random selection of $|\phi\rangle$, the disturbance caused by any unauthorized

measurement, and the Hamiltonian witness that amplifies any subtle tampering into a detectable signal. Hence, κ can serve as a one-time pad key, offering absolute security.

This completes the proof of the theorem.
End of Proofs

Notational and Conceptual Preliminaries

- Let $\mathcal{H}$ denote a Hilbert space associated with the quantum system used to generate and store the key.
- Let $\mathcal{M}$ be a random manifold derived from quantum-random processes, encoding information holographically.
- The holographic encoding is represented by a map $\Psi : \mathcal{M} \to \mathcal{H}$, which assigns to each manifold configuration a corresponding quantum state $|\psi\rangle \in \mathcal{H}$.
- A Markov "Las Vegas" quantum circuit $\mathcal{C}$ acts on states in $\mathcal{H}$ to generate non-deterministic evolutions: $|\phi\rangle = \mathcal{C}(|\psi\rangle)$.
- Let $\{|\varphi_\alpha\rangle\}$ be a set of measurement bases indexed by $\alpha \in \mathbb{A}$, where $\mathbb{A}$ is an index set representing different measurement schemes.
- A final measurement process $\mathcal{M}_f$ extracts a classical key $\kappa \in \{0,1\}^n$ from $|\phi\rangle$.
- A trusted human interpreter (or a trusted algorithm) tests consistency with a static Hamiltonian H acting on $\mathcal{H}$. The solution/witness ensures no tampering has occurred.

Axioms (Foundational Assumptions)

Axiom 1 (Quantum No-Cloning):
It is impossible to create an identical copy of an unknown quantum state. Formally, there exists no unitary U such that $U|\psi\rangle|e\rangle = |\psi\rangle|\psi\rangle$ for all $|\psi\rangle \in \mathcal{H}$.

Axiom 2 (Measurement Disturbance):
A measurement in a non-commuting basis disturbs the original state. If $|\psi\rangle$ is prepared in a basis associated with $\alpha \in \mathbb{A}$, then measuring in a basis $\beta \in \mathbb{A}, \beta \neq \alpha$, introduces a nonzero probability of error and irreversibly alters the state.

Axiom 3 (Holographic Randomness):
The mapping $\Psi : \mathcal{M} \to \mathcal{H}$ is surjective onto a complex subset of $\mathcal{H}$ and is chosen according to a probability measure $\mu(\mathcal{M})$ derived from inherently quantum-random processes. Thus, the induced distribution of states $|\psi\rangle$ is unpredictable and uniform over a suitable subset of states.

Axiom 4 (Markov Las Vegas Randomization):
The circuit $\mathcal{C}$ induces a Markovian stochastic process on the manifold's parameter space, ensuring that the final state $|\phi\rangle = \mathcal{C}(|\psi\rangle)$ cannot be predicted by an adversary who has not interacted with the system. Formally, for any fixed adversarial strategy $\mathcal{E}$, the distribution of $|\phi\rangle$ conditioned on no eavesdropping remains uniform over a designated state set.

Axiom 5 (Static Hamiltonian Witness):
There exists a Hamiltonian H and a known reference ground (or low-energy) state manifold $\mathcal{G} \subset \mathcal{H}$. If $|\phi\rangle \in \mathcal{G}$ or close to it by an agreed precision ε, we say $|\phi\rangle$ "witnesses" the integrity of the protocol. Unauthorized measurements produce deviations $\Delta > \delta(\varepsilon)$ detectable by verifying the Hamiltonian solution.

Lemmas

Lemma 1 (Unpredictability of Final State):
Statement: Given $|\psi\rangle$ chosen via Ψ and evolved by $\mathcal{C}$ into $|\phi\rangle$, any adversary $\mathcal{E}$ with no prior interaction and no knowledge of the random seed defining $\mathcal{M}$ cannot predict $|\phi\rangle$ with probability greater than $1/|\mathcal{S}|$, where $\mathcal{S} \subset \mathcal{H}$ is the set of likely final states.
Sketch of Proof: By Axiom 3 and 4, the distribution of final states is uniform over $\mathcal{S}$. Predicting $|\phi\rangle$ reduces to guessing a uniformly distributed outcome. Thus, $\Pr[\mathcal{E} \text{ predicts } |\phi\rangle] \leq 1/|\mathcal{S}|$.

Lemma 2 (No-Disturbance, No-Information):
Statement: If an eavesdropper $\mathcal{E}$ attempts to measure $|\phi\rangle$ in a basis not aligned with its preparation subspace, the final measurement distribution observed by the authorized parties will deviate from the expected distribution by at least a factor $\eta > 0$.
Sketch of Proof: By Axiom 2 (Measurement Disturbance) and the linearity of quantum mechanics, a wrong-basis measurement collapses $|\phi\rangle$ into states orthogonal or partially orthogonal to the intended measurement basis. Thus, the distribution of measurement outcomes differs detectably, ensuring a minimum distinguishability η.

Lemma 3 (Hamiltonian Integrity Check):
Statement: If $|\phi\rangle$ is measured and found to approximate a known Hamiltonian ground state $|\phi_0\rangle$ such that $\langle\phi|H|\phi\rangle \leq E_0 + \varepsilon$ (where E_0 is the ground state energy), then with high probability no tampering occurred.
Sketch of Proof: Any tampering shifts the state's distribution away from the set $\mathcal{G}$ of states that yield the correct Hamiltonian signature. By the variational principle and Axiom 5, such tampering leads to an energy deviation $\Delta E > \varepsilon$, which is detectable.

Equations for Quantities and Conditions

1. **Random Manifold Selection:**

$$\mathcal{M} \sim \mu(\mathcal{M}) \implies |\psi\rangle = \Psi(\mathcal{M}) \in \mathcal{H}.$$

2. **Markov Las Vegas Circuit Evolution:**

   $|\phi\rangle = \mathcal{C}(|\psi\rangle)$, with transition probabilities $p_{\alpha\to\beta}$ defined by a quantum Markov chain.

3. **Measurement and Disturbance Condition:**
   For a chosen measurement basis $\{|\varphi_\gamma\rangle\}$, if the state was prepared in basis $\{|\chi_\delta\rangle\}$ ($\delta \neq \gamma$), then:

   $\exists \epsilon_0 > 0 : \sum_\gamma |\langle\varphi_\gamma|\chi_\delta\rangle|^2 = 1$ but outcomes differ from intended distribution by ϵ_0.

4. **Hamiltonian Witness Condition:**
   Let H be the Hamiltonian and $|\phi_0\rangle \in \mathcal{G}$ be the reference ground state with energy E_0:

   $$\langle\phi|H|\phi\rangle \leq E_0 + \varepsilon \implies |\phi\rangle \in \mathcal{G}_\varepsilon.$$

   Deviations caused by tampering yield:

   $$\langle\phi|H|\phi\rangle > E_0 + \varepsilon \implies \text{Detected tampering.}$$

5. **Key Extraction:**
   The final key κ is extracted by a function:

   $$\kappa = K(|\phi\rangle), \quad \kappa \in \{0,1\}^n.$$

   Due to the uniformity and randomness ensured by the holographic encoding and the Markovian process:

   $$\Pr(\kappa = s) = 2^{-n}, \ \forall s \in \{0,1\}^n.$$

Proof Sketch of Security (Theorem):
Theorem: Given the axioms and lemmas, the Custom QOTP derived from a random manifold holographically encoded and verified via a Hamiltonian witness is secure. That is, for any eavesdropper $\mathcal{E}$, the probability of learning the key κ without detection is negligible.

Proof Outline:

1. **Randomness and Unpredictability:**
   By Lemma 1, the final state $|\phi\rangle$ is unpredictable. Hence the extracted key κ is uniformly random.

2. **No Gain Without Disturbance:**
   Suppose $\mathcal{E}$ attempts to measure $|\phi\rangle$. By Lemma 2, any partial measurement in the wrong basis introduces a detectable disturbance. Because $\mathcal{E}$ does not know the correct basis a priori (due to the complexity and randomness of $\mathcal{M}$ and $\mathcal{C}$), $\mathcal{E}$'s action changes the distribution observable by the legitimate parties.

3. **Hamiltonian Verification:**
   After $|\phi\rangle$ is prepared, the legitimate receiver solves or verifies the Hamiltonian witness condition. By Lemma 3, any tampering increases the effective "energy" above $E_0 + \varepsilon$, revealing the presence of $\mathcal{E}$.

4. **Conclusion:**
   Since $\mathcal{E}$ cannot measure $|\phi\rangle$ without introducing detectable errors, and cannot guess $|\phi\rangle$ or κ with better than random chance, the system ensures that κ is secure. The key is thus suitable for use in a one-time pad encryption, guaranteeing information-theoretic security. No classical or quantum polynomial-time algorithm exists for $\mathcal{E}$ to exploit hidden structure due to the inherent quantum randomness and topological complexity.

Hence, the constructed scheme realizes a form of QOTP—albeit in an elaborate geometric and holographic scenario—retaining the absolute security property: if the legitimate protocol requirements are met, no adversary can extract useful information about κ without being detected.

End of Proof and Formulation