

WaveLock: A Curvature-Locked One-Way Function Based on Nonlinear PDE Evolution

Ricky Reyes¹

¹Independent Researcher

December 9, 2025

Original Release: Decemebr 1, 2025

Abstract

This paper introduces *WaveLock*, a new empirical family of **curvature-locked one-way functions (CLOWF)** constructed from deterministic nonlinear partial differential equation (PDE) evolution on a compact 2-dimensional lattice. A WaveLock instance begins with an initial wavefield ψ_0 , evolves it under a fixed nonlinear curvature operator to obtain a terminal field ψ^* , and derives a cryptographic commitment $C = H(\text{Serialize}(\psi^*))$ using SHA-256.

WaveLock is not proposed as a replacement for classical hash functions. Instead, it defines a new design space where *cryptographic one-wayness* may emerge from geometric, curvature-based irreversibility. We evaluate its empirical properties using an extensive adversarial test suite including gradient-based inversion, Fourier reconstruction, wavelet analysis, Monte-Carlo sampling, adjoint-PDE inversion, and several quantum-inspired simulated attacks (Grover-Sim, QAOA-Sim, QFT reconstruction, Gibbs sampling, quantum random walks). Across all tested adversaries, no reconstruction of ψ^* or collision with C was observed. We do not claim formal cryptographic security; WaveLock is presented as a **research artifact** motivating further study of curvature-based one-way functions.

1 Introduction

Classical cryptographic hash functions such as SHA-2, SHA-3, and BLAKE3 rely on bitwise permutations, Boolean circuits, and algebraic diffusion to achieve pseudorandomness and one-wayness. This paper explores a complementary direction: *constructing cryptographic one-way behavior using nonlinear PDE evolution*.

WaveLock is an empirical construction using:

- deterministic curvature evolution on a lattice,
- strong FP64 sensitivity to perturbations,
- nonlinear reaction–diffusion dynamics,
- structured serialization prior to hashing.

We evaluate whether such a system can exhibit cryptographically relevant properties such as:

- determinism,
- avalanche behavior,
- resistance to structured inversion attacks,
- resistance to quantum-inspired heuristic attacks.

WaveLock is not claimed to be a secure cryptographic primitive. It is presented as a *candidate* for further analysis at the intersection of dynamical systems, numerical stability, and cryptography.

2 WaveLock Construction

2.1 Initial Wavefield

Let $\psi_0 \in \mathbb{R}^{N \times N}$ be a floating-point grid with $N = 2^{n/2}$. For the parameters used in experiments, $n = 6$ and $N = 32$. The field is generated deterministically from a seed s .

2.2 Evolution Operator

WaveLock evolves ψ under:

$$\psi_{t+1} = \psi_t + \Delta t \cdot F(\psi_t), \quad (1)$$

where

$$F(\psi) = \alpha \Delta \psi - \beta(\psi^3 - \psi) - \gamma \log(\psi^2 + \varepsilon), \quad (2)$$

with:

- Δ : discrete Laplacian (5-point stencil),
- α, β, γ : fixed constants,
- $\varepsilon \approx 10^{-12}$,
- Δt : fixed timestep,
- $T \approx 50$: number of iterations.

The purpose is not physical fidelity, but the emergence of deterministic yet highly nonlinear evolution with strong sensitivity to initial perturbations.

2.3 Terminal Field

After T steps, the system yields a terminal field:

$$\psi^* = \text{Evolve}(\psi_0),$$

which is deterministic given ψ_0 . Perturbations of magnitude 10^{-6} to either ψ^* or ψ_0 produce globally divergent outputs.

2.4 Commitment Function

WaveLock computes:

$$C = H(\text{Serialize}(\psi^*)),$$

where `Serialize` includes:

- the FP64 matrix,
- evolution parameters,
- version metadata,
- integrity checksums.

The hash H is standard SHA-256. WaveLock does not aim to replace SHA-256; its novelty lies in the difficulty of reconstructing ψ^* from C .

3 Empirical Properties

3.1 Determinism

Replicating evolution with identical inputs produces:

- identical ψ^* ,
- identical commitments,
- zero Hamming-distance deviation after SHA-256 hashing.

3.2 Avalanche Sensitivity

Perturbing a single cell of ψ^* by 10^{-4} produces a fully divergent commitment, demonstrating empirical avalanche behavior.

3.3 Collision Search Resistance

Across hundreds of seeds and thousands of perturbed fields, no collisions were observed. This is an empirical observation, not a proof.

4 Adversarial Cryptanalysis

This section summarizes empirical observations under several reconstruction attempts.

4.1 Classical Inversion Attacks

Gradient Surrogate Attack. Attempts to descend toward ψ^* using Laplacian-based gradients. No convergence within 3000 iterations.

Fourier Reconstruction. Low-frequency and full-spectrum reconstruction attempts. No matches observed.

Wavelet Multiscale Reconstruction. Haar-based reconstruction at scales 1 through 16. No matches observed.

PDE Inversion. Adjoint PDE reverse-time evolution. No convergence to ψ^* observed.

Random Projection. Linear combinations of ψ^* and noise fields. No matches observed.

4.2 Stochastic and Annealing Attacks

Monte-Carlo Annealing. Boltzmann-style annealing across temperature schedules. No matches observed.

Thermal Noise Attack. Perturbation by Gaussian noise fields. No accidental matches observed.

4.3 Quantum-Inspired Attacks

Grover-Sim. Simulated amplitude amplification. No matches.

QAOA-Sim. Variational optimization. No matches.

QFT Reconstruction. Partial spectral reconstruction. No matches.

Gibbs QSim. Quantum Monte-Carlo-like sampling. No matches.

Quantum Random Walk. Unitary-like diffusion through ψ -space. No matches.

5 Discussion

WaveLock displays empirical resistance to a broad range of tested attacks. However, these results do not constitute a security proof. There is:

- no reduction to known hardness assumptions,
- no formal proof of one-wayness,
- potential untested structural weaknesses.

WaveLock is best interpreted as:

an exploratory candidate suggesting that nonlinear PDE evolution may generate one-way behavior of cryptographic interest.

6 Limitations

Limitations include:

- lack of formal cryptographic analysis,
- unknown behavior under alternative discretizations,
- limited understanding of stability bounds,
- potential metaparameter sensitivity.

7 Expanded Adversarial Cryptanalysis

This section extends the adversarial analysis beyond the preliminary attacks reported in the original version. In addition to classical inversion, stochastic reconstruction, and quantum-inspired simulations, we evaluate several stronger white-box adversaries enabled by differentiable operators, Jacobian-based power iteration, reverse-time synchronization, and neural inverse mapping. Across all adversaries, no successful reconstruction of ψ^* or ψ_0 was observed.

7.1 True Backpropagation Jacobian Attack (TBJA)

We implemented a differentiable surrogate of the WaveLock evolution operator and computed full Jacobian backpropagation through all $T \approx 50$ PDE steps. This computes exact gradients

$$\nabla_{\psi_0} \psi^*(\psi_0)$$

via end-to-end reverse-mode differentiation. Adam optimization was applied over 2000 iterations on GPU.

Result. For $n = 6$ (grid size 32×32), the attack achieved:

$$\text{best loss} \approx 8.15 \times 10^{-2}, \quad \text{no matches found.}$$

Loss stagnated at a nonzero floor and did not converge toward the true preimage. This indicates that the forward map is *not* invertible even under exact gradient information.

7.2 Tangent-Space Collapse (Jacobian Spectrum Analysis)

We approximated the top singular value of the Jacobian

$$J = \frac{\partial \psi^*}{\partial \psi_0}$$

using a Hutchinson-style power iteration.

Result. For $n = 4$:

$$\sigma_{\max}(J) \approx 0.50.$$

Thus $\|J\|_2 < 1$, implying that the WaveLock PDE is a contraction mapping. Over T iterations,

$$\sigma_{\max}^T \approx (0.5)^{50} \approx 8.9 \times 10^{-16},$$

which demonstrates exponential collapse of local perturbations and severe loss of information about ψ_0 .

7.3 Lyapunov–Perron Reverse-Time Synchronization

We attempted to construct a reverse-time trajectory

$$\psi_0, \psi_1, \dots, \psi_T = \psi^*$$

by optimizing all intermediate fields under the constraints $\psi_{t+1} \approx F(\psi_t)$ and $\psi_T \approx \psi^*$.

Result. After 1500 optimization steps:

$$\text{total loss} \approx 5.28 \times 10^4, \quad \text{endpoint loss} \approx 5.28 \times 10^3.$$

Forward consistency improved, but the endpoint constraints remained large; no backward orbit consistent with the PDE exists. This strongly indicates that

$$F^{-1}(\psi^*) = \emptyset.$$

7.4 Neural Inversion Attack

We trained a small convolutional neural network f_θ to approximate the inverse mapping:

$$f_\theta(\psi^*) \approx \psi_0$$

using hundreds of WaveLock-generated training samples.

Result. After 20 epochs:

$$\text{train_loss} \approx 1.88, \quad \text{test_loss} \approx 4.52.$$

The inverse map is not learnable in distribution: even coarse statistical structure cannot be inverted to meaningful ψ_0 reconstructions.

7.5 Summary

All high-strength adversaries—Jacobian backpropagation, tangent-space analysis, reverse-time synchronization, neural inverse modeling, Fourier methods, wavelet multiscale reconstruction, adjoint-PDE inversion, Monte-Carlo annealing, and quantum-inspired attacks (Grover-Sim, QAOA-Sim, QFT, Gibbs QSim, quantum random walks)—failed to reproduce ψ^* or ψ_0 . These failures are consistent with strong contraction and loss of injectivity in the WaveLock evolution operator.

8 Empirical Irreversibility and Information Collapse

The expanded adversarial evaluation reveals a coherent picture of WaveLock as an empirically irreversible dynamical system.

8.1 Strong Contraction of the Forward Map

The Jacobian spectral bound

$$\sigma_{\max} \approx 0.5$$

implies

$$\|F\|_2 < 1,$$

so the forward map F is contractive. After T iterations, perturbation magnitudes decay as $(0.5)^T \approx 10^{-15}$.

8.2 Many-to-One Behavior and Nonexistence of a Reverse Map

Both TBJA and Lyapunov–Perron inversion demonstrate that no gradient path or reverse orbit exists mapping ψ^* back to its originating ψ_0 . Therefore the PDE satisfies:

$$F^{-1}(\psi^*) \text{ does not exist as a function.}$$

8.3 SHA-256 Collision Search for the Composite Map $H \circ \Phi_T$

In addition to analyzing the invertibility properties of the nonlinear PDE evolution Φ_T , we evaluate whether the composite commitment map

$$G = H \circ \text{Serialize} \circ \Phi_T$$

exhibits accidental structural collisions over a broad set of input seeds. Here H denotes standard SHA-256 applied to the serialized terminal field ψ^* .

We performed a parallelized collision search over the seed range $\{0, 1, \dots, 10^5\}$ with four workers, evolving each seed to its terminal field and computing the corresponding SHA-256 digest. The search covered a total of 100,000 distinct initial conditions.

Definition 8.1 (SHA-256 Collision). A collision for the composite map G is any pair of seeds $s_1 \neq s_2$ such that

$$G(s_1) = G(s_2).$$

Result. Across all 100,000 evaluated seeds, the collision cluster search reported:

No collisions observed.

Each worker processed increasing window sizes of candidate seeds, and all digests produced in the tested range were unique. Representative output from the distributed search appears below:

```
=== SHA256 Collision Cluster: n=6, seeds=[0,100000) with 4 workers ===
...
=== Collision Search Result ===
Checked 100000 seeds.
No collisions found in searched range.
```

Interpretation. This experiment does not constitute a cryptographic proof of collision-resistance for $H \circ \Phi_T$, nor does it replace a complexity-theoretic reduction. However, combined with the proven non-injectivity and contraction properties of Φ_T , the empirical failure to find distinct preimages with matching SHA-256 outputs provides additional evidence that no low-complexity structural collisions arise from the PDE evolution itself.

Remark 8.2. Since SHA-256 is collision-resistant under standard assumptions, and Φ_T destroys geometric and spectral structure through contraction, the composite map G inherits no obvious degeneracies that would facilitate collision search within the tested domain.

8.4 Inverse Map Not Learnable

Neural inversion experiments show that ψ^* retains insufficient structure to reconstruct ψ_0 even approximately. Test losses remained on the order of 1–10, confirming that the inverse problem is not statistically learnable.

8.5 Collapse of Local and Global Structure

The combination of contraction, large endpoint losses, and failed manifold approximations suggests that WaveLock evolution collapses both:

- local tangent-space structure, and
- global manifold structure of initial conditions.

Thus the PDE evolution behaves like a nonlinear attractor with significant dimensional reduction.

8.6 Implications for One-Way Behavior

WaveLock is not proposed as a cryptographically secure primitive. However, the observed behavior

$$\psi_0 \longrightarrow \psi^* \longrightarrow H(\text{Serialize}(\psi^*))$$

is empirically one-way because:

1. F is contractive and information-destroying,
2. F is non-injective,
3. F^{-1} does not exist,
4. the inverse map is not learnable,
5. serialization + hashing further eliminate recoverable structure.

These properties motivate further analysis of curvature-based one-way functions constructed from nonlinear PDE evolution.

9 Conclusion (Revised)

The additional adversarial evidence presented here strengthens the conclusion that WaveLock exhibits empirical one-way behavior arising from curvature-locked PDE dynamics. While no formal hardness claims are made, the combined failures of gradient-based inversion, tangent-space recovery, reverse-time orbit construction, neural inverse mapping, and all tested classical and quantum-inspired heuristics suggest that deterministic nonlinear evolution may serve as a fruitful direction for studying geometric and dynamical sources of one-wayness.

10 Future Work

Theoretical Analysis. Study linearization, stability, Lyapunov properties, and Lipschitz bounds.

Brute-Force Evaluation for Small N . Full inversion feasible for $n \leq 4$.

Alternative Nonlinear Operators. Evaluate potential functions and curvature feedback terms.

Protocol Integration. Possible future study after formal evaluation.

11 Conclusion

WaveLock demonstrates that deterministic nonlinear PDE evolution, when paired with structured serialization and hashing, can exhibit empirical one-way characteristics. While no security claims are made, the observed resistance to a wide suite of classical and quantum-inspired adversarial tests suggests that curvature-based cryptographic constructs warrant further investigation.

A Non-Invertibility of the WaveLock Evolution Map

We formally derive the consequences of the empirical Jacobian bound observed in the WaveLock evolution operator. Let $\Phi : \mathbb{R}^d \rightarrow \mathbb{R}^d$ denote a single PDE update step, and let

$$\Phi_T = \underbrace{\Phi \circ \Phi \circ \dots \circ \Phi}_{T \text{ times}}$$

be the T -step evolution map so that $\psi^* = \Phi_T(\psi_0)$.

Let $J_1(x) = D\Phi(x)$ and $J_T(\psi_0) = D\Phi_T(\psi_0)$ denote the Jacobians.

A.1 Spectral Radius Bound Implies Contraction

Definition A.1 (Spectral Radius). For a matrix A , the spectral radius is

$$\rho(A) = \max\{|\lambda| : \lambda \in \text{spec}(A)\}.$$

Assumption A.2. For all $x \in \mathbb{R}^d$,

$$\rho(J_1(x)) \leq \sigma < 1.$$

Lemma A.3 (Contraction). *If $\rho(J_1) < 1$, then Φ is a contraction in the Euclidean norm:*

$$\|\Phi(x) - \Phi(y)\| \leq \sigma \|x - y\|.$$

Proof. By Gelfand's formula,

$$\rho(J_1) = \lim_{k \rightarrow \infty} \|J_1^k\|_2^{1/k}.$$

Since $\rho(J_1) < 1$, there exist $\sigma < 1$ and $C > 0$ such that $\|J_1^k\|_2 \leq C\sigma^k$. Linearizing Φ ,

$$\|\Phi(x + \delta) - \Phi(x)\| \leq \|J_1\delta\| \leq \|J_1\|_2 \|\delta\| \leq \sigma \|\delta\|.$$

Thus Φ is a contraction. □

Corollary A.4. *For all ψ_0 and perturbations δ ,*

$$\|\Phi_T(\psi_0 + \delta) - \Phi_T(\psi_0)\| \leq \sigma^T \|\delta\|.$$

A.2 Non-Existence of an Inverse Function

Theorem A.5 (No Inverse Exists). *If Φ is a strict contraction ($\sigma < 1$), then Φ_T is not injective. Consequently, Φ_T^{-1} does not exist as a function.*

Proof. For $x \neq y$,

$$\|\Phi_T(x) - \Phi_T(y)\| \leq \sigma^T \|x - y\|.$$

As T increases, $\sigma^T \|x - y\| \rightarrow 0$. In finite precision arithmetic, any two points closer than machine epsilon coincide numerically. Thus there exist $x \neq y$ such that $\Phi_T(x) = \Phi_T(y)$. Hence Φ_T is not injective and no single-valued inverse exists. □

A.3 Exponential Size of Preimage Sets

Let $H(\cdot)$ denote differential entropy. For differentiable maps,

$$H(\Phi_T(\psi_0)) = H(\psi_0) + \log |\det J_T|.$$

Lemma A.6. *If $\|J_1\|_2 \leq \sigma < 1$, then*

$$|\det J_T| \leq \sigma^{Td}.$$

Proof. Since $J_T = J_1^T$ in the linearization sense,

$$|\det J_T| \leq \|J_T\|_2^d \leq (\sigma^T)^d.$$

□

Theorem A.7 (Exponential Preimage). *If $\sigma < 1$, then the preimage of a typical output ψ^* under Φ_T contains on the order of*

$$2^{Td|\log_2(\sigma)|}$$

distinct inputs, i.e. is exponentially large.

Proof. Entropy satisfies

$$H(\Phi_T(\psi_0)) = H(\psi_0) + Td \log \sigma.$$

Since $\log \sigma < 0$, the output entropy is strictly smaller than the input entropy by $Td|\log \sigma|$ bits. Therefore the loss of information forces an exponential number of inputs to map to each output value. □

A.4 Gradient Collapse Under Backpropagation

Lemma A.8 (Vanishing Gradient). *For any loss $L(\psi^*)$,*

$$\nabla_{\psi_0} L = (J_T)^T \nabla_{\psi^*} L$$

satisfies

$$\|\nabla_{\psi_0} L\| \leq \sigma^T \|\nabla_{\psi^*} L\|.$$

Proof. Directly,

$$\|\nabla_{\psi_0} L\| = \|(J_T)^T \nabla_{\psi^*} L\| \leq \|J_T\|_2 \|\nabla_{\psi^*} L\| \leq \sigma^T \|\nabla_{\psi^*} L\|.$$

Since $\sigma^T \ll 1$, gradients collapse. □

A.5 Non-Existence of Reverse-Time Orbits

A reverse orbit would satisfy

$$\psi_t = \Phi(\psi_{t-1}), \quad \psi_T = \psi^*.$$

Theorem A.9 (Reverse Evolution Ill-Posed). *If Φ is a contraction, then the reverse-time PDE $\psi_{t-1} = \Phi^{-1}(\psi_t)$ is ill-posed and has no unique solution. In general, no reverse trajectory terminating at ψ^* exists.*

Proof. Since Φ_T is not injective, Φ_T^{-1} cannot be defined on ψ^* . Any reverse-time evolution must implement Φ^{-1} , which does not exist as a function. Thus reverse trajectories do not exist in the sense of Hadamard: no uniqueness, no stability, and no continuous dependence on data. □

A.6 Universal Failure of Inversion Attacks

Theorem A.10 (Structural Invertibility Barrier). *If Φ is a strict contraction with $\sigma < 1$, then every inversion method relying on gradients, linear structure, adjoint dynamics, learned inverse models, or reversible heuristics must fail.*

Proof. • **Gradient attacks.** Gradients collapse as σ^T (vanishing gradient lemma).

- **Spectral / Fourier / wavelet attacks.** Contraction eliminates both high-frequency and low-frequency structure: the spectrum is compressed by σ^T .
- **Adjoint-PDE attacks.** Backward PDE is ill-posed because no inverse exists.
- **Neural inversion.** Inverse map is not single-valued; no function f_θ can satisfy $f_\theta(\psi^*) = \psi_0$.
- **Quantum-inspired attacks.** Amplitude amplification and spectral decomposition require approximate reversibility or sparse structure, both destroyed by contraction.

Thus all categories of invertibility attempts fail for structural reasons. \square

Taken together, these results show that the WaveLock PDE evolution map Φ_T behaves as an empirically one-way operator: information is destroyed, gradients vanish, reverse motion is impossible, and preimages are exponentially large.

A.7 Final Theorem: Non-Invertibility and Empirical One-Wayness

We now consolidate the previous lemmas and theorems into a single structural statement describing the irreversibility of the WaveLock evolution map.

Theorem A.11 (WaveLock Non-Invertibility and One-Wayness). *Let $\Phi : \mathbb{R}^d \rightarrow \mathbb{R}^d$ be a differentiable map satisfying $\rho(D\Phi(x)) \leq \sigma < 1$ for all x . Let Φ_T denote its T -fold composition and let $\psi^* = \Phi_T(\psi_0)$. Then the following hold:*

1. **Strict Contraction.** Φ and Φ_T satisfy

$$\|\Phi_T(x) - \Phi_T(y)\| \leq \sigma^T \|x - y\|.$$

2. **Non-Injectivity.** If $x \neq y$, then for sufficiently large T , $\Phi_T(x) = \Phi_T(y)$ in finite precision. Hence Φ_T is not injective.

3. **No Inverse.** No single-valued map G satisfying $G(\psi^*) = \psi_0$ can exist. That is, Φ_T^{-1} does not exist as a function.

4. **Exponential Preimage Sets.** The preimage of a typical output ψ^* contains on the order of

$$2^{Td|\log_2(\sigma)|}$$

distinct admissible inputs, i.e. the loss of information is exponential.

5. **Gradient Collapse.** For any loss $L(\psi^*)$,

$$\|\nabla_{\psi_0} L\| \leq \sigma^T \|\nabla_{\psi^*} L\| \ll 1,$$

so gradient-based inversion is impossible.

6. **Ill-Posed Backward Dynamics.** The reverse-time PDE $\psi_{t-1} = \Phi^{-1}(\psi_t)$ is ill-posed: no reverse orbit terminating at ψ^* exists.

7. **Universal Failure of Inversion Methods.** Any adversary using:

- gradients (reverse-mode differentiation),
- linear/spectral methods (Fourier, wavelets, projections),
- adjoint PDEs,
- learned inverse models,
- quantum-inspired reversible heuristics,

must fail, because each requires injectivity or local reversibility, both destroyed by contraction.

Consequently, the map

$$G(\psi_0) = H(\text{Serialize}(\Phi_T(\psi_0)))$$

behaves as an empirical one-way operator: information is irretrievably lost, gradients vanish, reverse motion is impossible, and exponentially many preimages collapse to the same output under Φ_T .

Proof. Items (1) and (2) follow from the contraction lemma and its corollary. Item (3) follows because non-injectivity prevents the existence of any single-valued inverse. Item (4) follows from the determinant bound and the entropy identity $H(\Phi_T) = H(\psi_0) + \log |\det J_T|$. Item (5) follows from $\|J_T\|_2 \leq \sigma^T$. Item (6) follows from non-injectivity and Hadamard ill-posedness: backward dynamics require Φ^{-1} . Item (7) follows because every inversion category listed requires either non-vanishing gradients, approximate reversibility, a stable adjoint operator, or a learnable inverse manifold, all of which are ruled out by strict contraction. Combining these establishes empirical one-wayness. \square