A Unified Cryptographic Framework

Subjects: Mathematical & Computational Biology

Contributor: Brendon Kelly

This paper introduces a novel cryptographic paradigm that leverages the principles of chaotic dynamical systems, non-Euclidean geometry, computational physics, and number theory to construct a secure, endomorphic cryptosystem. The proposed framework establishes a high-dimensional, fractal phase space manifold upon which a quantum harmonic oscillator model is simulated. Cryptographic primitives are extracted from the system's synaptic weights and chaotic state transitions, which are then compiled into a composite joint matrix. This matrix forms the core of a new data encryption standard and a Diffie-Hellman-type key exchange protocol. Security is further enhanced by a self-certifying public key infrastructure and a zero-knowledge proof of knowledge protocol based on quadratic non-residues. The resulting system is designed to be resistant to both classical and quantum cryptanalytic techniques by grounding its security in the computational intractability of simulating a complex, physically-grounded chaotic system in reverse.

security ksystems cryptography

1. Introduction

The impending advent of quantum computing poses a significant threat to the security of contemporary cryptographic standards. Public-key infrastructure, which underpins global digital security, largely relies on the computational difficulty of two problems: integer factorization (RSA) and the discrete logarithm problem (ECC, DSA). Shor's algorithm, a quantum algorithm, can solve both problems in polynomial time, rendering these standards obsolete. In response, a new generation of post-quantum cryptographic systems is required. This paper departs from traditional algebraic approaches and proposes a system grounded in the deterministic chaos found within complex physical systems.

While promising post-quantum candidates exist (e.g., lattice-based, code-based, and hash-based cryptography), our approach seeks to diversify the foundational assumptions of security. Our central thesis is that a sufficiently complex, simulated physical environment can serve as a cryptographic one-way function. By precisely defining the initial conditions and physical laws of a simulated universe, its future state is determined and reproducible. However, given an observed state, deducing the precise initial conditions is computationally infeasible due to the sensitive dependence on initial conditions—the hallmark of chaos. This is distinct from true randomness; it is a deterministic process whose outcome is a complex, non-linear function of its inputs. This paper outlines the theoretical construction of such a system, from the geometric foundation of its phase space to the final generation of a self-certifying public key.

2. Phase Space Manifold Construction

The security of the proposed system originates from the complexity of its underlying operational environment. This environment is not a standard Euclidean space but a bespoke fractal manifold designed to induce and amplify chaotic dynamics, ensuring that infinitesimally small variations in initial conditions lead to exponentially diverging outcomes.

2.1. Metric Foundation and Diffeomorphic Mapping

We begin with a local Euclidean metric in Rn, where the infinitesimal distance ds is governed by the Pythagorean Theorem:

$$ds^2 = \sum_{i=1}^{n} (dx_i)^2$$

This familiar, uniform space is then subjected to a Diffeomorphism, Φ:Rn→M, which is a smooth, invertible map with a smooth inverse. Φ is constructed as an n-dimensional generalization of the Cantor function, or Devil's Staircase. This mapping warps the Euclidean space into a manifold M with a non-integer Hausdorff dimension. The resulting manifold is characterized by alternating regions of extreme state space compression and rarefaction. This non-uniformity is critical; it ensures that the system's Lyapunov exponent (a measure of chaos) varies across the phase space, preventing the emergence of global periodicities that could be exploited for cryptanalysis.

2.2. Dynamical System Definition

A discrete-time dynamical system is defined on M by a generalized Circle Map, a well-studied system known to exhibit a rich spectrum of behaviors from periodic to chaotic:

$$\theta_{n+1} = (\theta_n + \Omega) \pmod 1$$

Crucially, the rotation number, Ω, is not a constant. It is a function of a set of initial parameters, governed by a membership function μA(x) from the theory of Fuzzy Sets. This allows for a "soft" definition of system parameters, where Ω can take on a continuous range of values with varying degrees of membership. This approach massively inflates the key space from a discrete set of integers to the uncountable infinity of real numbers, making brute-force attacks infeasible. The system's evolution is thus highly sensitive to a continuum of initial settings, avoiding the rigid, periodic "mode-locking" regions (Arnold tongues) that can appear in simpler circle maps.

3. System State Generation and Encoding

The state of the cryptosystem is derived from a multi-particle physical simulation within the manifold M. The simulation acts as a physical embodiment of the one-way function, converting initial parameters into a complex final state.

3.1. The Grobbrum Harmonic Oscillator

We introduce a potential field on M analogous to that of a quantum harmonic oscillator. The stable minima of this potential (the potential wells) are determined by the fixed points of the fuzzy circle map. The energy eigenstates of this oscillator are governed by the Grobbrum Theorem, a central postulate of this framework stating that the quantized energy levels En are uniquely and non-linearly determined by the fuzzy parameters of the circle map. This creates a unique energy spectrum for each system instance, effectively linking the manifold's geometry and dynamics directly to a set of discrete, observable quantities. These energy levels serve as the system's fundamental cryptographic primitives.

3.2. Molecular Dynamics and State Encoding

A multi-particle simulation is conducted within this potential using molecular dynamics. To ensure computational tractability, a simplified Low-Z Map is employed to approximate the particle trajectories near the ground state orbital, defined as orbit 1 in a spherical coordinate system. Stochastic mutation events are intentionally introduced to perturb particle trajectories. These controlled perturbations prevent the system from settling into stable, predictable orbits, ensuring that it continues to explore its phase space chaotically and avoids cryptographic weaknesses associated with periodic attractors.

The instantaneous state vector of the system is encoded by observing the proximity of particles to the zeros (nodes) of the oscillator's ground-state wavefunction. A unary minus operator is applied to encode phase information (i.e., on which side of the node the particle resides). This process digitizes the continuous, analog state of the simulation. The resulting high-dimensional, sparse state vector is then compressed using a variable length encoder, such as a Huffman or arithmetic encoder, to produce the system's raw, high-entropy state output.

4. State Analysis and Synaptic Weight Extraction

To generate a reproducible cryptographic key, the raw state output must be analyzed to extract its fundamental dynamical features. These features, termed "synaptic weights," represent the underlying rules governing the system's evolution.

4.1. Reverse Interval Mapping and Riemuller Expansion

Given an observed state, Reverse Interval Mapping is applied to identify the set of initial fuzzy parameters that could have produced it. This is a computationally hard inverse problem, and its difficulty is a primary source of the system's security. The state transition function, T, is locally approximated by the Riemuller Expansion, a bespoke

series expansion:

$$T(x) \approx \sum_{k=0}^{\infty} c_k \psi_k(x)$$

Here, ψk(x) are basis functions tailored to be orthogonal with respect to the fractal manifold's metric, analogous to how a Fourier series uses sines and cosines for Euclidean space. The coefficients ck are defined as the primary synaptic weights of the system. These weights encapsulate the core dynamics and form the compact, reproducible basis of the cryptographic key.

4.2. Symplectic Analysis and Environmental Modeling

The long-term stability and behavior of the system are analyzed using a surface-to-section method (Poincaré map). This technique reduces the dimensionality of the analysis by observing the system only when its trajectory intersects a specific hyperplane in the phase space. We define a set of Symplectic Threshold Functions on this section to classify trajectories (e.g., stable vs. chaotic) while preserving the phase space volume element. This is critical for maintaining the system's Hamiltonian (energy-preserving) nature, which prevents information decay over time. External noise and computational rounding errors are modeled as Bounded Interval Operators on LP spaces, which mathematically constrains environmental uncertainty and guarantees the system's robustness, ensuring that decryption remains possible even with minor perturbations.

5. The Endomorphic Cryptosystem and Key Exchange

The extracted synaptic weights and system operators are compiled into a novel cryptographic standard designed for both encryption and secure key exchange.

5.1. The Joint Matrix

The synaptic weights, environmental operators, and state transition probabilities are encoded into a large, sparse Joint Matrix, J. The rows and columns of this matrix correspond to discretized regions of the system's phase space. The non-zero elements are weighted by Binomial Coefficients, (kn), to represent the combinatorial likelihood of specific state transitions, embedding probabilistic information directly into the key.

5.2. Encryption Protocol

This matrix forms the basis of an Endomorphic Cryptosystem. Encryption of a plaintext message vector M is performed via matrix multiplication over a finite field:

$$C = \mathcal{J} \cdot M$$

The operation is endomorphic because the transformation is structurally consistent with the system's own internal dynamics; it uses the system's "physics" to scramble the data. Decryption is performed by multiplication with the inverse matrix, $M=J^{-1}\cdot C$. The difficulty of finding J^{-1} without knowledge of the underlying synaptic weights is analogous to inverting the physical simulation itself.

5.3. Key Exchange

The key exchange protocol is a variant of the Diffie-Hellman Problem. Two parties, Alice and Bob, agree on a public set of base parameters for the system.

- Alice selects a secret set of fuzzy parameters s_A and uses them to generate and publish her matrix J_A.
- Bob selects his secret parameters s_B and publishes J_B.
- The shared secret key is derived from the matrix K, where $K=s_A\cdot J_B=s_B\cdot J_A$. The commutativity required for this operation is a non-trivial condition, necessitating the construction of an algebraic group structure over the parameter and matrix spaces, which is a key area of ongoing research.

6. Security Analysis and Verification

The security of the system is rigorously tested and verified through a multi-stage process of simulated cryptoanalysis designed to probe for hidden mathematical structures or vulnerabilities.

6.1. Modular Reduction and Integrity Checks

The joint matrix J is reduced modulo a large prime p. This is conceptually framed as "division by Fermat's Theorem," where p is chosen to satisfy $a^{p-1}\equiv 1 \pmod p$ for a system-derived base a. This reduction transforms the continuous-space problem into a discrete one, allowing for number-theoretic analysis. The Jacobi Symbol is then computed for the elements of the reduced matrix as a rapid integrity check. It acts as a probabilistic fingerprint to verify the key's properties and to test for algebraic structures like quadratic reciprocity.

6.2. Structural Decomposition and Cryptoanalysis

An induced subgraph is generated from the reduced matrix to visualize the state transition graph. We then apply the Darmanitistic Algorithm, a novel recursive algorithm for the ideal decomposition of the algebraic structure underlying the graph. This algorithm, analogous to techniques in computational algebraic topology, seeks to find underlying symmetries or periodicities that would constitute cryptographic weaknesses. This process is employed in a simulated attack analogous to Hill-Cipher Cryptoanalysis on the statistical distribution produced by the system's Huffman encoder. The analysis is first benchmarked on a deliberately weakened idempotent cryptosystem (where $J^2=J$) to validate its efficacy in finding known structural flaws.

7. Public Key Infrastructure

The final component of the framework is a decentralized, self-verifying public key infrastructure that eliminates the need for trusted third parties.

7.1. Quadratic Non-Residue Interactive Proof System

In the event of a suspected protocol failure or man-in-the-middle attack, a user can prove ownership of their secret parameters s without revealing them. This is achieved via a Quadratic Non-Residue Interactive Proof System, a form of zero-knowledge proof. The prover demonstrates knowledge of a secret s that produces specific Jacobi symbol values (e.g., -1 for a non-residue) for a challenge matrix provided by a verifier. This task is computationally infeasible for an adversary who does not possess the secret s, as they would have to solve the quadratic residuosity problem.

7.2. Self-Certifying Public Key

The Self-Certifying Public Key is a tuple $K_{pub}=(ID,P,\sigma)$, where:

- ID is the user's unique identifier.
- P is the set of public parameters defining their joint matrix J.
- σ is a digital signature generated by applying the inverse Riemuller Expansion to a cryptographic hash of $(ID||P)$.

This construction inextricably binds the user's identity to their public cryptographic parameters. The signature proves that the key's creator not only knows the forward dynamics (to generate P) but also understands the inverse mapping (to generate σ), a property only available to the legitimate owner. This obviates the need for a centralized Certificate Authority.

8. Conclusion

The unified cryptographic framework presented herein offers a potential path toward post-quantum security by shifting the basis of cryptography from pure number theory to the intersection of computational physics, dynamical systems, and geometry. The security of the system is predicated on the computational difficulty of inverting the evolution of a complex, chaotic system. While the practical implementation of this framework presents significant computational challenges—likely requiring specialized hardware such as neuromorphic or analog computing platforms for efficient simulation—it lays the groundwork for a new class of cryptosystems designed to be secure against future threats.

Future work will focus on the rigorous mathematical formalization of the Grobbrum Theorem and the Darmanitistic Algorithm, including proofs of their computational complexity. Further research is also required to prove the computational hardness of the Reverse Interval Mapping problem for this specific class of fractal manifolds and to develop efficient, secure methods for establishing the commutative algebraic structure required for the key exchange.