Title

Love's Algorithm

Description

Field of the Invention

The invention relates to cybersecurity, identity verification, digital access control, cryptographic key management, post-quantum cryptography, machine-learning-based behavioural analysis, and distributed system security. Specifically, it concerns systems and methods for dynamically orchestrating identity and trust using fractal entropy, behavioural biometrics, device attestation, artificial intelligence, and post-quantum cryptographic primitives.

Background of the Invention

Current identity and access-control systems rely on static authentication factors, predictable key rotation schedules, and fixed access policies. These systems are vulnerable to:

• credential theft

• behavioural spoofing

• malware impersonation

• insider manipulation

• timing attacks

• cryptographic compromise

• quantum-enabled decryption via Shor's algorithm

• adversarial modelling of predictable security behaviours

Modern infrastructures lack the ability to re-evaluate identity continuously, adjust trust adaptively, or respond to subtle behavioural anomalies in real time. Post-quantum cryptographic standards address mathematical weaknesses but do not address human or device identity. Behavioural biometrics exist, but they operate in isolation. Key rotation exists, but it is triggered on predictable intervals. No system integrates chaotic entropy, behavioural biometrics, device attestation, continuous AI risk scoring, and post-quantum cryptography into a single trust fabric. Thus, there is a need for a unified trust orchestration system capable of continuously adapting to behavioural and

environmental changes, resistant to quantum attacks, and able to dynamically govern security posture across distributed systems.

This invention is related to, and builds upon, four earlier applications by the same inventor:

- GB2520379.5 — a portable identity device (sometimes referred to as "TuringKey")
- GB2520380.3 — a behavioural entropy-based key derivation system
- GB2520385.2 — a device environment attestation mesh for context-bound identity and trust enforcement
- GB2520368.8 — systems and methods for chaotic-entropy-driven multi-layer trust orchestration

These earlier systems provide specific embodiments of hardware identity vaults, behavioural-entropy engines, device and environment attestation modules, and multi-layer trust-orchestration components. The present invention, Love's Algorithm, unifies these capabilities into a single adaptive trust-fabric architecture.

Summary of the Invention

The invention introduces Love's Algorithm, a trust-orchestration engine operating across human, device, behavioural, and cryptographic layers simultaneously. The system generates a real-time trust score that governs:

- authentication requirements
- access permissions
- cryptographic key rotation frequency
- node isolation
- session termination
- privilege escalation or suppression
- PQC key life-cycle transitions
- anomaly response actions

Trust is evaluated continuously using a fractal entropy generator, behavioural-biometric models, device attestation, environmental fingerprinting, and post-quantum cryptographic signals. The system introduces:

- fractal timing to prevent adversarial prediction
- continuous behavioural identity verification
- multi-layered MFA escalation

• adaptive PQC key rotation

• chaotic access windows

• autonomous security posture scaling

This produces a dynamic, unpredictable, quantum-resistant identity system that surpasses any fixed-rule authentication architecture.

The invention provides a unified trust-fabric architecture integrating chaotic entropy, behavioural entropy, distributed attestation, dynamic trust scoring, and post-quantum key governance into a single orchestration system.
This architecture subsumes multiple identity, attestation, trust, and cryptographic subsystems into a cohesive, adaptive enforcement framework.

This invention establishes a new class of cybersecurity architecture referred to as Chaotic-Entropy-Driven Trust Fabric Systems.

The unified trust fabric described herein may incorporate, interface with, or extend the systems disclosed in GB2520379.5, GB2520380.3, GB2520385.2, and GB2520368.8 as module-level embodiments within the overarching Chaotic-Entropy-Driven Trust Fabric architecture.

Detailed Description of the Invention

Figure 1: The overall system architecture of the trust orchestration platform. The system comprises a Fractal Entropy Generator, a Behavioural Biometric Engine, a Device and Environment Attestation Module, an Anomaly Detection Engine, a Post-Quantum Cryptography Controller, an Adaptive Trust Engine and a Distributed Node Enforcement Layer. In some embodiments, the portable identity device disclosed in GB2520379.5 implements the hardware identity vault and local reflex trust engine; the behavioural entropy-based key derivation mechanism disclosed in GB2520380.3 corresponds to the behavioural-entropy engine; the environment attestation mesh disclosed in GB2520385.2 provides contextual attestation indicators; and the multi-layer orchestration framework disclosed in GB2520368.8 maps to the distributed trust-fabric and enforcement layer within which Love's Algorithm operates. Data produced by the Fractal Entropy Generator, Behavioural Biometric Engine, Device and Environment Attestation Module and Anomaly Detection Engine is provided to the Adaptive Trust Engine, which computes a dynamic trust score. The trust score is used to control the Post-Quantum Cryptography Controller and the Distributed Node Enforcement Layer, enabling key management and enforcement actions across nodes.

Figure 2: The data flow used to compute the trust score and resulting security posture. interaction-derived entropy, including timing variance, motion-pattern irregularities, and

response-dynamics characteristics, device attestation data, environmental fingerprint data, fractal entropy values and anomaly indicators are all provided as inputs to the trust calculation process. The Adaptive Trust Engine combines these inputs into a single trust score. This trust score is then used to determine security posture outputs, including access permissions, required authentication factors, session lifetime and cryptographic key rotation or regeneration.

Figure 3: Timing behaviour of cryptographic key rotation controlled by fractal entropy. A timeline of system operation is associated with a sequence of key rotation events. The intervals between rotation events vary according to the output of the Fractal Entropy Generator rather than following fixed periods. This produces non-predictable key rotation timings, which are used by the Post-Quantum Cryptography Controller to regenerate or invalidate keys under control of the Adaptive Trust Engine.

Figure 4: The evolution of the trust score over time and associated security actions. The trust score varies in response to changes in behaviour, device state, environment and anomaly detection signals. When the trust score remains above a defined threshold, normal access is maintained. When the trust score drops below the threshold, one or more security actions are triggered, such as requiring additional authentication factors, reducing access privileges, terminating a session or isolating a node. When the trust score recovers, access conditions can be relaxed accordingly.

Figure 5: The integration of post-quantum cryptographic primitives within the trust-controlled key life-cycle. The Post-Quantum Cryptography Controller manages key exchange based on a Lattice-based, hash-based, or other post-quantum cryptographic primitives. The Adaptive Trust Engine issues commands to regenerate, rotate or revoke these keys according to the current trust score, anomaly conditions and fractal entropy outputs, resulting in a dynamic cryptographic state.

Figure 6: An adaptive multi-step authentication path governed by the trust score. Multiple authentication mechanisms are available, device-state verification, user-interaction validation, cryptographic proofing, or environmental consistency checks, including timing variance, motion-pattern irregularities, response-dynamics characteristics and validation of post-quantum certificates. The Adaptive Trust Engine selects which steps are required, in which order and within what time constraints, based on the current trust score and entropy state. Higher-risk situations cause more steps to be required, while lower-risk situations can allow a reduced set of steps.

Figure 7: The isolation of a node in a distributed system based on a low trust score. Multiple nodes operate within a shared infrastructure. For a node whose associated trust score falls below a defined isolation threshold, the Adaptive Trust Engine instructs the Distributed Node Enforcement Layer to restrict or block its communications, regenerate its cryptographic keys and require fresh attestation before it can rejoin

normal operation. Other nodes with acceptable trust scores continue operating without interruption.

Figure 8: Multi-modal behavioural interaction entropy, including timing variance, motion-pattern irregularities, and response-dynamics characteristics.

Figure 9: Cryptographically verifiable device-state, environment-state, and context-state indicators

Figure 10: A session-governance subsystem wherein session duration, privilege levels, idle timers, and re-authentication events are dynamically modulated based on trust score trajectories and entropy-derived timing variance.

Figure 11: A security-posture adjustment subsystem that autonomously scales restrictions, verification requirements, and cryptographic transitions according to ongoing trust-state changes and contextual shifts

Figure 12: Access-control windows that expand or contract unpredictably based on chaotic entropy samples, thereby preventing adversarial timing analysis or session hijacking.

Figure 13: A zero-retention identity verification process comprising cryptographic validation of an identity document, user-interaction validation, and device-state attestation, resulting in a non-reversible verification proof stored solely on the user-controlled vault.

Figure 14: In some embodiments, trust evaluation is split between a local reflex trust engine running on the PIV and a cloud-based cognitive trust engine implementing the full Love's Algorithm. The local engine performs any combination of cryptographically verifiable device-state, user-interaction, or context-state indicators. The cloud engine performs:

• multi-dimensional trust scoring

• distributed node attestation

• environmental fingerprinting

• large-scale behavioural entropy analysis

• PQC key lifecycle management

• global anomaly correlation

The two layers exchange trust signals without sharing personal data, enabling adaptive, unpredictable authentication pathways.

Figure 15: The system introduces fractal entropy–controlled authentication pathways, wherein:

• the order, timing, number, and type of authentication steps

• vary non-deterministically

• based on fractal entropy, trust score, behavioural variance, and environmental context.

Authentication may require any combination of authentication factors selected from any combination of user-interaction validation, device-state verification, cryptographic proofing, or environmental consistency checks. Because authentication sequences mutate based on chaotic timing values, adversaries cannot predict or replicate them.

Figure 16: Optional user-controlled distress-response mechanisms that suppress, invalidate, or falsify identity output under coercive or abnormal interaction conditions.

Claims

Claim 1: A system comprising a fractal entropy generator, behavioural biometric engine, anomaly detection engine, device attestation module, post-quantum cryptography subsystem, and adaptive trust engine, wherein said trust engine computes a dynamic trust score used to continuously govern access rights and cryptographic key management.

Claim 2: The system of claim 1 wherein the fractal entropy generator produces chaotic timing windows that trigger cryptographic key rotations, authentication prompts, or access modifications.

Claim 3: The system of claim 1 wherein interaction-derived behavioural entropy is analysed in real time to generate an identity validity signal for trust evaluation.

Claim 4: The system of claim 1 wherein device attestation includes cryptographic verification of device-state, environment-state, or context-state indicators.

Claim 5: The system of claim 1 wherein trust values decay or escalate continuously based on behavioural deviation, anomaly detection, and environmental drift.

Claim 6: The system of claim 1 wherein the trust score dynamically initiates post-quantum key-pair regeneration, isolation of nodes, or multi-factor authentication escalation.

Claim 7: A method of preventing adversarial modelling by introducing fractal or chaotic variability to authentication timing, key scheduling, and identity verification sequences.

Claim 8: An adaptive authentication system wherein multiple authentication factors are required in varying combinations determined by fractal entropy and dynamic trust scoring.

Claim 9: A distributed system capable of autonomously isolating nodes, terminating sessions, or regenerating cryptographic keys based on trust-engine outputs. Claim

10: A continuous identity verification method comprising: (a) analysing behavioural biometrics; (b) generating fractal entropy values; (c) computing a trust score; and (d) modifying access permissions and cryptographic states accordingly.

Claim 11: A hardware identity vault comprising a secure element, fractal entropy generator, behavioural biometric collector, and encrypted storage, wherein a time-varying cryptographic key is derived using behavioural entropy, fractal entropy, and anomaly detection signals.

Claim 12: The system of claim 11 wherein personal identity information is stored exclusively on said hardware vault and never externally retained.

Claim 13: A zero-retention identity verification method comprising:
(a) obtaining cryptographic proof of identity;
(b) performing user-interaction consistency validation;
(c) generating a verification proof hash stored solely on a hardware vault;
(d) discarding all raw verification inputs.

Claim 14: A dual-layer trust system comprising a local reflex trust engine embedded in a hardware device and a cloud-based adaptive trust engine, wherein trust calculations are shared across both layers without transmitting personal identifiable information.

Claim 15: A chaotic authentication pathway governed by fractal entropy and trust scores, wherein authentication requirements change unpredictably across sessions.

Claim 16: A coercion-resistant identity system comprising user-controlled distress-response pathways that suppress, invalidate, or falsify identity output under coercive or abnormal interaction conditions.

Claim 17: A session-control subsystem wherein session parameters, re-authentication timings, and privilege levels are dynamically adjusted based on trust trajectories and entropy-driven timing.

Claim 18: A security posture-scaling subsystem that modifies access constraints, verification demands, and cryptographic enforcement based on continuous trust-evaluation.

Claim 19: An access-control mechanism wherein the allowable authentication or interaction timeframe varies unpredictably based on chaotic entropy.

Claim 20: A unified trust-fabric system integrating entropy-driven behaviour analysis, device and environment attestation, post-quantum key lifecycle governance, and distributed enforcement within a continuous adaptive trust engine.

Abstract

The invention provides a system and method for adaptive trust orchestration across digital infrastructures using a combination of fractal entropy, behavioural biometrics, device attestation, and post-quantum cryptographic key management. The system continuously evaluates a user or machine's identity by generating a multi-dimensional trust score derived from behavioural indicators, hardware authentication, environmental context, anomaly detection, and chaotic entropy signals. This trust score dynamically governs access permissions, authentication requirements, session controls, and cryptographic key rotations. The invention introduces a fractal entropy generator for producing non-deterministic timing windows, enabling unpredictable cryptographic life-cycle events and thwarting adversarial modelling. A behavioural-biometric engine derives real-time identity signatures from human and device interaction patterns. A post-quantum cryptography module provides lattice-based key exchange, digital signatures, and key life-cycle governance. An adaptive orchestration layer adjusts trust states continuously, enabling rapid escalation, isolation, or revocation of access rights. The invention is suitable for distributed computing environments, secure cloud infrastructures, identity systems, access-control systems, and autonomous security frameworks. It provides quantum-resistant, behaviourally adaptive, self-healing security architecture.