Behavioural Entropy-Based Key Derivation System

Technical Field

The invention relates to cryptography, identity verification, behavioural modelling, entropy generation, post-quantum key derivation, privacy-preserving authentication, and trust orchestration in distributed systems.

Background

Conventional authentication systems depend on static keys, passwords or stored biometric records, each vulnerable to theft, replay, coercion, or spoofing. Behavioural biometrics exist but typically require storage of sensitive patterns, exposing users to privacy and security risks. Cryptographic systems seldom integrate behavioural entropy in key generation, and post-quantum preparations require new forms of entropy and identity binding to resist future computational threats. There is a need for a key-derivation model that transforms behavioural indicators into non-reversible entropy without retention, enabling privacy-preserving, contextually-bound, user-specific cryptographic keys.

Summary of the Invention

The invention provides a behavioural entropy-based key derivation system that converts behavioural indicators into non-reversible entropy values. Behavioural inputs including micro-timing signatures, pressure variance, interaction rhythms, dynamic motion characteristics, tremor distribution and contextual response behaviours are fused with fractal-entropy modulation and device attestation signals. These combined values form an entropy state used to generate cryptographic keys in post-quantum schemes or classical-hybrid schemes. The system performs zero-retention processing: behavioural indicators are immediately transformed into entropy values that cannot be reverse-engineered. The derived keys are unique per user, per context and per session. The system integrates with trust-fusion engines and portable identity devices disclosed in GB2520368.8 and GB2520379.5.

Detailed Description

Behavioural Entropy Inputs

The system receives behavioural indicators including:

1. Micro-timing intervals during interaction.
2. Pressure variability across input events.
3. Tremor distribution signatures.
4. Motion-path micro-dynamics.
5. Interaction rhythm consistency.
6. Response-time deviations under contextual variation.
7. Micro-gesture modulation patterns.
8. Short-term adaptation dynamics.

Raw values are not stored. Sampling occurs in volatile memory only.

Pre-Processing Layer

Behavioural indicators undergo:
- normalisation,
- noise filtration,
- fractal-pattern decomposition,
- gesture-field segmentation,
- entropy extraction transforms.

Outputs form non-reversible behavioural-entropy values.

Fractal-Entropy Modulation

A fractal-entropy generator introduces additional device-anchored and environment-bound entropy. Modulation blends:
- behavioural entropy,
- fractal entropy,
- context-attestation signatures.

This forms a composite entropy field used in key derivation.

Contextual Attestation Integration

Environmental and device-state indicators include:
- temperature variance,
- acceleration signatures,
- location randomness markers,
- posture-stability patterns,
- device-state proofs.

These bind keys to specific contexts and prevent replay.

Entropy Fusion Engine

The system fuses:
- behavioural entropy,
- fractal entropy,
- attestation entropy,
- anomaly-adjusted modifiers.

Fusion produces a high-entropy composite state.

Key Derivation Process

The composite entropy state is processed using:
- post-quantum key encapsulation mechanisms,
- lattice-based key scheduling,
- or hybrid classical-PQC derivation sequences.

Keys are unique per behavioural event, per session, or per device-context pair.

Zero-Retention Guarantee

Raw behavioural signals are discarded immediately after transformation.
No biometric or behavioural pattern is stored, transmitted or made recoverable.

Identity Binding

The derived keys serve as proof of behavioural presence and identity continuity. They cannot be used to reconstruct the underlying behaviour.

Session Establishment

The system generates:
- session keys,
- authentication signatures,
- identity proofs,
- trust values for trust-fusion engines.

Coercion-Resistance

Abnormal behavioural entropy (stress signatures, rhythm collapse, tremor anomalies) triggers:
- restricted key output,
- degraded authentication state,
- session denial or emergency revocation.

Integration with Related Systems

The system complements:

- the multi-layer trust orchestration of GB2520368.8,
- the portable PQ identity device of GB2520379.5.

Claims

Claim 1

A behavioural entropy-based key derivation system comprising a pre-processing layer, an entropy extraction module, a fractal-entropy generator, a context-attestation module and a key derivation engine, wherein behavioural indicators are transformed into non-reversible entropy values used to derive cryptographic keys without storing raw behavioural data.

Claim 2

The system of Claim 1 wherein behavioural indicators comprise micro-timing signatures, pressure variability, tremor distribution, motion micro-dynamics and interaction rhythm patterns.

Claim 3

The system of Claim 1 wherein the pre-processing layer performs normalisation, noise filtration, gesture-field segmentation and fractal decomposition.

Claim 4

The system of Claim 1 wherein the fractal-entropy generator introduces device-anchored non-deterministic values to modulate behavioural entropy.

Claim 5

The system of Claim 1 wherein the context-attestation module provides environmental and device-state indicators incorporated into the entropy fusion process.

Claim 6

The system of Claim 1 wherein the entropy fusion engine combines behavioural entropy, fractal entropy and attestation entropy into a composite entropy field.

Claim 7

The system of Claim 1 wherein the key derivation engine applies post-quantum key generation processes to the composite entropy field.

Claim 8

The system of Claim 1 wherein cryptographic keys are unique per behavioural event, per session or per device-context pairing.

Claim 9

The system of Claim 1 wherein raw behavioural indicators are discarded immediately after entropy transformation in a zero-retention process.

Claim 10

The system of Claim 1 wherein derived keys bind identity by behavioural presence without permitting reconstruction of original behavioural data.

Claim 11

The system of Claim 1 wherein anomaly-based behavioural entropy triggers restricted authentication output or session denial.

Claim 12

The system of Claim 1 wherein entropy-derived keys form trust-values integrable with a multi-layer trust orchestration system.

Claim 13

The system of Claim 1 wherein the entropy fusion engine integrates anomaly indicators to adjust trust weighting.

Claim 14

The system of Claim 1 wherein session keys and identity proofs are generated based on dynamic behavioural-entropy variation.

Claim 15

The system of Claim 1 referencing GB2520368.8 and GB2520379.5 as related prior art by the same inventor.

Abstract

A system for deriving cryptographic keys from behavioural entropy signals without storing biometric or raw behavioural data. Behavioural indicators including timing patterns, micro-movements, interaction consistency, pressure variance and contextual response signatures are transformed into non-reversible entropy values used for cryptographic key derivation, identity verification and secure session establishment. The invention integrates fractal-entropy modulation, contextual attestation and post-quantum cryptographic processes. The system operates without the retention of sensitive behavioural material, enabling privacy-preserving identity generation and dynamic key cycles resilient to spoofing and coercion. The invention relates to GB2520368.8 and GB2520379.5 as prior art by the same inventor.