System and Method for Emotional Coherence-Based Biometric Cryptographic Key Generation (COHERENCE™ Framework)

Inventor: Justin Bilyeu

April 2025

Abstract

An emotional biometric cryptographic key system is disclosed, which dynamically generates and manages encryption keys based on a user's physiological and emotional coherence. Multi-modal biometric inputs, including electroencephalogram (EEG) brainwave synchrony and heart rate variability (HRV) coherence, are fused to produce a cryptographic key when the user's mind-heart state is coherent. The keys are inherently ephemeral and collapse (become invalid) upon detecting emotional trauma or loss of coherence, as indicated by a sudden increase in an emotional turbulence metric (e.g., curl of an emotional field exceeding a threshold). A symbolic artificial intelligence (AI) context engine provides a semantic emotional embedding $h(t)$ that modulates key generation parameters and validity duration based on the user's emotional context. In one embodiment, the system (branded COHERENCE™) enforces "ephemeral identity," meaning authentication persists only while emotional synchrony is maintained. Optionally, the cryptographic keys may control quantum cryptographic processes, including biologically entangled quantum gates, to further bind the key to the user's physiological state. This Continuation-in-Part improves upon prior EEG-based key methods by introducing multi-modal resonance inputs, trauma-triggered key revocation, semantic context awareness, and quantum coupling for enhanced security and ethical, consent-based access control.

Claims

1. A method for generating and managing a cryptographic key based on emotional biometric coherence, comprising:
    - acquiring EEG brainwave signals and HRV signals from a user;
    - computing a coherence value representing real-time synchrony;
    - generating a cryptographic key from a fusion of EEG and HRV data when coherence exceeds a threshold;

- monitoring for trauma indicators based on $\mathrm{curl}(\mathcal{E}) > \epsilon$;
- invalidating the key if trauma or incoherence is detected;
- wherein the key is ephemeral and only valid during continuous physiological coherence.

2. The method of claim 1, further comprising modulation by a symbolic emotional context signal $h(t)$.

3. The method of claim 2, wherein $h(t)$ is derived from a symbolic AI model, and modifies λ or key duration.

4. The method of claim 1, wherein key generation comprises:

    - computing $K = H(\mathrm{HRV}_{\mathrm{sync}} \oplus \nabla\mathcal{E})$.

5. The method of claim 1, wherein trauma is detected via changes in HRV, EEG, or symbolic context.

6. The method of claim 1, wherein the key governs authentication for a secure system, and session collapses upon loss of coherence.

7. A system implementing the above method, comprising:

    - biometric sensors (EEG, HRV);
    - a processor computing coherence;
    - symbolic AI engine for $h(t)$;
    - key management system enforcing collapse.

8. The system of claim 7, wherein coherence thresholds, time-to-live, or trauma sensitivity are adjusted by $h(t)$.

9. The system of claim 7, further comprising a quantum subsystem, wherein biometric coherence sustains quantum entanglement.

10. The system of claim 9, wherein EPS-QC coupling collapses quantum keys upon emotional incoherence.

References

1. IBM, U.S. Patent No. 9,049,499 B2 (June 2, 2015).

2. COHERENCE™ White Paper (April 2025).