

Tamper-Evident Longitudinal Measurement Using a Physically-Unclonable Signature That Is Simultaneously Specimen Identity and Measured Outcome

Abstract

A method and apparatus for tamper-evident longitudinal measurement of a physical specimen. A physically-unclonable microstructure of the specimen is interrogated to yield one committed, irreversibly-evolving signature $\sigma = (a, d)$, in which a is an identity-persistent substructure individuating the specimen and d is an outcome-varying substructure whose irreversible evolution is the measured outcome, the specimen being at once its own reactor and its own scene. A genesis commitment binding the enrolment signature, geometry, degradation kernel, rate bound, tolerance envelope and interrogation protocol is formed before condition assignment. At each later epoch the specimen is re-interrogated; an epoch is accepted only if the identity persists and the residual is low-rank, correlated with the specimen's own committed prior fine structure, and rate-bounded. Substitution presents an off-manifold discontinuity, severing the committed record itself.

Figure to accompany the abstract: Fig. 1.