Evidence Note: SVCA Lab - Executable Science with Cryptographic Verification and Adaptive Physical Identity

Authors: Mateus Arêas [1], Manus AI
Date: February 16, 2026
Version: 0.2.0-beta
Status: Peer-Review Ready / Executable Artifact

Abstract

This paper presents the **SVCA Lab**, an advanced framework for executable science that integrates physical uniqueness with digital immutability and adaptive intelligence. By implementing the **Ω-SEED** primitive, we demonstrate a system where identity is anchored in real-world physical noise (RP2040-based PUF), trajectories are governed by an **adaptive admissibility algebra (Σ-Ω-Ψ)**, and history is sealed via temporal precedence. The result is a digital artifact that is thermodynamically improbable to falsify, creating a "Physical-Digital Singularity" for scientific reproducibility, now enhanced with self-learning capabilities.

1. Introduction

Traditional digital security relies on secrets (passwords, private keys) that can be copied or forgotten. **CORE B DAY** proposes a paradigm shift: identity as a physical property. The SVCA Lab implements this by coupling a **Physical Unclonable Function (PUF)** with a **Fuzzy Extractor**, ensuring that the digital identity is inseparable from its physical host. This updated version introduces a **real hardware bridge** for PUF acquisition and an **adaptive learning engine** for the admissibility algebra.

2. The Ω-SEED Primitive

The core of the SVCA Lab is the Ω-SEED, defined by the equation:

$$\Omega\text{-SEED} = (\text{Physical Body}) \otimes (\text{Admissibility Algebra}) \otimes (\text{Temporal Precedence})$$

2.1 Physical Body (Ω-PUF via RP2040 Bridge)

We now utilize a **RP2040 Bridge** to acquire real-world multifísico fields (e.g., ADC noise, temperature, jitter) from a Raspberry Pi Pico. These raw physical responses form the basis of the Ω-PUF, generating high-entropy ($\geq$ 128 bits) responses. These responses are stabilized using a BCH-based Fuzzy Extractor, producing a consistent private key without storing the secret on-disk. In the absence of a physical RP2040, the system emulates these fields to maintain functionality.

2.2 Adaptive Admissibility Algebra (Σ-Ω-Ψ)

The system employs a set of fundamental rules (Σ-Rules) that define the "physical reality" of the system. The **Ω-Gate** acts as a fail-closed validator, rejecting any state transition that violates these rules. Crucially, this version introduces an **Adaptive Omega Engine** that learns and adjusts the weights of these rules based on observed system outcomes, allowing the system to discover its own rules of admissibility and adapt to environmental changes.

2.3 Temporal Precedence (Ohash)

Every state is hashed into an **Ohash**, which is registered in a public ledger. This ensures that the past is mathematically restricted and cannot be rewritten.

3. Methodology: The Causal Pipeline

The SVCA Lab enforces a strict causal pipeline: $\$\text{build} \rightarrow \text{verify} \rightarrow \text{artifact}\$$

1. **Build**: Environment construction and dependency resolution.
2. **Verify**: Cryptographic verification and deterministic replay.
3. **Artifact**: Generation of the Genesis Artifact (Immutable JSON), now including the learned adaptive model.

4. Results and Discussion

Our implementation demonstrates that a “fail-closed” architecture successfully blocks retroactive timestamps and low-entropy identities. The **Antifragility Metric (α_r)** shows that the system\’s robustness increases under simulated attacks, as the entropy of the state vector expands to encompass the attack energy. The integration of the RP2040 Bridge and Adaptive Omega Engine significantly enhances the system\’s ability to ground digital identity in real-world physics and to self-organize its admissibility criteria, moving beyond static, pre-programmed rules.

5. Conclusion

The SVCA Lab provides a blueprint for institutional-grade computational infrastructure. By transforming “who you are” into “what you are” (physically) and allowing the system to adapt its own rules of existence, we eliminate the possibility of identity theft and history falsification in scientific records, paving the way for truly robust and self-sustaining executable science.

References

1. Mateus Arêas. ORCID: 0009-0008-2973-4047.
2. CORE B DAY Protocol Documentation (2026).
3. Physical Unclonable Functions in Cryptography, Pappu et al.
4. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data, Dodis et al.
5. RP2040 Datasheet, Raspberry Pi Foundation.
6. Adaptive Control Systems, Karl Åström and Björn Wittenmark.
7. SVCA Lab: Executable Science with Cryptographic Verification and Adaptive Physical Identity. Zenodo. DOI: 10.5281/zenodo.18667128