Information-Dispersive Hardness under Rule-Constrained Interfaces

Abstract

We study a form of hardness that arises not from the non-existence of solutions, but from the structure of the rule systems under which solutions are verified. The central phenomenon, which we call *information-dispersive hardness*, occurs when admissible operations are efficiently computable and verifiable under a fixed rule system, yet no procedure permitted by those same rules can recover the underlying generative structure. This perspective separates existence from recoverability in an NP-style manner and provides a unifying structural explanation for cryptographic hardness, local verification systems, and related no-go phenomena.

1 Rule Systems as First-Class Objects

We treat rules, rather than functions or algorithms in isolation, as the primary objects of analysis.

Definition 1 (Rule System). *A rule system Θ consists of:*

- *a set of admissible objects $\mathcal{O}_\Theta$;*
- *a set of admissible operations $\mathcal{F}_\Theta$ executable under the rules;*
- *a verification predicate $\mathcal{V}_\Theta$ specifying admissibility.*

All notions of feasibility, computability, and recoverability in this work are explicitly relative to a fixed rule system Θ. No operation is considered unless it is derivable from, or explicitly added to, Θ.

This shift is deliberate: hardness is not viewed as an intrinsic property of a function, but as a relational property between an operation and the rules under which it is executed.

2 Verification Semantics and Witness Sets

Let $V_\Theta(x, w) \in \{0, 1\}$ be a deterministic polynomial-time verification predicate permitted by Θ. For each instance x, this induces a witness set

$$W_\Theta(x) = \{\, w \mid V_\Theta(x, w) = 1 \,\}.$$

Observation 1. *Verification under Θ has set-valued semantics: it establishes membership in $W_\Theta(x)$, but does not identify a unique witness.*

This observation is elementary but foundational. In particular, the verification interface answers the question “is this admissible?”, not “how was this generated?”

3 Rule-Internal and Rule-External Procedures

Definition 2 (OWF-Induced NP Relation under a Rule System)**.** *Let Θ be a rule system whose admissible operations $\mathcal{F}_\Theta$ include a family of forward-efficient mappings*

$$g_\lambda : \{0,1\}^{n(\lambda)} \to \{0,1\}^{m(\lambda)},$$

generated by a polynomial-time procedure.

Assume that inversion of g_λ is infeasible for any probabilistic polynomial-time rule-internal procedure under Θ (i.e., g_λ is one-way relative to Θ).

Define the induced NP verification relation by

$$R^{(g)}_\lambda(x, w) \;=\; \mathbf{1}[\, g_\lambda(w) = x \,],$$

and the corresponding induced language by

$$L^{(g)}_\lambda \;=\; \{\, x \mid \exists w\; R^{(g)}_\lambda(x, w) = 1 \,\} \;=\; \mathrm{Im}(g_\lambda).$$

Rule-internal procedures describe what is possible within the verification interface. Rule-external procedures introduce additional generative capability by augmenting the rule system.

This distinction is not about computational power, but about rule access.

Definition 3 (Rule-Internal Constructibility)**.** *Let Θ be a rule system and let $f \in \mathcal{F}_\Theta$ be an admissible operation mapping witnesses to instances.*

We say that f is rule-internally constructible relative to Θ *if there exists a probabilistic polynomial-time rule-internal procedure $\mathcal{A}$ such that, for all admissible instances x in the image of f,*

$$\Pr\bigl[f(\mathcal{A}(x)) = x\bigr] \geq \frac{1}{\mathrm{poly}(|x|)}.$$

4 Information-Dispersive Operations

We now formalize the central notion of this work.

Definition 4 (Information-Dispersive Operation)**.** *Let Θ be a rule system and let $f \in \mathcal{F}_\Theta$ be an admissible operation mapping witnesses to instances.*

We say that f is information-dispersive relative to Θ *if:*

(i) f is efficiently computable using only operations permitted by Θ;

(ii) consistency with respect to f is decidable under the verification predicate $\mathcal{V}_\Theta$;

(iii) no rule-internal procedure under Θ can invert f with non-negligible probability.

Observation 2. *Information-dispersive hardness is not a property of functions in isolation, but of functions viewed relative to a fixed rule system.*

In this sense, the same function may be dispersive under one rule system and recoverable under another.

5 Existence Without Recoverability

We now state the central conjecture.

Conjecture 1 (Existence Without Recoverability under Rule-Constrained Interfaces)**.** *Let $\Phi : \mathcal{S} \to \mathcal{I}$ be an interface map induced by a rule system Θ, and define fibers $\mathcal{S}_i = \Phi^{-1}(i)$.*

We conjecture that, generically, such interfaces exhibit the following NP-style phenomenon:

*(i) (*Existence*) For every realizable interface datum $i \in \Phi(\mathcal{S})$, there exists at least one $s \in \mathcal{S}$ such that $\Phi(s) = i$.*

*(ii) (*Non-recoverability*) No rule-internal procedure under Θ can uniformly recover a representative $s \in \mathcal{S}_i$ from i with non-negligible success.*

*(iii) (*Structured exceptions*) Recoverability becomes feasible only when the rule system is augmented with rule-external structure, such as trapdoors or highly regular auxiliary information.*

This conjecture concerns recoverability relative to a fixed rule system and interface. Non-recoverability does not imply non-existence of generative structure, but reflects the structural limits imposed by rule-internal access.

Why NP-style? The conjecture is NP-style because it separates existence from construction. As in **NP**, admissibility is verifiable given a witness, and existence is asserted, while uniform recovery of such witnesses is obstructed by the rules governing access.

6 Illustrative Domains

We briefly indicate how the same structure appears across several domains.

6.1 Cryptography

Public-key cryptography exposes a verification-complete rule-internal interface, while private keys supply rule-external structure enabling construction. Hardness arises from the non-recoverability of generative structure under public rules.

6.2 PCP and Local Verification

PCP systems allow global consistency to be verified via local checks. The induced verification interface is information-theoretically incapable of recovering the underlying proof, illustrating information-dispersive hardness without computational assumptions.

6.3 Quantum Measurement

Quantum measurement provides access to statistical correlations via a fixed measurement interface. When the accessible measurements are not informationally complete, the mapping from quantum states to observable statistics is non-invertible. Entanglement exemplifies verification-complete but generation-incomplete structure.

7 Scope

This work does not propose new algorithms, cryptographic primitives, or physical theories. It does not resolve the P versus NP question, nor does it modify quantum mechanics. Its contribution is structural: it isolates a common interface-level obstruction underlying diverse hardness and no-go phenomena.