# Rule-Internal Verification and Interface Non-Invertibility

**Abstract**

This note summarizes a unifying structural perspective that arises across complexity theory, cryptography, proof systems, and quantum theory. The central distinction is between *rule-internal* verification interfaces and *rule-external* generative structure. We show that many celebrated hardness and no-go results can be understood as instances of a single phenomenon: interface non-invertibility caused by dimensional or informational compression at the verification interface. The contribution is not a new domain-specific theorem, but a formal framework that makes this shared obstruction explicit.

## 1 Rule-Based Verification Framework

We fix a public rule system $\Theta$. A verification predicate

$$V_\Theta(x, w) \in \{0, 1\}$$

runs in deterministic polynomial time. It induces a set-valued semantics

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

**Definition 1** (Rule-Internal and Rule-External Procedures)**.** A *rule-internal* algorithm is any probabilistic polynomial-time algorithm whose access is restricted to the public description of $\Theta$ and evaluation of $V_\Theta$, and whose output depends only on $x$ and internal randomness.

A *rule-external* algorithm is an algorithm that additionally receives auxiliary structure $t$ not derivable from the public verification semantics (e.g. trapdoors, generative rules, or provenance information).

Rule-internal procedures correspond to what an observer or verifier can do within the accepted rules of the system; rule-external procedures represent additional generative structure.

## 2 Verification vs Construction

**Proposition 1** (Verification is Rule-Internal)**.** *For any $(x, w)$, membership in $W_\Theta(x)$ is decidable in deterministic polynomial time by evaluating $V_\Theta(x, w)$.*

**Proposition 2** (Construction May Be Rule-External)**.** *If for every PPT rule-internal algorithm $\mathcal{A}$,*

$$\Pr[\mathcal{A}(x) \in \mathcal{W}_\Theta(x)] \leq \mathrm{negl}(|x|).$$

*then any procedure that constructs a witness in $W_\Theta(x)$ with non-negligible probability must rely on rule-external structure.*

These propositions isolate the core asymmetry: verification is closed under the public rules, while construction may fundamentally require additional structure.

# 3 Interface Non-Invertibility

We abstract verification interfaces as maps from hidden generative objects to observer-accessible data.

**Definition 2** (Interface Map)**.** Let $\mathcal{S}$ be a space of underlying structures (states, proofs, or witnesses) and $\mathcal{I}$ a space of observable data. An interface is a map

$$\Phi : \mathcal{S} \longrightarrow \mathcal{I}.$$

The interface is *invertible* if $\Phi$ is injective, and *non-invertible* otherwise.

**Theorem 3** (Interface Non-Invertibility)**.** *If the interface $\Phi$ factors through a projection whose image has strictly lower dimension or information content than $\mathcal{S}$, then $\Phi$ is non-invertible: distinct underlying structures induce identical observable behavior.*

*Proof.* Any such projection identifies multiple points in $\mathcal{S}$. Thus $\Phi(s) = \Phi(s')$ for some $s \neq s'$, and $\Phi$ cannot be injective. □

This theorem is elementary but fundamental: it explains why verification interfaces can be complete for admissibility while incomplete for generation.

# 4 Canonical Instances

## 4.1 Quantum Measurement Interfaces

A quantum state $\rho$ is accessed via measurement operators $\mathcal{M} = \{M_i\}$, yielding expectation values

$$\Phi_Q(\rho) = \{\mathrm{Tr}(\rho M_i)\}_i.$$

The interface $\Phi_Q$ is invertible if and only if $\mathcal{M}$ is informationally complete. In typical experimental settings it is not, and the measurement interface is therefore non-invertible. Quantum entanglement exemplifies this phenomenon: correlations are verifiable, but the global generative structure cannot be reconstructed from the interface.

## 4.2 PCP Local Verification

A PCP proof $\pi \in \{0,1\}^N$ is accessed by a verifier that queries $O(1)$ bits per random seed $r$. The induced interface

$$\Phi_P(\pi) = \{\Pr[\text{Verifier accepts with randomness } r]\}_r$$

is non-invertible by an information-theoretic counting argument. Distinct proofs induce identical local verification behavior.

## 4.3 Cryptographic Hardness

Public-key cryptography fits the same pattern. Public rules define a verification-complete interface, while secret keys provide rule-external structure enabling construction. Hardness arises precisely from the non-invertibility of the public interface.

## 5 Interpretive Observation

*Observation* 1. Across these domains, apparent hardness or non-classical behavior is not caused by a lack of structure, but by the deliberate separation between rule-internal verification interfaces and rule-external generative structure. What cannot be reconstructed is not absent; it lies outside the accessible interface.

**Conjecture 4** (Internal–External Rule Separation as a Structural Principle)**.** *Across multiple foundational theories—including computational complexity, cryptography, proof systems, and quantum mechanics—there appears a recurring structural distinction between rule-internal verification interfaces and rule-external generative structure.*

*We conjecture that this separation is not accidental, but reflects a general organizational principle: systems that admit efficient, stable verification necessarily restrict access to their full generative structure, rendering the verification interface non-invertible.*

*Under this view, distinctions such as* $\mathbf{P}$ *versus* $\mathbf{NP}$*, public-key cryptography, proofs without recoverability, and quantum entanglement arise as theory-specific manifestations of the same abstract rule-separation phenomenon, instantiated at different levels of description.*

**Conjecture 5** (Observer Interface Non-Invertibility)**.** *Let* $\mathcal{S}$ *be a space of underlying structures and let* $\mathcal{I}$ *be a space of observer-accessible data. Let*

$$\Phi : \mathcal{S} \longrightarrow \mathcal{I}$$

*be a map induced by a fixed rule system* $\Theta$ *governing admissible observations.*

*Assume that* $\Theta$ *specifies a verification-complete interface in the sense that, for any* $s \in \mathcal{S}$*, relational properties of* $s$ *expressible in terms of* $\mathcal{I}$ *are decidable via* $\Phi(s)$ *using only the rules in* $\Theta$*.*

*We conjecture that, generically, such observer interfaces are non-invertible: there exist distinct* $s, s' \in \mathcal{S}$ *with*

$$\Phi(s) = \Phi(s').$$

*Equivalently, the rule system* $\Theta$ *induces an information-compressing projection from* $\mathcal{S}$ *to* $\mathcal{I}$*, under which reconstruction of the full generative structure from observer-accessible data is not possible.*

*Under this conjecture, limits on explanation arise from structural non-invertibility of the observation interface rather than from lack of underlying structure or insufficient computational power.*

**Conjecture 6** (Existence Without Recoverability under Rule-Constrained Interfaces)**.** *Let* $\mathcal{S}$ *be a space of generative structures and* $\mathcal{I}$ *a space of observer-accessible data. Let*

$$\Phi : \mathcal{S} \longrightarrow \mathcal{I}$$

*be an interface map induced by a fixed rule system* $\Theta$*, and define the 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* $i \in \mathcal{I}_0 := \Phi(\mathcal{S})$*, there exists at least one* $s \in \mathcal{S}$ *such that* $\Phi(s) = i$*. Equivalently, a selector (right-inverse) exists non-constructively on* $\mathcal{I}_0$*.*

*(ii)* Non-recoverability under rules. *There is no rule-internal probabilistic polynomial-time procedure that can uniformly obtain such a selector or recover a representative* $s \in \mathcal{S}_i$ *from* $i$ *with non-negligible success. Recoverability fails relative to the rule system* $\Theta$ *and the interface* $\Phi$*, despite existence.*

*(iii)* Structured exceptions. *Recoverability becomes feasible only upon augmenting the rule system with additional rule-external structure (e.g., trapdoors or highly regular auxiliary information) that effectively alters the interface. Such exceptions are non-generic and correspond to deliberately engineered or highly constrained regimes.*

*This conjecture concerns recoverability* relative to a fixed interface and rule system. *Non-recoverability is not a claim about non-existence of generative structure, but about the structural impossibility of obtaining it through rule-internal access alone.*

**Why NP-style?** The conjecture is NP-style because it separates *existence* from *recoverability*.

In classical complexity theory, a language $L$ belongs to **NP** if membership admits a witness whose validity is efficiently verifiable, even if no efficient procedure is known for constructing such a witness. The defining feature is not hardness of verification, but the gap between existence and construction.

The interface setting exhibits the same structure. For each observable datum $i \in \mathcal{I}_0$, existence asserts

$$\exists\, s \in \mathcal{S} \quad \Phi(s) = i,$$

while non-recoverability asserts that no rule-internal procedure can obtain such an $s$ from $i$ with non-negligible success. Thus the conjecture formalizes an $\exists$-statement without an accompanying search procedure, directly mirroring the semantic core of **NP**.

In this sense, the conjecture is NP-style not by complexity classification, but by logical form: existence is guaranteed, verification is well-defined, and construction is obstructed by the interface.

## 6 Scope and Non-Claims

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 identifies a shared interface-level obstruction underlying diverse no-go and hardness results, and provides a uniform language in which they can be compared.