CNVS

Formal Mathematical Synthesis

Version 6.4

This paper is intended to be self-contained with respect to its formal definitions, assumptions, lemmas, and theorems.

Author
Massimo Comitato

GENERAL INDEX

Abstract

This paper introduces closed native verification systems (CNVS), a formal class of verification systems in which raw structural membership in a candidate state is primitive, whereas admissibility, accepted state validity, and state evolution are verification-dependent. Thus, an element may structurally belong to a candidate configuration independently of its current verification status; however, only candidate states satisfying local admissibility, relational consistency, and global invariant constraints are admitted as valid CNVS states.

The theory combines a typed structural universe, a context-preserving and type-compatible recursive decomposition, random assignment of non-uniform fragments, limited verifier knowledge, and global invariant checking, first enforcing data convergence in a local verification environment.

External verifiers are not provided with the internal declared payload $d \in D_\sigma$; they receive only a task specification and independently measure the assigned attribute, the result of which is internally compared to the value maintained by the system.

CNVS therefore does not perform syntactic slicing of the payload. The decomposition generates atomic evaluation primitives (which have the local semantics to be computable via a Local Verification function) and injects them into a randomized routing topology.

The fragment is not the payload, but a measurement grid that is randomly distributed along the graph and that requires a convergent observation with respect to the unknown payload.

Lemma 10 formalizes bounded topological leakage: the routing network is not required to reveal zero information about the payload, but any semantic information leaked through topology and metadata must remain quantitatively bounded and insufficient for deterministic reconstruction.

A conditional probabilistic theorem limits unauthorized reconstruction through weighted adversarial information and exponential concentration inequalities. An asymptotic scaling theorem shows that security can increase as the system expands in the presence of explicit assumptions.

The technical difficulty of reconstruction outside the system arises from the strictly local knowledge available to each verifier.

1. Primitive Domains and Typed Structural Universe

Let $B = \{0, 1\}$ and let B^* be the set of all finite binary strings.

Let $\boldsymbol{\mathcal{T}}$ be a strictly finite set of structural types.

To guarantee semantic consistency and type preservation, we define the primitive domains not as flat sets, but as families of sets indexed by their structural type $\sigma \in \boldsymbol{\mathcal{T}}$

- $Id_\sigma \subseteq B^*$: the space of identifiers for type σ .
- $D_\sigma \subseteq B^*$: the space of declared data payloads structured according to type σ. An element $d \in D_\sigma$ represents a candidate assertion, digital archive, structured datum, object specification, or cryptographic record submitted by one or more users, entities, or system agents to the CNVS layer for verification.
- $At_\sigma \subseteq B^*$: the space of attribute classes for type σ .
- $Obs_\sigma \subseteq B^*$: the space of externally reported values for type σ .

Let P be a finite set of logical properties, and let $\mathcal{P}(P)$ denote the set of all its strictly finite subsets.

To model the absence of data without introducing domain collisions or ambiguity with the empty string $\varepsilon \in B^*$, we introduce a distinguished element $\perp \notin B^*$. We define the observational domain as a disjoint union:

$Obs^{\perp}_\sigma \triangleq Obs_\sigma \uplus \{\perp\}$

where the ⊥ element rigorously denotes the absence of an external observation at non-terminal structural levels.

We define the Structural Universe $\mathcal{S}$ as a dependent sum (Sigma-type) over the set of structural types $\mathcal{T}$:

(1)

$\mathcal{S} \triangleq \Sigma_{\sigma \in \mathcal{T}} (Id_\sigma \times D_\sigma \times At_\sigma \times Obs^{\perp}_\sigma \times \mathcal{P}(P))$

Consequently, each structural state $s \in \mathcal{S}$ assumes the dependent form:

$s = \langle \sigma. (id, d, a, obs, p) \rangle$

This construction guarantees ontologically that the identifier, the payload, and the attributes are intrinsically bound to their specific structural type σ at instantiation, preventing type-mismatch vulnerabilities prior to any verification phase.

2. State Space and Verification Signatures

A system state at time t is formally defined as a tuple:

(2)

$S(t) = \langle E(t), R(t), C(t) \rangle$

where:

- $E(t) \in \mathcal{P}_{fin}(\mathcal{S})$ is a finite set of structural elements active in the system at time t.

- $R(t) \subseteq E(t) \times E(t)$ is the relational graph defining structural dependencies between elements.
- $C = \{c_1, ..., c_m\}$ is a finite set of global system invariants (consistency constraints). Formally, let $\mathcal{C}$ be the universe of all definable structural predicates. Each invariant $c_i \in \mathcal{C}$ is a boolean function $c_i : \boldsymbol{\mathcal{P}}_{fin}(\boldsymbol{\mathcal{S}}) \times \boldsymbol{\mathcal{P}}_{fin}(\boldsymbol{\mathcal{S}} \times \boldsymbol{\mathcal{S}}) \rightarrow \{0, 1\}$ that evaluates a specific topological or logical consistency rule over the elements and their relations.

The State Space Σ is therefore the strictly bounded set of all such well-formed tuples:

$$\Sigma \triangleq \{\langle E(t), R(t), C(t)\rangle \mid E \in \boldsymbol{\mathcal{P}}_{fin}(\boldsymbol{\mathcal{S}}), R \subseteq E \times E, C \subseteq \mathcal{C}\} \quad \textbf{(3)}$$

Terminal Elements (Ter)

Let $D : \boldsymbol{\mathcal{S}} \rightarrow \boldsymbol{\mathcal{P}}_{fin}(\boldsymbol{\mathcal{S}})$ be the recursive decomposition operator. We formally define the subset of terminal fragments (leaf nodes) at time t as the elements that cannot be further decomposed:

$$Ter(t) \triangleq \{s \in E(t) \mid D(s) = \emptyset\} \quad \textbf{(4)}$$

Hierarchical Depth (n) and Partial States

Because the decomposition operator D is recursively applied, we define the hierarchical depth of the system as a natural number $n \in \mathbb{N}_{>0}$, representing the maximum path length from any root element to its terminal leaves. Consequently, the state S(t) can be stratified into n discrete topological levels. We denote $S^{(k)}(t)$ as the partial state reconstruction at level k, where $k \in \{0, ..., n-1\}$. By definition, the base level $S^{(0)}(t)$ contains the terminal fragments Ter(t), while the maximal level $S^{(n-1)}(t)$ corresponds to the fully reconstructed roots.

Definition of Relational Consistency ($Cons_R$)

To ensure that the state topology strictly adheres to the decomposition rules, the relational consistency predicate evaluates to 1 if and only if the edge set R(t) perfectly maps to the recursive decomposition operator D over the active element set E(t):

$$Cons_R(R(t), E(t)) = 1 \Leftrightarrow \forall s, s' \in E(t), ((s, s') \in R(t) \Leftrightarrow s' \in D(s)). \quad \textbf{(5)}$$

Verification Signatures

The Local Verification Function V_L evaluates the formal admissibility and attribute convergence of a single element. It maps an element to a tuple containing a boolean validity flag and a finite set of verified logical properties P:

$$V_L : \boldsymbol{\mathcal{S}} \rightarrow \{0, 1\} \times \boldsymbol{\mathcal{P}}(P). \quad \textbf{(6)}$$

Let $\pi_1 : \{0, 1\} \times \boldsymbol{\mathcal{P}}(P) \rightarrow \{0, 1\}$,
be the standard projection operator extracting the boolean verification result.

The Global Verification Function V_G acts as the absolute structural veto for the framework. It evaluates the entire system state $S(t) = \langle E(t), R(t), C(t) \rangle$, mapping it to a boolean validity flag:

$V_G : \Sigma \rightarrow \{0, 1\}$

Using the predefined hierarchical depth n, the preliminary global validity condition evaluates the system recursively from the terminal leaves up to the root:

$V_G(S(t)) = 1 \Leftrightarrow (\forall s \in Ter(t), \pi_1(V_L(s)) = 1) \wedge Cons_R(R(t), E(t)) \wedge Inv_C(S(t))$.

This preliminary recursive schema is formalized and strictly bounded in Axiom III, where global verification is definitively decomposed into local admissibility, relational consistency, and invariant satisfaction.

3. Local Verification and Admissibility Signatures

To formalize the local evaluation of a structural element, we define the verification primitives directly over the type-indexed components of the Structural Universe $\boldsymbol{\mathcal{S}}$.

Let the Local Verification Function V_L be formally declared with the following signature:

$V_L : \boldsymbol{\mathcal{S}} \rightarrow \{0, 1\} \times \boldsymbol{\mathcal{P}}(P)$,

for each structural type $\sigma \in \boldsymbol{\mathcal{T}}$, we define — with respect to the elements active at time t — two distinct boolean verification predicates operating strictly on their corresponding index-bound domains:

1. Formal Admissibility ($Form_\sigma$): Evaluates the structural integrity, formatting, and cryptographic bounds of the element's components.

   $Form_\sigma : Id_\sigma \times D_\sigma \times At_\sigma \times Obs^{\perp}_\sigma \rightarrow \{0, 1\}$

2. Attribute Convergence ($Conv_\sigma$): Evaluates the semantic coherence between the declared payload d, the governing attributes a, and the externally reported values obs.

   $Conv_\sigma : At_\sigma \times D_\sigma \times Obs^{\perp}_\sigma \rightarrow \{0, 1\}$.

To guarantee decidability and consistency for internal structural elements lacking physical external observations, we formally impose the following axiomatic condition for the vacuous truth of convergence:

$\forall a \in At_\sigma, \forall d \in D_\sigma, \quad Conv_\sigma(a, d, \perp) = 1$

Given an element $s = \langle \sigma, (id, d, a, obs, p) \rangle \in \boldsymbol{\mathcal{S}}$, the operational definition of V_L is therefore constructed as:

(7)

$V_L(s) \triangleq \langle Form_\sigma(id, d, a, obs) \wedge Conv_\sigma(a, d, obs), p \rangle$

where $\wedge$ denotes the strict logical AND operator.

Let $\pi_1 : \{0, 1\} \times \boldsymbol{\mathcal{P}}(P) \to \{0, 1\}$ be the standard projection to the boolean domain.
We define the local admissibility condition Adm_L for an element s as:

$Adm_L(s) = 1 \iff \pi_1(V_L(s)) = 1$

This architecture ensures that verification is inherently type-preserving and free of domain collisions, satisfying the prerequisites for the global state evaluation.

3a. Epistemic Restriction in Local Verification

In CNVS, the External Verification Agent does not receive the internally declared datum d associated with the Fragment. Instead, the Agent independently observes or measures a local property of the Object under restricted knowledge conditions.
In the evaluation of $V_L(s)$ for any terminal element $s = \langle \sigma, (id, d, a, obs, p) \rangle \in \boldsymbol{\mathcal{S}}$, the internal payload $d \in D_\sigma$ is strictly restricted to the CNVS system.
The external verification agent assigned to element s receives only the task specification derived from $a \in At_\sigma$ and independently produces the observed value $obs \in Obs^{\perp}_\sigma$. The system natively evaluates $Conv_\sigma(a, d, obs)$ without external payload disclosure.

Remark 3a. (Polymorphism of Convergence and Tolerance Bounds)

The Local Verification Function abstracts the physical and semantic complexity of real-world observations by delegating the tolerance logic to the attribute domain At_σ. The convergence predicate $Conv_\sigma$ acts as a polymorphic interface that accommodates both continuous and discrete state evaluations, ensuring that minor environmental noise or subjective categorizations do not break the systemic decidability.

Depending on the structural type $\sigma \in \boldsymbol{\mathcal{T}}$, the evaluation falls into two macro-categories, governed entirely by the parameter $a \in At_\sigma$:

1. Quantitative Convergence (Metric Spaces):

   If σ dictates a measurable physical scalar or vector space, the attribute a securely encodes a tolerance threshold ε_a. The convergence evaluates to 1 if and only if the distance function $\boldsymbol{\delta}_\sigma$ between the payload d and the observation obs satisfies the bound:

   $Conv_\sigma(a, d, obs) = 1 \iff \boldsymbol{\delta}_\sigma(d, obs) \leq \varepsilon_a$ **(8)**

2. Qualitative Convergence (Categorical and Semantic Spaces):

If σ represents a qualitative, logical, or symbolic state (e.g., colors, classification labels, bit-strings), the tolerance is modeled as a semantic neighborhood or an equivalence class mapping. The attribute a defines an acceptable boundary function $\Psi_a : D_\sigma \rightarrow \boldsymbol{\mathcal{P}}(Obs_\sigma)$, which maps the expected datum to a finite set of admissible observations (e.g., mapping "red" to a cluster of acceptable hex-color subsets or semantic neighbors). Convergence evaluates to 1 if and only if the observation falls within this valid neighborhood:

$Conv_\sigma(a, d, obs) = 1 \Leftrightarrow obs \in \Psi_a(d)$

This architecture securely delegates the specific digitalization encodings (e.g., continuous-to-discrete quantization, threshold algorithms, clustering) to the system implementation layer, while maintaining a mathematically strictly bounded global verification.

4. Recursive Decomposition and Reconstruction

Let type : $\boldsymbol{\mathcal{S}} \rightarrow \boldsymbol{\mathcal{T}}$ be the fundamental projection function that assigns to each structural element its specific structural type.
We define the primary decomposition operator D as a function mapping a well-formed element to a strictly finite set of its constituent sub-elements:
$D : \boldsymbol{\mathcal{S}} \rightarrow \boldsymbol{\mathcal{P}}_{fin}(\boldsymbol{\mathcal{S}})$.
To ensure logical consistency and non-trivial state distribution, we impose a strict disjunctive cardinality constraint on the output of D(s) for any element $s \in \boldsymbol{\mathcal{S}}$:
$|D(s)| = 0 \ \vee |D(s)| \geq 2$

if $|D(s)| = 0$(i.e., $D(s) = \emptyset$), the element cannot be further decomposed and is formally classified as a terminal node ($s \in Ter$).
If $|D(s)| \geq 2$, the element is decomposed into a finite set of child fragments $\{f_1, f_2, ..., f_k\}$.

To allow heterogeneous local validation while preserving the typed structure of the universe, we associate with every structural type $\sigma \in \boldsymbol{\mathcal{T}}$ a finite admissible evaluative spectrum:

$\Omega(\sigma) \subseteq \boldsymbol{\mathcal{T}}$.

The elements of Ω(σ) are the structural types that may occur as admissible local evaluative fragments for a parent element of type σ.

To guarantee structural consistency across hierarchical levels, the decomposition operator is not required to preserve strict type equality. Instead, it must preserve type compatibility. For any element $s \in \boldsymbol{\mathcal{S}}$ and every resulting fragment $f_i \in D(s)$, the fragment remains a well-formed element of the typed structural universe and its type must belong to the admissible evaluative spectrum of the parent type:

$\forall s \in \boldsymbol{\mathcal{S}}, \forall f_i \in D(s), f_i \in \boldsymbol{\mathcal{S}} \wedge type(f_i) \in \Omega(type(s))$. **(9)**

The strict type-preserving case is recovered as the special case:

$\Omega(\sigma) = \{\sigma\}$.

Thus, recursive decomposition remains compatible with the typed structural universe while allowing heterogeneous terminal fragments when the parent type admits heterogeneous local evaluative validation.

5. Non-Uniform Fragmentation

Let $I_{total} : \boldsymbol{\mathcal{S}} \to \mathbb{N}$ denote the total informational complexity (measured in bits) of any structural element $\forall s \in \boldsymbol{\mathcal{S}}$. We formally decompose this measure into two strictly positive functions:

- $I_{payload} : \boldsymbol{\mathcal{S}} \to \mathbb{N}$ defining the semantic informational content inherited from the original root element.
- $I_{metadata} : \boldsymbol{\mathcal{S}} \to \mathbb{N}$ defining the systemic structural information required for fragment identification, assignment consistency, relational reconstruction, and verification coordination.

For every structured element $s \in \boldsymbol{\mathcal{S}}$, the total encoded information is defined as the linear sum:

$I_{total}(s) = I_{payload}(s) + I_{metadata}(s)$. **(10)**

Remark 5.

The CNVS framework strictly distinguishes between semantic payload ($I_{payload}$) and systemic coordination data ($I_{metadata}$). Unauthorized reconstruction is therefore bounded not solely by the entropic threshold of the semantic fragments, but by the computational hardness of inferring the structural graph topology, relational dependencies, and admissible invariants encoded within $I_{metadata}$.

Non-Uniformity Axiom.

To mathematically enforce this informational asymmetry, the recursive decomposition D is intentionally non-uniform. For any non-terminal element $\forall s \in \boldsymbol{\mathcal{S}}$ such that $D(s) \neq \emptyset$, there exist at least two child fragments within its decomposition that carry strictly unequal semantic payload measures:

1. $\forall s \in \boldsymbol{\mathcal{S}}$ such that $D(s) \neq \emptyset$, $I_{payload}(s) = \Sigma_{f_i \in D(s)} I_{payload}(f_i)$,

2. $\forall s \in \boldsymbol{\mathcal{S}}$ such that $D(s) \neq \emptyset$, $\exists f_a, f_b \in D(s)$ such that $I_{payload}(f_a) \neq I_{payload}(f_b)$

Practical Decomposition Limit.

Recursive decomposition cannot grow indefinitely without incurring a monotonic increase in structural cost. Excessive fragmentation linearly increases the metadata overhead ($I_{metadata}$) while reducing the operational significance of the payload ($I_{payload}$) carried by terminal fragments. Consequently, the CNVS framework admits a strictly finite decomposition limit governed by this informational balance, mathematically averting asymptotic non-termination anomalies.

6. Knowledge Restriction and Asymptotic Negligibility

To formalize the restricted-knowledge and privacy-preserving properties of the framework, we must strictly bound the informational exposure to external actors.

Let $\mathcal{V}$ be a finite set of external verifiers. We introduce the knowledge measure function $\mathcal{K} : \mathcal{V} \times \boldsymbol{\mathcal{S}} \to \mathbb{N}$, which quantifies the exact structural and semantic information (in bits) exposed to a specific verifier $v \in \mathcal{V}$ concerning an element $s \in \boldsymbol{\mathcal{S}}$ during the verification process.

For a verifier $v \in \mathcal{V}$ assigned to validate a specific attribute $a \in At_\sigma$ of a terminal fragment $f \in Ter(t)$, let $I_{min}(a) \in \mathbb{N}_{>0}$ denote the absolute minimum informational complexity required to perform the assigned task without semantic loss. Knowledge cannot converge to zero absolutely ($\mathcal{K}(v, f) \geq 1$), as a complete loss of information would render the verification undecidable.

We formally define the structural domains of total information iteratively:

- $I_{total}(f)$: The total information encoded in the terminal fragment f.
- $I_{total}(s)$: The total information encoded in the reconstructed parent node $s = Rec(D(s))$.
- $I_{global}(S(t))$: The absolute total information of the entire system state at time t.

The framework imposes the following Strict Informational Subordination Chain:

$$I_{min}(a) \leq \mathcal{K}(v,f) < I_{total}(f) \ll I_{total}(s) \ll I_{global}(S(t))$$

Implementation Note.

In an implementation-level CNVS deployment, transport and storage confidentiality may be enforced by encrypting internal payloads and structural metadata. Each verification agent may be provisioned with a unique cryptographic key enabling decryption only of its own assigned task specification. This operational layer reinforces the structural restriction that external verifiers do not receive the internal declared payload d_i and cannot decrypt or inspect tasks assigned to other agents.
This implementation layer is not used as a substitute for the information-theoretic and probabilistic assumptions of the formal model, which still allows bounded observable metadata leakage as captured by Lemma 10.

Remark 6.

In general, the verifier's accessible knowledge $\mathcal{K}(v,f)$ does not coincide with the fragmental information $I_{total}(f)$ itself. The internal declared payload $d \in D_\sigma$ remains strictly confined within the system boundary. The verifier receives only a minimal semantic projection required to independently report an external observation $obs \in Obs^{\perp}_{\sigma}$.

The strict inequality $\mathcal{K}(v,f) < I_{total}(f)$ guarantees that no single verifier holds the complete semantic state of a fragment.

Furthermore, the operator $\ll$ denotes asymptotic informational negligibility.
To formalize this without violating the finite cardinality bounds of $\boldsymbol{\mathcal{P}}_{fin}(\boldsymbol{\mathcal{S}})$, we define a sequence of system configurations parameterized by a global structural fragmentation scale $m \in \mathbb{N}$, defined as the lower bound of system-wide decomposition: $m = \min_{s \notin Ter(t)} |D(s)|$.

By the principle of informational conservation, the parent node information scales with its partition complexity: $I_{total}(s) \geq I_{payload}(s) = \Sigma_{f\_i \in D(s)} I_{payload}(f_i)$.
Consequently, for any strictly bounded local verifier knowledge $\mathcal{K}(v,f)$, the informational ratio converges to zero as the macroscopic system scale expands:

$$\lim_{m \to \infty} \sup_{v \in \mathcal{V},\, s \notin Ter(t),\, f \in D(s)} (\mathcal{K}(v, f) / I_{total}(s)) = 0$$

This provides an asymptotic epistemic restriction condition supporting the subsequent security analysis.

Internal Payload and External Measurement-Grid Convention

A terminal fragment in CNVS must be understood as a closed native evaluative unit with two distinct informational layers.
First, each terminal fragment f_i possesses an internal declared payload d_i. This payload belongs to the native CNVS state and remains inside the system boundary during ordinary operation.

Second, each terminal fragment exposes to the external verifier only a measurement grid or task specification derived from its attribute structure. The verifier receives the local task, performs an independent observation obs_i, and returns that observation to the system.
The verifier does not receive d_i.

Thus, the terminal fragment is not a payload share in the external cryptographic sense. It may contain internal semantic payload, but that payload is not externally disclosed to the verifier.

Accordingly, $I_{payload}(f_i)$ measures the internal semantic payload associated with f_i, not the information exposed to the verifier. The verifier-accessible knowledge is instead measured by $\mathcal{K}(v, f_i)$, and in the operational CNVS model:

$\mathcal{K}(v, f_i) < I_{total}(f_i)$, because d_i remains hidden.

CNVS may internally decompose a global semantic condition into local payload-bearing evaluative units, while externally exposing only measurement grids and observations.

The probabilistic security model later adopts a strictly pessimistic convention: whenever f_i is assigned to a colluding verifier, the adversary is temporarily assumed to obtain full semantic access to d_i. This is not the ordinary CNVS exposure model, but a worst-case semantic exposure assumption used to upper-bound reconstruction risk.

Remark 6.a Definition: Structural Nature of Terminal Fragments

To preclude fundamental misinterpretations of the Knowledge Restriction limits, it is strictly necessary to define the structural nature of a fragment within the CNVS framework.

A terminal fragment $f \in Ter(t)$ is not a syntactic fraction (e.g., a data "shard" or a cryptographic sub-string) of the global payload.

Instead, f is formally defined as an Autonomous Evaluative Primitive. The recursive decomposition function D_t does not slice the data geometrically; here D_t denotes the time-indexed instantiation of the recursive decomposition operator D at transition time t.
It extracts localized logical conditions from the global state and encapsulates them into discrete, executable measurement tasks.

Consequently, the terminal fragment possesses sufficient local semantic coherence — satisfying the semantic lower bound $I_{payload}(f) \geq I_{min}$ — which enables the external verifier to execute the task and yield a deterministic Boolean output. However, because this localized task is structurally decoupled from the global relational graph, the verifier does not obtain sufficient semantic knowledge to reconstruct the overarching systemic payload.

In conclusion, in CNVS, the system does not destroy the semantic content, but extracts the logical predicates (the truth conditions) and transforms them into Local Tasks that are non-uniform in content and volume (Terminal Fragments) which are then randomly distributed along a hidden graph to disperse the connections.

7. Random Assignment

To prevent deterministic collusion and isolate adversarial clusters, terminal fragments are dynamically assigned to external verifiers through a randomized topological mapping.

Let $\mathcal{V}$ be the finite set of external verifiers, and let:

$Q \triangleq |\mathcal{V}|$

be the size of the verifier pool.

Let Ξ denote a cryptographic probability space acting as the source of secure randomness.

Let:
$Ter(t) = \{f_1, \ldots, f_k\}$
be the set of terminal fragments active at time t, with:

$k \triangleq |Ter(t)|$. **(11)**

The assignment mapping at time t is formalized as a probabilistic function:

$A_t : Ter(t) \times \Xi \to \mathcal{V}$. **(12)**

The CNVS framework imposes a one-fragment-per-verifier constraint at each assignment cycle. Therefore, for any random seed $\xi \in \Xi$ and for any two distinct terminal fragments $f_i, f_j \in Ter(t)$:

$f_i \neq f_j \Rightarrow A_t(f_i, \xi) \neq A_t(f_j, \xi)$.

Thus, for each $\xi \in \Xi$, the map $A_t(\cdot, \xi)$ is an injective matching from Ter(t) into $\mathcal{V}$.

If an active verifier set $\mathcal{V}_t \subseteq \mathcal{V}$ is selected with $|\mathcal{V}_t| = k$, then A_t induces a bijection:

$A_t(\cdot, \xi) : Ter(t) \to \mathcal{V}_t$. **(13)**

Accordingly, the hidden assignment is not a set of independent verifier choices with replacement. It is a randomized injective matching, or equivalently a randomized permutation over the active verifier slots.

Let $\mathcal{A}_{inj}(t)$ denote the set of all admissible injective assignments:

$\mathcal{A}_{inj}(t) \triangleq \{a : Ter(t) \to \mathcal{V} \mid a \text{ is injective}\}$.

The general CNVS assignment law is a probability distribution over admissible injective assignments:

$\mu_t : \mathcal{A}_{inj}(t) \to [0, 1]$,

with:

$\sum_{a \in \mathcal{A}\_inj(t)} \mu_t(a) = 1.$

This formulation allows non-uniform randomized matching, including risk-weighted verifier selection, criticality-weighted assignment, or redundancy-aware assignment, provided that the realized assignment remains cryptographically randomized and not externally predictable.

For a terminal fragment f_i and a verifier $v \in \mathcal{V}$, the marginal assignment probability is defined as:

$\mu_t(v \mid f_i) \triangleq \mathbb{P}(A_t(f_i, \xi) = v)$

or equivalently:

$\mu_t(v \mid f_i) = \sum_{a \in \mathcal{A}\_inj(t),\, a(f_i) = v} \mu_t(a).$ **(14)**

For every $f_i \in Ter(t)$, the marginal probabilities satisfy:

$\sum_{v \in \mathcal{V}} \mu_t(v \mid f_i) = 1.$

In the uniform bijective baseline, where $|\mathcal{V}_t| = k$ and all bijections between $Ter(t)$ and $\mathcal{V}_t$ are equiprobable, the number of admissible assignments is:

$k!,$

and the corresponding assignment entropy is:

$H_{assign}(k) = \log_2(k!).$ **(15)**

In that case, for every $v \in \mathcal{V}_t$:

$\mu_t(v \mid f_i) = 1 / k.$

If the active verifier set is not fixed in advance and the assignment is uniformly sampled among all injective maps from $Ter(t)$ into the full verifier pool $\mathcal{V}$, with $Q = |\mathcal{V}| \geq k$, then the number of admissible injective assignments is:

$Q! / (Q - k)!,$

and the corresponding assignment entropy is:

$H_{assign}(Q, k) = \log_2(Q! / (Q - k)!).$

In this full-pool uniform injective case, the marginal assignment probability satisfies:

$\mu_t(v \mid f_i) = 1 / |\mathcal{V}| = 1 / Q,$

for every $f_i \in Ter(t)$ and every $v \in \mathcal{V}$.

However, this marginal uniformity does not imply independence between different fragment assignments. Under injective matching, if one verifier is assigned to one fragment, the same verifier cannot simultaneously be assigned to another fragment in the same assignment cycle.

Therefore, Section 7 defines the operational CNVS assignment mechanism as a randomized injective matching. The adversarial acquisition variables, compromise probabilities, and concentration bounds are introduced separately in the probabilistic security model.

8. Axiom I: Verification-Independent Structural Existence and Verification-Dependent Admissibility

The structural existence of an element inside a candidate system state is independent of its verification status.

Let Σ_{cand} denote the candidate state space. For any candidate state

$$S_{cand}(t) = \langle E_{cand}(t), R_{cand}(t), C(t) \rangle \in \Sigma_{cand}, \quad \textbf{(16)}$$

the relation $s \in E_{cand}(t)$ denotes raw structural membership in the candidate configuration. This membership relation is not created, destroyed, or modified by the verification maps V_L or V_G. Verification does not determine whether a candidate element exists; it determines whether the element, and ultimately the state containing it, is admissible.

For every terminal element $s \in Ter(t)$, local admissibility is defined by:

$$Adm_L(s) = 1 \Leftrightarrow \pi_1(V_L(s)) = 1.$$

Accordingly, the locally admissible terminal subset is:

$$Ter^+(t) \triangleq \{s \in Ter(t) \mid Adm_L(s) = 1\}.$$

The accepted CNVS state space is defined as:

$$\Sigma^+ \triangleq \{S \in \Sigma_{cand} \mid V_G(S) = 1\}. \quad \textbf{(17)}$$

Therefore:

$s \in E_{cand}(t)$ does not imply $Adm_L(s) = 1$,

and

$(\forall s \in Ter(t), Adm_L(s) = 1)$ does not imply $V_G(S_{cand}(t)) = 1$.

The first implication fails because structural membership is prior to local verification. The second implication fails because global validity additionally requires relational consistency and invariant satisfaction.

Thus, verification-dependent existence in CNVS must be understood strictly as verification-dependent admissibility into the accepted state evolution, not as primitive creation of raw structural elements. The verification process partitions candidate states into accepted and rejected states without retroactively denying the structural existence of the rejected candidate configuration.

9. Axiom II: Randomized Non-Uniform Fragmentation

Every element $s \in \mathcal{S}$ such that $D(s) \neq \emptyset$ is recursively decomposed into a non-uniform set of fragments. The assignment operator A_t defines a probabilistic mapping to the verifier set $\mathcal{V}$:

- $|D(s)| \geq 2$
- $\exists\, f_a, f_b \in D(s) : I_{payload}(f_a) \neq I_{payload}(f_b)$
- $Rec(D(s)) = s$

The assignment operator is a randomized injective matching as defined in Section 7.
The independent-assignment model is used only later as an analytical baseline.

10. Axiom III: Non-Reducibility of Global Validity

Global validity is not an emergent property of terminal elements, but a systemic invariant. Let $Cons_R(R(t), E(t))$ be the relational consistency and $Inv_C(S(t))$ be the satisfaction of the global invariants C. The Global Verification Function is defined as the strict conjunction:

$Cons_R(R(t), E(t)) = 1 \Leftrightarrow \forall s, s' \in E(t), ((s, s') \in R(t) \Leftrightarrow s' \in D(s))$,
$Inv_C(S(t)) = 1 \Leftrightarrow \forall c_i \in C, c_i(E(t), R(t)) = 1.$

$$V_G(S(t)) = 1 \Leftrightarrow (\forall s \in Ter(t), \pi_1(V_L(s)) = 1) \wedge Cons_R(R(t), E(t)) \wedge Inv_C(S(t)) \quad \textbf{(18)}$$

Non-Reducibility Principle:

$$\exists S(t) \in \Sigma \text{ such that } (\forall s \in Ter(t), \pi_1(V_L(s)) = 1) \wedge (V_G(S(t)) = 0) \quad \textbf{(19)}$$

This asserts the existence of "locally valid but globally inconsistent" states. This proves that the global system state cannot be reduced to the mere verification of its terminal fragments, thereby mandating the Global Veto.

11. State Transition Law

The evolution of the system state to a candidate successor S' is governed by the absolute admissibility condition:

(20)

$$S(t+1)=\begin{cases} S' & \text{if } V_G(S')=1 \\ S(t) & \text{if } V_G(S')=0 \end{cases}$$

Any candidate state S' such that $V_G(S') = 0$ is formally rejected.
This establishes that state evolution is strictly verification-dependent and constrained by the totality of structural invariants C and the relational consistency $Cons_R$. The system admits no "invalid" transitions; the state space is self-correcting via the Global Veto.

Remark 11.1 (Topological Refresh and Sybil/Fault-Injection Resistance)

To preclude cross-cycle structural inference, the CNVS framework enforces an absolute Topological Refresh upon any state rejection.

An adversarial coalition (e.g., executing a Sybil attack) might theoretically attempt a *Fault Injection* strategy: intentionally submitting invalid external observations to deliberately trigger the Global Veto ($V_G(S') = 0$). If the structural topology were static, the adversary could iterate this process infinitely, accumulating semantic and topological metadata across successive failed cycles to eventually reconstruct the relational graph.

To mathematically neutralize this vector, the CNVS mandates that the recursive decomposition operator (D) and the random assignment mapping (A_t) are strictly ephemeral and bound to the specific transition attempt.

Therefore, whenever $V_G(S') = 0$:

1. The prior topological decomposition D(s) is dissolved.
2. A new, statistically independent randomization of the structural cut is generated via the cryptographic space Ξ.
3. The terminal fragments are completely reassigned across the verifier set $\mathcal{V}$.

Consequently, any relational metadata $I_{metadata}$ acquired by the adversary during a failed state transition does not directly transfer to the next randomized transition attempt. The combinatorial entropy of the system is regenerated under a fresh randomized configuration at every new cycle, thereby limiting iterative metadata accumulation.

12. Fundamental Lemmas

The robustness of the CNVS framework is supported by the following lemmas, derived from the axioms of structural decomposition and local verification:

- **Lemma 1 (Terminal Membership):** $\forall s \in Ter(t), s \in E(t) \subseteq \boldsymbol{\mathcal{S}}$ (Existence is primitive).
- **Lemma 2 (Global Necessity):** $\exists S(t) \in \Sigma : (\forall s \in Ter(t), Adm_L(s)=1) \wedge V_G(S(t))=0$ (Proves that local validity does not imply global consistency).
- **Lemma 3 (Type Compatible Decomposition):**

  For every structural element $s \in \boldsymbol{\mathcal{S}}$ and every fragment f generated by its decomposition, the fragment remains a well-typed element of the structural universe and its native type belongs to the admissible evaluative spectrum of the parent type: $\forall s \in \boldsymbol{\mathcal{S}}, \forall f \in D(s), f \in \boldsymbol{\mathcal{S}} \wedge type(f) \in \Omega(type(s))$.
  Consequently, recursive decomposition does not erase type structure. It preserves formal well-typedness while allowing heterogeneous local evaluative fragments.

- **Lemma 4 (Internal Payload Accounting):**

  For every decomposable structural element $s \in \boldsymbol{\mathcal{S}}$ with $D(s) \neq \emptyset$, the internal semantic payload associated with s is distributed across the closed native terminal or sub-terminal evaluative units generated by D.
  Formally: $I_{payload}(s) = \Sigma\, f_i \in D(s)\ I_{payload}(f_i)$.
  This equation is an internal accounting identity. It does not imply that external verifiers receive semantic payload shares. In ordinary CNVS operation, the verifier receives only the measurement grid or task specification associated with f_i and independently produces obs_i. The internal payload d_i remains inaccessible to the verifier.

  Therefore, internal payload conservation is compatible with external knowledge restriction.

- **Lemma 5 (Metadata Overhead):** $\forall s \in \boldsymbol{\mathcal{S}}$ such that $D(s) \neq \emptyset$, $I_{metadata}(Rec(D(s))) < \Sigma_{f\_i \in D(s)}\ I_{metadata}(f_i)$.
  (Fragmentation increases systemic metadata costs).
- **Lemma 6 (Asymptotic Epistemic Negligibility):**

  Let $\mathcal{K}(v, f)$ denote the verifier-accessible information associated with a terminal fragment f, and let Iglobal(S(t)) denote the total informational content of the system state.
  If the verifier-accessible information remains locally bounded while the global

informational structure increases with the structural fragmentation scale m(t), then: $\lim_{m(t)\to\infty} \mathcal{K}(v, f) / I_{global}(S(t)) = 0$.

- **Lemma 7 (Residual Structural Inference Bound)**: see Section 17a for the full statement and proof.
- **Lemma 8 (Hidden-Invariant Residual Non-Inferability Bound):**

  To preclude deterministic algebraic reconstruction, the CNVS framework does not assume that an adversarial coalition has access to the instantiated global validation constraints.

  An adversary may know the general public class of admissible invariant forms, denoted by C_{pub}, but does not know the internal instantiated invariant parameters θ_C, the complete relational topology R_{int}, or the specific invariant binding that maps terminal fragments into global validation equations.

  Let
  $C_{int} \triangleq \langle \theta_C, R_{int} \rangle$ **(21)**
  where:
  θ_C = hidden internal invariant parameters
  R_{int}= hidden internal relational topology.

  Let f_{miss} denote a critical terminal fragment not directly controlled by the adversarial coalition, and let d_{miss} be its true internal semantic payload.

  Let W_k denote the complete worst-case semantic information acquired from compromised terminal fragments, including the local payloads pessimistically granted to colluding verifiers in the adversarial model of Section 15.

  Let M_s denote the observable topological metadata, subject to the bounded topological leakage condition defined in Lemma 10.

  For the purpose of this residual non-inferability bound, the relevant adversarial view may be represented by the tuple of components:

  $View_{adv} \triangleq (W_k, M_s, C_{pub})$. **(22)**

  The CNVS residual non-inferability condition requires that the adversarial view does not collapse the conditional min-entropy of the missing payload. There must exist a strictly positive residual entropy margin $h_{min} > 0$ such that:

  $H_\infty(d_{miss} | View_a\, d_v) \geq h_{min}$. **(23)**

  Equivalently, the optimal adversarial guessing probability is bounded by:

  $\mathbb{P}_{guess}(d_{miss} | W_k, M_s, C_{pub}) \leq 2^{-h\_min}$. **(24)**

  This condition means that the adversary may possess many compromised local payloads and may know an abstract schema-level class of admissible validation

forms, but still lacks the hidden instantiated constraint structure Cint required to deterministically infer the missing critical payload.

The rigorous security condition is therefore not that the adversary observes fewer equations than unknowns in a purely syntactic linear-algebraic sense. Rather, the condition is that the adversarial view lacks sufficient information to reduce the residual min-entropy of the missing critical payload to zero.

Since conditional min-entropy bounds the optimal guessing probability, the inference probability for the missing critical fragment satisfies:

$p_{inf} \leq 2^{-h\_min}$. **(25)**

Consequently, if $h_{min} > 0$, then:

$p_{inf} < 1$.

If h_{min} is large, then p_{inf} becomes exponentially small. This provides the information-theoretic basis for the dependent-collusion model, in which the composite compromise probability remains strictly sub-unitary:

$p_{comp} = q + (1 - q)\, p_{inf} < 1$,

provided $q < 1$.

- **Lemma 9 (Decidability Constraint of Global Validation):**

  To prevent systemic undecidability and avoid non-terminating validation procedures, the evaluative functions governing the Global Veto are formally restricted to a bounded validation language.

  Let L_V denote the formal validation language used to express the systemic structural invariants C and the relational consistency checks $Cons_R$ evaluated by V_G. The language L_V admits only total computable predicates with polynomially bounded evaluation. In particular, L_V excludes unbounded recursion, non-terminating procedures, and validation loops whose depth is not structurally bounded by the finite state representation or by the hierarchical depth n of the state.

  For every candidate state $S' = \langle E', R', C' \rangle \in \Sigma$, assume that:

  1. $Cons_R(R', E')$ is expressed in L_V;
  2. every invariant predicate $c_i \in C'$ is expressed in L_V;
  3. all quantifications range only over the finite sets E', R', and C';
  4. every iterative validation loop is bounded by the finite cardinalities of the state components or by the hierarchical depth n.

  Then the global verification function

  $V_G(S') = 1 \Leftrightarrow (\forall s \in Ter(S'), \pi_1(V_L(s)) = 1) \wedge Cons_R(R', E') \wedge (\forall c_i \in C', c_i(E', R') = 1)$

is decidable. Moreover, its evaluation time is bounded by a polynomial in the encoded size of the candidate state S'. If the encoded size of S' is polynomially bounded by the hierarchical depth n, then there exists a constant exponent $\alpha \in \mathbb{N}$ such that:

$\text{Time}(V_G(S')) \leq O(n^{\alpha})$.

Proof. The sets E', R', and C' are finite by definition of the CNVS state space. The evaluation of V_G is a finite conjunction of: local verification predicates over terminal elements, the relational consistency predicate Cons_R, and the invariant predicates $c_i \in C'$. By assumption, each of these predicates is expressed in L_V and therefore is total and polynomial-time bounded. Since finite sums and finite compositions of polynomial-time computations remain polynomial-time, the complete evaluation of V_G halts and returns a binary value in polynomial time. Therefore, for every $S' \in \Sigma$:

$V_G(S') \in \{0, 1\}$.

Proof Consequence. Because V_G is decidable under the L_V restriction, the State Transition Law introduced in Section 11 is strictly decidable. Every candidate transition is either accepted or rejected in finite bounded time, and the rejection of an invalid state is well-defined rather than subject to infinite deferral.

- **Lemma 10 (Bounded Topological Leakage and Entropy Separation):**
To prevent the theoretical vulnerability of entropic overlap — whereby the structural shape of the routing topology may reveal information about the native semantic payload — the CNVS framework does not require perfect semantic independence between topology and payload. Instead, it imposes a bounded-leakage condition.

  Let X_S be the random variable representing the native semantic payload of the system state S, and let M_S be the random variable representing the observable structural metadata of the CNVS configuration, including routing topology, fragment assignment structure, and coordination metadata.

  The CNVS topology is said to satisfy γ-topological leakage if: $I(X_S ; M_S) \leq \gamma_{top}$,

  where $\gamma_{top} \geq 0$ is a bounded leakage parameter. Equivalently, the residual uncertainty of the semantic payload after observing the topological metadata satisfies: $H(X_S \mid M_S) \geq H(X_S) - \gamma_{top}$. **(26)**

  Thus, the routing topology is not required to be perfectly independent from the semantic payload. It may reveal limited structural information. However, such information remains quantitatively bounded and does not suffice for deterministic reconstruction.

  A CNVS configuration is semantically non-reconstructive if there exists a strictly positive residual entropy margin $h_{min} > 0$ such that: $H(X_S \mid M_S, W) \geq h_{min}$, **(27)**

where W denotes the adversarially acquired fragment-level information.

This condition means that even after observing the available topology and the compromised local information, the adversary still faces irreducible uncertainty about the native semantic payload.

Proof Consequence. Under γ-topological leakage, the structural map may leak limited metadata about the organization of the verification process, but it does not collapse the semantic uncertainty of the payload. Therefore, the adversary cannot deterministically reconstruct the global state unless the residual entropy margin h_{min} vanishes.
In the idealized limiting case $\gamma_{top} = 0$, the model reduces to perfect semantic-agnostic topology: $I(X_S ; M_S) = 0$.

However, the general CNVS security model only requires the weaker and more realistic bounded-leakage condition: $I(X_S ; M_S) \leq \gamma_{top}$,
together with positive residual uncertainty: $H(X_S \mid M_S, W) \geq h_{min} > 0$.

13. Principle of Knowledge Restriction

The CNVS framework does not assume Knowledge Restriction as a passive, static property, but enforces it as a structural consequence of recursive decomposition, local task restriction, randomized assignment, and hidden global binding.

In the present compact formal paper the security argument only requires the following abstract condition: as the system expands, the verifier-accessible knowledge remains negligible relative to the total informational structure of the global state.

Let m(t) denote the active structural fragmentation scale of the system at time t. As m(t) increases, the verifier-accessible knowledge becomes strictly negligible relative to the global informational structure. Thus, we define epistemic restriction through the following asymptotic condition:
(28)

$$\lim_{m(t) \to \infty} \mathcal{K}(v, f) \,/\, I_{global}(S(t)) = 0.$$

This condition states that the information available to any verifier about a local terminal fragment remains asymptotically negligible with respect to the total informational content of the system state.

To translate this structural bound into information-theoretic terms, let X_s be the random variable representing the true internal semantic payload of a node s, and let Y_v be the random variable representing the externally observable information available to verifier v.

The verifier's information about the native semantic content is asymptotically bounded by a vanishing sequence $\varepsilon_m \to 0$ as $m(t) \to \infty$:
(29)

$$I(X_s ; Y_v) \leq \varepsilon_m.$$

Equivalently, the conditional entropy of the internal payload, given the verifier's knowledge, remains close to maximal uncertainty:
(30)

$$H(X_s \mid Y_v) \geq H(X_s) - \varepsilon_m.$$

Therefore, knowledge restriction is not treated here as a consequence of a specific density-control formula, but as a formal asymptotic condition enforced by CNVS decomposition, assignment, and verification architecture.

13a. Worst-Case Semantic Exposure Convention

In the operational CNVS architecture, an external verifier assigned to a terminal fragment f_i does not receive the internal declared payload d_i. The verifier receives only a task specification or measurement grid derived from the attribute structure and independently produces an observation obs_i. The convergence predicate is then evaluated internally by the CNVS system through $Conv_\sigma(a_i, d_i, obs_i)$.
However, the probabilistic security analysis developed in the following sections intentionally adopts a strictly pessimistic adversarial convention.

For the purpose of upper-bounding reconstruction risk, whenever a terminal fragment f_i is assigned to a colluding verifier, the adversary is assumed to obtain full semantic access to the local internal payload d_i associated with that fragment.

This assumption is stronger than the operational CNVS exposure model. In the real protocol, the colluding verifier only observes the measurement task and its own reported observation. In the probabilistic model, by contrast, the adversary is temporarily granted the entire local semantic content d_i.

Therefore, the weighted adversarial information W_k analyzed below is not the ordinary information exposed to honest or dishonest verifiers during normal operation. It is a worst-case semantic exposure variable. Any security bound proven under this pessimistic assumption also upper-bounds the risk of the operational model in which d_i remains hidden and only obs_i is externally available.

14. Probabilistic Security Model

We formalize the security bounds against an adversarial coalition attempting unauthorized state reconstruction under a pessimistic semantic exposure model and using the assignment framework of Section 7.
Independence is an analytical baseline, not the CNVS operating model.
Let:

- $\mathcal{V}$ be the finite set of total verifiers, with $Q = |\mathcal{V}|$;
- $\mathcal{V}_{adv} \subset \mathcal{V}$ be the adversarial colluding coalition;
- $k = |Ter(t)|$ be the total number of active terminal fragments;
- $q = |\mathcal{V}_{adv}| / Q$ denotes the common marginal compromise probability under the full-pool uniform injective baseline;
- d_i be the internal declared payload associated with terminal fragment f_i;
- $I_{payload}(f_i)$ be the semantic information content of d_i.

Although d_i is not disclosed to the verifier in the operational CNVS protocol, the present probabilistic model assumes, pessimistically, that an adversarial verifier assigned to f_i obtains full access to d_i.

Let $I_{ref} \in \mathbb{R}_{>0}$ be a fixed semantic reference capacity chosen so that every terminal fragment satisfies:

$0 < I_{payload}(f_i) \leq I_{ref}$.

We define the normalized local semantic weight of fragment f_i as:
(31)

$\omega_i \triangleq I_{payload}(f_i) / I_{ref}$.

Hence:

$0 < \omega_i \leq 1$.

Let $Y_i \in \{0, 1\}$ be the adversarial acquisition indicator:

$Y_i = 1$ if f_i is assigned to a colluding verifier (i.e., $A_t(f_i, \xi) \in \mathcal{V}_{adv}$),

$Y_i = 0$ otherwise.

Let $q_i \triangleq \mathbb{P}(Y_i = 1)$

denote the corresponding marginal compromise probability.
Using the marginal assignment probabilities defined in Section 7, this becomes:
$q_i = \sum_{v \in \mathcal{V}\_adv} \mu_t(v \mid f_i)$.

In the full-pool uniform injective case, if $|\mathcal{V}| = Q$ and $|\mathcal{V}_{adv}| = r$, then: $q_i = r / Q$.

If q denotes this common marginal compromise probability, then:

$q = |\mathcal{V}_{adv}| / |\mathcal{V}| = r / Q$, **(32)**

Thus, q is only the common compromise probability in the uniform marginal case.

Under injective assignment, the variables $Y_1, \ldots, Y_k$ are generally not mutually independent. Therefore, the independent-assignment Hoeffding model should be understood as a simplified analytical baseline, while the exact operational assignment mechanism is the randomized injective matching defined in Section 7.

Under the independent randomized assignment assumption, the variables Y_i are independent Bernoulli random variables with:

$\mathbb{E}[Y_i] = q$.

The cumulative worst-case adversarial semantic acquisition is therefore:
(33)

$W_k \triangleq \Sigma^k_{i=1} Y_i \omega_i$.

Let:

$\bar{\omega}_k \triangleq (1/ k) \Sigma^k_{i=1} \omega_i$

be the average normalized semantic weight of the terminal fragments.

Then:
(34)

$\mathbb{E}[W_k] = \Sigma^k_{i=1} \mathbb{E}[Y_i]\omega_i = q \Sigma^k_{i=1} \omega_i = q\ k\ \bar{\omega}_k$.

Unauthorized systemic reconstruction is modeled as a threshold event over the extensive worst-case semantic acquisition variable W_k. Let $\tau \in (0, 1]$ denote the critical normalized semantic acquisition density required for reconstruction. The adversarial reconstruction event is:

$W_k \geq \tau\ k$.

Thus, the conditional security regime is:

$q\,\bar{\omega}_k\,k < \tau\,k.$

This formulation is dimensionally coherent because W_k and τk are both extensive quantities measured in units of normalized terminal semantic capacity. It also preserves the pessimistic nature of the model: the adversary is assumed to acquire d_i whenever it controls the assigned verifier, even though d_i is not externally disclosed in the operational CNVS protocol.

In Sections 15–17, we restrict the analysis to the uniform independent-assignment baseline, where $q_i = q$ for all terminal fragments.
The general dependent-collusion model is addressed in Section 17a.

15. Conditional Security Theorem

We establish the foundational condition under which adversarial reconstruction is probabilistically bounded in the independent-assignment baseline.
Let the absolute reconstruction threshold be defined as:

$$\mathbb{T} \triangleq \tau\,k,$$

where $\tau \in (0, 1]$ represents the critical normalized semantic acquisition density required to compromise the state.

Theorem 1. Conditional Worst-Case Semantic Security

Let W_k be the cumulative worst-case adversarial semantic acquisition:

$$W_k = \Sigma^{k}_{i=1}\ Y_i\omega_i,$$

where each $\omega_i \in (0,1]$ is the normalized semantic weight of the internal payload d_i associated with terminal fragment f_i.

Let

$$\bar{\omega}_k \triangleq (1/k)\,\Sigma^{k}_{i=1}\,\omega_i$$

be the average normalized semantic weight.

If:

$$q\,\bar{\omega}_k < \tau,$$

then the expected worst-case semantic information acquired by the colluding coalition remains strictly below the reconstruction threshold $\tau\,k$.

Proof

By linearity of expectation:

$\mathbb{E}[W_k] = \mathbb{E}[\sum^{k}_{i=1} Y_i\omega_i]$
$= \sum^{k}_{i=1} \mathbb{E}[Y_i]\omega_i$
$= q \sum^{k}_{i=1} \omega_i$
$= q\ k\ \bar{\omega}_k.$

By the theorem hypothesis:

$q\ \bar{\omega}_k < \tau.$

Multiplying both sides by k gives:

$q\ k\ \bar{\omega}_k < \tau\ k.$ **(35)**

Therefore:

$\mathbb{E}[W_k] < \tau\ k.$

Hence, even under the pessimistic assumption that every colluding verifier obtains the full internal payload d_i of its assigned fragment, the expected adversarial semantic acquisition remains below the reconstruction threshold.

16. Exponential Concentration Bound

The following concentration estimate is a baseline result under the simplified independent-assignment model. It assumes that terminal assignments are independent and that adversarial acquisition occurs through direct assignment to colluding verifiers.

Theorem 2. Baseline Hoeffding Concentration Bound

Let:

$W_k = \sum^{k}_{i=1} Y_i\omega_i,$

where each Y_i is an independent Bernoulli random variable with parameter q, and each weighted acquisition variable $Y_i\omega_i$ is bounded in the interval $[0, \omega_i]$.

If the worst-case semantic acquisition density satisfies:

$q\ \bar{\omega}_k < \tau,$

then:

$\mathbb{P}(W_k \geq \tau\, k) \leq \exp(-2\, k^2(\tau - q\, \bar{\omega}_k)^2 / \Sigma^k_{i=1} \omega_i^2)$.

In particular, since $\omega_i \leq 1$ for every i:

$\Sigma^k_{i=1} \omega_i^2 \leq k$,

and therefore:

$\mathbb{P}(W_k \geq \tau k) \leq \exp(-2k(\tau - q\bar{\omega}_k)^2)$. **(36)**

This theorem is a baseline concentration result. It proves exponential suppression under independent randomized assignment, but it does not claim that all realistic CNVS compromise processes are independent.

Proof

We write:

$\mathbb{P}(W_k \geq \tau k)$

$= \mathbb{P}(W_k - \mathbb{E}[W_k] \geq \tau\, k - q\, k\, \bar{\omega}_k)$.

Since:

$\tau\, k - q\, k\, \bar{\omega}_k = k(\tau - q\, \bar{\omega}_k)$,

and since $\tau - q\, \bar{\omega}_k > 0$ by hypothesis, Hoeffding's inequality yields:

$\mathbb{P}(W_k \geq \tau\, k) \leq \exp(-2\, k^2(\tau - q\, \bar{\omega}_k)^2 / \Sigma^k_{i=1} \omega_i^2)$.

Because each $\omega_i \leq 1$, we have:

$\Sigma^k_{i=1}\, \omega_i^2 \leq k$.

Therefore:

$\mathbb{P}(W_k \geq \tau\, k) \leq \exp(-2k\, (\tau - q\, \bar{\omega}_k)^2)$.

This proves exponential decay in k whenever the positive security margin $\tau - q\, \bar{\omega}_k$ is bounded away from zero.

17. Emergent Security Scaling Theorem

We now state the asymptotic consequence of the baseline concentration bound.

Theorem 3. Asymptotic Emergent Security under Worst-Case Payload Exposure

Let k(m) be the number of terminal fragments generated at fragmentation scale m, with:

$k(m) \to \infty$ as $m \to \infty$.

Assume:

1. in the independent-assignment analytical baseline, the acquisition variables Y_i are independent;
2. each colluding verifier is pessimistically assumed to obtain the full internal payload d_i of each assigned terminal fragment f_i;
3. the normalized semantic weights satisfy $0 < \omega_i \leq 1$;
4. there exists a fixed positive security margin $\delta > 0$ such that:

$\tau - q\,\bar{\omega}_{k(m)} \geq \delta$

for all sufficiently large m.

Then:

$\lim_{m \to \infty} \mathbb{P}(W_{k(m)} \geq \tau\, k(m)) = 0.$

Moreover:

$\mathbb{P}(W_{k(m)} \geq \tau k(m)) \leq \exp(-2\delta^2\, k(m)).$ **(37)**

Proof

From Theorem 2:

$\mathbb{P}(W_k \geq \tau\, k) \leq \exp(-2k\,(\tau - q\,\bar{\omega}_k)^2).$

By assumption, for sufficiently large $k = k(m)$:

$\tau - q\,\bar{\omega}_k \geq \delta > 0.$

Therefore:

$\mathbb{P}(W_{k(m)} \geq \tau\, k(m)) \leq \exp(-2\delta^2\, k(m)).$

Since $k(m) \to \infty$ as $m \to \infty$, the exponent diverges to $-\infty$:

$-2\delta^2\, k(m) \to -\infty.$

Consequently:

$\lim_{m \to \infty} \mathbb{P}(W_{k(m)} \geq \tau\, k(m)) = 0.$

Thus, even under the pessimistic semantic exposure convention in which colluding verifiers are assumed to obtain the internal payload d_i of every assigned fragment, unauthorized

reconstruction probability converges to zero under the independent-assignment analytical baseline and a fixed positive semantic security margin.

Transition to the Generalized Dependent-Collusion Model

The independent Hoeffding baseline captures the idealized case in which fragment assignments are independent and adversarial acquisition occurs only through direct assignment to colluding verifiers.

However, real adversarial coalitions may attempt to exploit structural inference, partial metadata leakage, repeated observations, adaptive coordination, or correlations between compromised fragments. In such cases, the compromise events are no longer adequately modeled as independent Bernoulli acquisitions.

For this reason, the CNVS security analysis does not rely exclusively on the Hoeffding baseline.
The independent model is generalized by introducing a composite compromise probability:

$$p_{comp} = q + (1 - q)p_{inf},$$

where q represents direct assignment to colluding verifiers and p_{inf} represents the bounded probability of inferring an uncompromised critical fragment from already acquired information.

The dependent-collusion model replaces independence with a conditional upper bound:

$$\mathbb{P}(c_{coll\_i} \mid c_{coll\_1}, \ldots, c_{coll\_i-1}) \leq p_{comp} < 1.$$

Thus, the essential CNVS security requirement is not strict independence of all compromise events, but the weaker and more general condition that each additional critical fragment remains non-deterministically inferable with probability bounded away from one.

17a. Generalized Emergent Security Scaling under Dependent Collusion

The independent-assignment concentration analysis (Sections 15-17) provides an idealized asymptotic bound. We now generalize the model to evaluate dependent compromise events, where an adversarial coalition attempts cryptanalytic inference across multiple fragments.

Let:

- $q \in [0, 1)$ denotes the probability that a critical fragment is directly assigned to colluding verifiers under the uniform marginal baseline defined in Section 14.
- $View_{adv}$ denotes the complete adversarial view available to the colluding coalition, including directly compromised fragments, observable metadata, public structural

information, and any information accumulated through previous compromise history.

- $p_{inf} \in [0, 1)$ denotes the probability of structural inference — the likelihood that a fragment not directly controlled can be compromised via cryptanalytic derivation from already compromised fragments.
- $m \in \mathbb{N}$ denotes the strictly positive number of critical low-inference fragments required for unauthorized systemic reconstruction.

We formally define the single-fragment composite compromise probability p_{comp} via the Law of Total Probability:

(38)

$$p_{comp} \triangleq q + (1 - q)\, p_{inf}$$

Let c_{coll_i} denote the adversarial event that the i-th critical fragment is successfully compromised. To formalize the conditional dependence between compromise events, we establish the following bounding lemma.

Lemma 7. Residual Structural Inference Bound:
A critical fragment may be compromised in two distinct ways:

1. by direct assignment to a colluding verifier;
2. by structural inference from previously compromised fragments, observable metadata, and abstract schema-level knowledge about the admissible validation framework.

In the uniform independent-assignment baseline, the probability of direct assignment to the adversarial coalition is q.

If the i-th critical fragment is not directly assigned to the adversarial coalition, then its compromise can occur only through inference. By Lemma 8, every non-controlled critical fragment retains a strictly positive residual conditional min-entropy margin $h_{min} > 0$ under the adversarial view. Therefore, the optimal inference probability is bounded by:

$p_{inf} \leq 2^{-h\_min}$.

Consequently, the conditional probability of compromising the i-th critical fragment, given any previous compromise history, satisfies:

$\mathbb{P}(c_{coll\_i} \mid c_{coll\_1}, \ldots, c_{coll\_i-1}) \leq q + (1 - q)p_{inf}$.

Define the composite compromise probability:

$p_{comp} \triangleq q + (1 - q)p_{inf}$.

Since $p_{inf} \leq 2^{-h\_min}$, we obtain:

$p_{comp} \leq q + (1 - q)2^{-h\_min}$.

Therefore, if $q < 1$ and $h_{min} > 0$, then:

$p_{comp} < 1$.

This establishes the conditional upper bound:

$\mathbb{P}(c_{coll\_i} \mid c_{coll\_1}, \ldots, c_{coll\_i-1}) \leq p_{comp} < 1$.

Thus, the dependent-collusion model does not require independence between compromise events. It requires only that each additional critical fragment remains non-deterministically inferable with probability bounded strictly below one.

Therefore for each additional critical fragment, the residual min-entropy condition is required to hold after incorporating into the adversarial view all previously compromised fragments, observable metadata, and any abstract schema-level knowledge available about the admissible validation language. Thus, previous compromise history may reduce residual uncertainty, but it must not collapse the conditional min-entropy of the next uncontrolled critical fragment to zero. The instantiated invariant parameters, the internal relational topology, and the specific invariant binding remain hidden inside the CNVS system.

Interpretive Note.

In Theorem 4, pcomp is used as a uniform conditional upper bound over the adversarial regime under consideration. The parameter p_{inf} need not be interpreted as a static fixed scalar; it may represent the worst-case upper bound of an inference probability depending on the adversarial view accumulated so far. Equivalently, one may read p_{comp} as satisfying

$p_{comp} \geq \sup_i \mathbb{P}(c_{coll\_i} \mid c_{coll\_1}, \ldots, c_{coll\_i-1})$,

with $p_{comp} < 1$.

The dynamic entropy-driven formulation of Remark 17a.2 generalizes this static upper-bound presentation by allowing p_{inf} and pcomp to vary with time or accumulated adversarial knowledge.

Theorem 4 (Generalized Emergent Security Scaling)

Under the constraints of the Residual Structural Inference Bound, the probability of an unauthorized full state reconstruction, denoted as Rec^*, satisfies the exponential decay inequality:

(39)

$$\mathbb{P}(Rec^*) \leq (p_{comp})^m$$

Proof

Unauthorized full reconstruction strictly requires the simultaneous compromise of all m critical low-inference fragments. In set-theoretic terms, the reconstruction event is a subset of the intersection of all compromise events:

$Rec^* \subseteq \cap^m_{i=1} c_{coll\_i}$

Therefore, by the monotonicity of probability measures:

$\mathbb{P}(Rec^*) \leq \mathbb{P}(\cap^m_{i=1} c_{coll\_i})$

Applying the general chain rule of probability:

$\mathbb{P}(\cap^m_{i=1} c_{coll\_i}) = \prod^m_{i=1} \mathbb{P}(c_{coll\_i} | c_{coll\_1}, ..., c_{coll\_i-1})$

Substituting the conditional upper bound established in Lemma 7 into the product series:
(40)

$\mathbb{P}(Rec^*) \leq \prod^m_{i=1} p_{comp} = {p_{comp}}^m$

This demonstrates that systemic security scales exponentially against dependent collusion, provided the underlying composite probability remains strictly sub-unitary.

Corollary 4.1 (Asymptotic Dependent Security)

Because $0 \leq p_{comp} < 1$, the geometric sequence $(p_{comp})^m$ converges to zero. Therefore, as the system scale expands and the requisite critical fragments increase:
$\lim_{m \to \infty} \mathbb{P}(Rec^*) = 0$

Corollary 4.2 (Non-Inferable Limit)

In the idealized non-inferable case $p_{inf} = 0$, the composite compromise probability reduces to $p_{comp} = q$.
The generalized security bound then reduces to the idealized direct-assignment boundary:

$\mathbb{P}(Rec^*) \leq q^m$

Systemic Design Formula: Minimum Critical Fragmentation

To operationalize the security model, the framework must determine the minimum decomposition depth required to satisfy a specific security target. Given a maximum tolerable target attack probability $\eta \in (0, 1)$, we seek the minimum number of critical low-inference fragments m_{min} such that:
(41)

$\mathbb{P}(Rec^*) \leq \eta$

By substituting the exponential bound derived in Theorem 4:
${p_{comp}}^m \leq \eta$

Taking the natural logarithm of both sides:

$m \ln(p_{comp}) \leq \ln(\eta)$

Since $\eta \in (0, 1)$ and $p_{comp} \in (0, 1)$, both logarithmic terms are strictly negative. Consequently, dividing both sides by ln(p_comp) reverses the inequality direction:

$m \geq \ln(\eta) / \ln(p_{comp})$

Because the fragmentation depth m must be a discrete natural number ($m \in \mathbb{N}$), we define the exact threshold using the ceiling function:

(42)

$m_{min} = \lceil \ln(\eta) / \ln(p_{comp}) \rceil$

This formula deterministically translates any theoretical cryptographic security requirement (η) into a precise topological constraint (m_{min}).

Remark 17a.1 (Semantic lower bound and practical scaling)

The asymptotic expression $m \to \infty$ utilized in Corollary 4.1 represents an idealized mathematical limit. In practical CNVS deployments, fragmentation cannot proceed indefinitely.

As formalized in Section 6, terminal fragments must preserve a sufficient semantic payload to allow honest external verifiers to perform their assigned local evaluation tasks without logical undecidability.

Therefore, the effective fragmentation depth is strictly constrained by the semantic lower bound:

(43)

$\forall f \in Ter(t), \; I_{payload}(f) \geq I_{min}$

where I_{min} denotes the absolute minimum informational quantum required for task comprehension.

Consequently, the practical system design problem is not to maximize fragmentation to infinity, but to solve a Bounded Optimization Problem:

Maximize epistemic restriction (by increasing m) subject to the constraint of local semantic verifiability.

Let m_{max} denote the theoretical maximum number of fragments derivable from a root element s before the payload of any resulting terminal fragment drops below I_{min}.

A specific CNVS configuration is considered structurally and cryptographically feasible if and only if the maximum semantically permissible fragmentation equals or exceeds the

minimum security requirement:
(44)

$m_{max} \geq m_{min}$

This feasibility condition formally guarantees that the system can achieve the target adversarial resistance η without sacrificing the operational computability of the global state.

Remark 17a.2 (Entropic Interpretation of Inference Probability)

The structural inference probability p_{inf} may increase over time as the adversarial coalition accumulates compromised fragment-level information, observable metadata, and partial structural correlations.

Let $H(S(t_0))$ denote the initial maximum Shannon entropy of the global state space prior to adversarial observation. Let $H(S(t) \mid W(t))$ denote the residual conditional entropy of the global state at time t, given the cumulative adversarial information W(t).

Assume $H(S(t_0)) > 0$ and $0 \leq \mathbb{E}[H(S(t) \mid W(t))] \leq H(S(t_0))$. We define the normalized residual entropy ratio:

$r(t) \triangleq \mathbb{E}[H(S(t) \mid W(t))] / H(S(t_0))$.

Thus:

$0 \leq r(t) \leq 1$.

A simple entropy-driven inference model may define the dynamic inference probability as:

$p_{inf}(t) \triangleq 1 - r(t)$.

Equivalently:

$p_{inf}(t) \triangleq 1 - \mathbb{E}[H(S(t) \mid W(t))] / H(S(t_0))$.

Under this model, the dynamic composite compromise probability becomes:

$p_{comp}(t) \triangleq q + (1 - q)\, p_{inf}(t)$.

Substituting the entropy-driven expression for $p_{inf}(t)$, we obtain:

$p_{comp}(t) = q + (1 - q)[1 - \mathbb{E}[H(S(t) \mid W(t))] / H(S(t_0))]$.

Equivalently:

$p_{comp}(t) = 1 - (1 - q) \cdot \mathbb{E}[H(S(t) \mid W(t))] / H(S(t_0))$.

The dependent-collusion bound therefore becomes time-dependent:

$\mathbb{P}(\mathrm{Rec}^{*}) \le p_{comp}(t)^{m(t)}$.

This does not imply unconditional dominance of fragmentation over entropy erosion. If $p_{comp}(t)$ approaches 1 too rapidly, the exponential bound may fail to converge to zero.

A sufficient asymptotic condition for security is:

$m(t)\,(-\ln p_{comp}(t)) \to \infty$.

Equivalently, if we define the residual compromise gap:

$\delta_p(t) \triangleq 1 - p_{comp}(t)$,

then a sufficient small-gap condition is:

$m(t)\,\delta_p(t) \to \infty$.

In the entropy-driven model above, this becomes:

$m(t)\,(1 - q) \cdot \mathbb{E}[H(S(t) \mid W(t))] \,/\, H(S(t_0)) \to \infty$.

Therefore, fragmentation suppresses dependent reconstruction only when the growth of the critical-fragment depth $m(t)$ dominates the rate at which residual entropy is depleted by adversarial knowledge accumulation.
This formulation preserves the thermodynamic interpretation while making the asymptotic security claim conditional, rate-aware, and mathematically defensible.

Note $\delta_p(t)$ is distinct from the fixed Hoeffding security margin δ introduced in Theorem 3. While δ measures the static acquisition-margin $\tau - q\,\bar{\omega}_k$ in the independent baseline, $\delta_p(t)$ measures the dynamic residual gap $1 - p_{comp}(t)$ in the dependent entropy-driven regime.

Remark 17a.3 (Worst-case leakage resilience)

The emergent security scaling demonstrated in Theorems 3 and 4 remains applicable even under a worst-case local leakage scenario
Assume a boundary condition where the local convergence function (Conv_σ) fails to project a minimized semantic view, granting the colluding verifiers absolute local knowledge of their assigned fragments. Formally, the Knowledge Restriction bound introduced in Section 6 collapses locally, yielding:

$\mathcal{K}(v, f) = I_{total}(f),\ \forall v \in \mathcal{V}_{adv},\ \forall f \in \mathrm{Ter}(t)$ such that $A_t(f, \xi) = v$. **(45)**

Even under this worst-case assumption, the asymptotic bound of Corollary 4.1 remains applicable provided that the composite compromise probability remains strictly sub-unitary:

$p_{comp} < 1$.

In that case:

$\lim_{m \to \infty} \mathbb{P}(Rec^{*}) = 0$.

This shows that worst-case local payload exposure does not by itself invalidate the dependent-collusion bound, as long as the residual inference condition still prevents p_{comp} from reaching 1.

Thus, the local verification mechanism and the fragmentation topology act as distinct defensive layers. The asymptotic claim remains conditional on the preservation of a strictly sub-unitary composite compromise probability.

Theorem Implications

This result formally generalizes the idealized independent-assignment model. It shows that exponential security scaling against coordinated collusion follows under the stated assumptions, provided that the inference probability of any single fragment remains strictly bounded by a constant smaller than one.

Remark 17a.4: Why No Classical Covariance Matrix is Required

In threshold-share cryptosystems, fragments are algebraically correlated shares of a common secret. For that reason, collusion analysis may require explicit covariance or reconstruction equations between shares.
CNVS does not model terminal fragments as algebraic shares of a monolithic payload. Terminal fragments are localized evaluative units whose external exposure is limited to measurement grids, task specifications, and reported observations. Their global meaning depends on hidden invariant binding and relational topology.

Therefore, a classical covariance matrix between algebraic shares is not the appropriate object for the CNVS security model.

This does not require assuming perfect semantic independence between fragments. By Lemma 10, topology and metadata may leak bounded information. The required condition is only that this leakage remains insufficient to determine the missing semantic payload or collapse its residual conditional min-entropy.

Accordingly, inter-fragment dependence is modeled through the bounded inference parameter p_{inf}, not through algebraic covariance.

The dependent-collusion analysis remains valid as long as each missing critical fragment retains positive residual non-inferability under the adversarial view.

18. Binding Entropy and Systemic Scaling interpretation

The structural growth of the CNVS framework increases the adversarial uncertainty associated with fragment assignment, hidden invariant binding, and relational topology. These sources of uncertainty must be distinguished.

At each assignment cycle, CNVS imposes a one-fragment-per-verifier constraint. Therefore, no active verifier receives more than one terminal fragment at the same time, and no terminal fragment is assigned to more than one active verifier.

Let

$Ter(t) = \{f_1, \ldots, f_k\}$

be the set of terminal fragments active at time t.

Let $\mathcal{V}$ be the finite verifier pool, with $Q = |\mathcal{V}|$, and let $\mathcal{V}_t \subseteq \mathcal{V}$ be the active verifier set selected at time t.

The assignment operator

$A_t : Ter(t) \times \Xi \to \mathcal{V}$

is subject to the injectivity constraint:

$\forall f_i, f_j \in Ter(t), f_i \neq f_j \Rightarrow A_t(f_i, \xi) \neq A_t(f_j, \xi)$.

Thus, for each random seed $\xi \in \Xi$, the map $A_t(\cdot, \xi)$ is an injective matching from terminal fragments to verifiers.

If $|\mathcal{V}_t| = k$, then A_t induces a bijection:

$A_t(\cdot, \xi) : Ter(t) \to \mathcal{V}_t$.

In the uniform bijective baseline, all bijections between Ter(t) and $\mathcal{V}_t$ are equiprobable. The number of admissible assignments is therefore:

$k!$,

and the corresponding assignment entropy is:

$H_{assign}(k) = \log_2(k!)$.

By Stirling's approximation:

$\log_2(k!) = \Theta(k \log_2 k)$.

This factorial term arises from the injective one-fragment-per-verifier matching constraint. It does not arise from unrestricted independent assignment with replacement.

If the active verifier set $\mathcal{V}_t$ itself is selected from a larger verifier pool $\mathcal{V}$ with $|\mathcal{V}| = Q \geq k$, then the number of admissible injective assignments is:

$Q! / (Q - k)!$,

and the corresponding assignment entropy is:

$H_{assign}(Q, k) = \log_2(Q! / (Q - k)!)$. **(46)**

The CNVS framework may also use non-uniform randomized matching, for example risk-weighted, criticality-weighted, or redundancy-aware assignment. Let $\mathcal{A}_{inj}(t)$ denote the set of admissible injective assignments at time t, and let $\mu_t(a)$ be the probability assigned to an injective assignment $a \in \mathcal{A}_{inj}(t)$. Then the general assignment entropy is:

$H_{assign}(t) = -\sum_{a \in \mathcal{A}\_inj(t)} \mu_t(a) \log_2 \mu_t(a)$. **(46a)**

The uniform bijective and injective cases are recovered when μ_t is uniform over the admissible assignment set.

CNVS also contains a second source of uncertainty: the hidden binding between terminal fragments and the internal invariant slots or relational positions used by global validation.

If the system internally binds k terminal fragments to k hidden validation slots through an unknown bijection, then the number of possible internal bindings is again:

$k!$,

with binding entropy:

$H_{bind}(k) = \log_2(k!)$.

This binding entropy is distinct from verifier-assignment entropy. Assignment determines which verifier receives which terminal fragment. Binding determines how terminal fragments are internally connected to hidden validation slots, invariant parameters, and relational constraints.

Finally, the hidden relational graph may contribute additional topological entropy.
Let $\mathcal{G}_t$ denote the admissible family of hidden relational graphs or structural bindings generated at time t. Then:

$H_{top}(t) = \log_2 |\mathcal{G}_t|$. **(47)**

The total structural uncertainty should therefore be understood as a joint entropy:

$H_{struct}(t) = H(A_t, B_t, G_t)$, **(48)**

where A_t denotes the injective verifier assignment, B_t denotes the hidden invariant binding, and G_t denotes the hidden relational topology.

If these sources are generated independently, the joint entropy decomposes additively:

$H_{struct}(t) = H_{assign}(t) + H_{bind}(t) + H_{top}(t)$. **(49)**

Without independence, this expression must be interpreted only as an upper decomposition, and implementation-specific lower bounds must be stated explicitly.

Consequently, the correct asymptotic interpretation is not that every CNVS uncertainty source is automatically factorial. Rather, factorial growth arises from injective matching and hidden bijective binding. Additional graph-topological uncertainty may further increase the adversarial search space.

Taking the limit as the system expands, CNVS structural uncertainty diverges whenever the admissible injective assignment space, hidden binding space, or topological graph family diverges:

$\lim_{m\to\infty} H_{struct}(t_m) = \infty.$ **(50)**

This divergence increases the adversarial search space for unauthorized reconstruction, provided that hidden binding and topology remain unavailable or only boundedly leaked according to Lemma 10.

Therefore, combinatorial entropy supports the CNVS security model as a structural uncertainty amplifier. It does not replace the probabilistic security bounds of Sections 15–17a; rather, it supplies the combinatorial substrate that makes hidden assignment, hidden binding, and hidden topology increasingly difficult to reconstruct as the system scales.

18a. Corollary: Global Veto Property

If at least one critical fragment essential to the evaluation of a global invariant $c_i \in C$ remains outside adversarial control and retains positive residual conditional min-entropy under the adversarial view, deterministic reconstruction of a globally valid state is blocked. Therefore any incorrect adversarial estimation of the missing structural or relational contribution will force the invariant to fail, triggering the absolute Global Veto:

$V_G(S') = 0$

and resulting in the immediate topological rejection of the candidate state S'.

Operational Remark 18a. — Authenticated Verifier Identities and Non-Paralyzing Validation

In concrete CNVS implementations, verifiers are assumed to be protocol-recognized entities bound to authenticated cryptographic keys. The global validation layer does not accept arbitrary anonymous submissions. Invalid, unauthenticated, duplicated, expired, or

unauthorized verification objects are rejected at the admissibility layer before reaching global validation.

Accordingly, the Global Veto Property applies only to well-formed candidate transitions submitted through authorized verifier identities and admissible validation channels. If a malicious or colluding verifier submits false, inconsistent, duplicated, or fraudulent verification objects, the authenticated identity associated with the corresponding cryptographic key can be deterministically identified, isolated from subsequent validation rounds, penalized, or excluded according to the implementation rules.

Malicious or false submissions therefore produce deterministic rejection, accountability, penalty, or verifier exclusion; they do not create an unbounded right to force repeated global validation.

This operational requirement does not replace the formal CNVS security theorem. It specifies the admissibility conditions under which the global validation function remains finite, authenticated, and non-paralyzing.

18b. Critical Fragment Principle

The security of the CNVS framework does not scale merely with the percentage of verifiers under adversarial control. It depends on whether the adversarial coalition can eliminate the residual uncertainty of every critical fragment required for global reconstruction.

Let $\mathcal{V}_{adv} \subset \mathcal{V}$ be the adversarial coalition, and let $F_c \subset Ter(t)$ be the subset of terminal fragments assigned to colluding verifiers.

A terminal fragment $f^* \in Ter(t)$ is called critical if its internal payload, structural role, or invariant binding is necessary for reconstructing a globally admissible candidate state.

A critical fragment f^* is called residual non-inferable with respect to the adversarial view if its internal semantic payload d^* satisfies:

$$H_\infty(d^* \mid View_{adv}) \geq h^*, \quad \textbf{(51)}$$

for some $h^* > 0$.

Equivalently, the optimal adversarial guessing probability is bounded by:

$$\mathbb{P}_{guess}(d^* \mid View_{adv}) \leq 2^{-h^{**}}. \quad \textbf{(52)}$$

Therefore, if at least one critical fragment f^* remains outside adversarial control and satisfies residual non-inferability, then any unauthorized reconstruction that requires d^* is bounded by:

$\mathbb{P}(\text{Rec}^*) \leq 2^{-h^{\wedge *}}$.

More generally, let $F_{miss} = \{f_1, \ldots, f_r\}$ be the set of missing critical fragments required for reconstruction, and let $D_{miss} = (d_1, \ldots, d_r)$ denote their internal semantic payloads.

We define the residual critical min-entropy as:

$H_{crit} \triangleq H_\infty(D_{miss} \mid View_{adv})$. **(53)**

If:

$H_{crit} > 0$,

then the optimal adversarial guessing probability for the missing critical payload vector satisfies:

$\mathbb{P}_{guess}(D_{miss} \mid View_{adv}) \leq 2^{-H\_crit}$. **(54)**

Accordingly, any unauthorized reconstruction event Rec^* requiring the correct recovery of D_{miss} is bounded by:

$\mathbb{P}(\text{Rec}^*) \leq 2^{-H\_crit}$.

This is the correct information-theoretic form of the Critical Fragment Principle.

The relevant security quantity is not the total information size $I_{total}(f^*)$ of the missing fragment. The relevant quantity is the residual conditional min-entropy that remains after conditioning on everything available to the adversary.

Thus, the previous informal bound based on $I_{total}(f^*)$ must be replaced by the residual min-entropy bound:

$\mathbb{P}(\text{Rec}^*) \leq 2^{-H\_\infty(D\_miss \mid view\_adv)}$. **(55)**

Consequently, extensive collusion does not imply deterministic reconstruction if at least one reconstruction-critical component remains outside adversarial control and retains strictly positive residual conditional min-entropy.

This principle is conditional: if the adversarial view collapses the residual min-entropy of every critical missing fragment to zero, then the Critical Fragment Principle no longer provides protection. CNVS security therefore requires that critical fragments remain not only uncompromised, but also non-inferable under the hidden-invariant and bounded-leakage conditions of Lemmas 8 and 10.

Remark 18.1 (Gold-Custody Invariant)

Suppose a CNVS state encodes a physical gold-custody verification process.
A colluding coalition controls 99 terminal fragments and obtains, under the pessimistic semantic exposure model, 99 local payloads corresponding to 99 kg of gold.

The coalition therefore knows that the exposed local payloads sum to 99 kg.

However, the coalition does not know the internal instantiated invariant C_{int}. In particular, it does not know whether the global validation condition requires:

- total mass equal to 100 kg;
- total mass equal to 120 kg;
- minimum mass above a hidden threshold;
- a mass-purity relation;
- a vault-distribution constraint;
- a temporal custody invariant;
- a relational mapping between different physical deposits.

Therefore, from the adversarial view alone, the missing fragment is not determined.

If the hidden instantiated invariant were publicly known to be: $x_1 + ... + x_{100} = 100$ kg,

then the missing value would be algebraically inferable: $x_{100} = 100 \text{ kg} - 99 \text{ kg} = 1$ kg.

But this is not the CNVS adversarial model.
In CNVS, the adversary may know the general class of conservation-type invariants, but not the internal invariant instance, its hidden parameters, or its relational binding.

Thus, possessing 99 kg does not imply knowing that the missing fragment must be 1 kg.
The missing fragment remains non-inferable as long as:

$H_\infty(D_{miss} \mid W_{adv}, View_{adv}, C_{pub}) \geq h_{min} > 0.$

Remark 18.2 (Reactor Example)

To clarify the ontology of a terminal fragment within the CNVS framework, consider the controlled verification of a classified reactor construction process.

In a traditional data-sharding model, fragmentation would correspond to cutting the reactor blueprint into several pieces and distributing those pieces to different workers. In that case,

each fragment would be a syntactic or cryptographic share of the global semantic payload. If sufficiently many workers colluded, they could attempt to reconstruct the underlying blueprint.

CNVS does not use this model.

In CNVS, terminal fragments are closed native evaluative units. Each fragment may contain an internal payload d_i within the system boundary, but the external verifier does not receive d_i. The verifier receives only a local measurement grid or task specification, performs an independent observation obs_i, and reports obs_i back to the system.

For example, the verifier may be instructed to measure the length and diameter of a specific screw. The verifier can execute this local task, but does not receive the internal expected value d_i, the global reactor design, the hidden invariant C_{int}, or the relational binding that explains how this local measurement participates in global validation.

Thus, the local task is semantically meaningful at the operational level, but not globally reconstructive by itself.

The topology and task structure may leak limited information about the system.
CNVS therefore does not require perfect zero mutual information between metadata and payload. Instead, by Lemma 10, such leakage is bounded:

$I(X_s ; M_s) \leq \gamma_{top}$.

Moreover, by Lemma 8, the adversarial view must not collapse the residual conditional min-entropy of any missing critical payload. For a missing critical payload d_{miss}, CNVS requires:

$H_\infty(d_{miss} \mid View_{adv}) \geq h_{min} > 0$.

The reactor example should therefore be understood through three adversarial scenarios.

Scenario 1. The adversary controls many local payloads, but lacks hidden binding and instantiated invariants.
The adversary may obtain many local payloads under the pessimistic semantic exposure model. However, without the hidden invariant instance C_{int}, the internal parameters Θ_C, and the relational binding R_{int}, those local payloads do not necessarily determine the missing critical payload.

Security in this scenario follows if the missing critical component retains positive residual min-entropy:

$H_\infty(d_{miss} \mid W_k, M_s, C_{pub}) \geq h_{min} > 0$.

Scenario 2. The adversary observes topology or metadata, but does not control the relevant payloads.

Topology and metadata may reduce uncertainty, but only within the bounded-leakage model. Observing M_s may reveal limited information about the verification structure, but does not by itself imply deterministic reconstruction if:

$I(X_s ; M_s) \leq \gamma_{top}$

and residual uncertainty remains positive after conditioning on the adversarial view.

Scenario 3. The adversary controls many payloads and observes substantial topology. This is the strongest case. CNVS does not claim unconditional security here. The system remains protected only if at least one reconstruction-critical component remains both uncompromised and non-inferable under the adversarial view.

Formally, if reconstruction requires a missing critical payload d_{miss} and:

$H_\infty(d_{miss} \mid View_{adv}) \geq h_{min} > 0,$

then:

$\mathbb{P}_{guess}(d_{miss} \mid View_{adv}) \leq 2^{-h\_min}.$

Accordingly, deterministic reconstruction is blocked only while the residual min-entropy condition holds.

If, instead, the adversary obtains the compromised payloads, the relevant topology, the instantiated hidden invariant C_{int}, and enough information to reduce:

$H_\infty(d_{miss} \mid View_{adv})$

to zero, then this specific CNVS security condition fails.

Therefore, the reactor example does not establish unconditional secrecy. It illustrates the CNVS principle that local measurement tasks, hidden invariant binding, bounded metadata leakage, and residual min-entropy jointly prevent deterministic reconstruction under explicit assumptions.

19. Scientific Positioning

The CNVS architecture synthesizes principles from Shannon Information Theory, probabilistic combinatorics, structural graph theory, and distributed formal verification into a unified mathematical framework.

Crucially, CNVS differs structurally from traditional threshold cryptography (e.g., Shamir's Secret Sharing). In standard threshold models, the fragment (the "share") intrinsically contains a mathematical projection of the plaintext payload.

In the CNVS framework, the verifier is never provided with a data share containing the internal semantic payload. Instead, the verifier receives strictly bounded metadata dictating a localized measurement task, subsequently producing observational data used solely for convergence verification. This epistemic decoupling shifts the security analysis away from cryptographic key-splitting and toward bounded topological leakage, hidden binding, and residual non-inferability.

Demarcation from Threshold Cryptography (Shamir Secret Sharing)

Traditional decentralized confidentiality relies heavily on threshold schemes like Shamir Secret Sharing (SSS). In SSS, the native payload is mathematically divided into polynomial shares; thus, the fragment itself *is* a cryptographic projection of the semantic payload. If an adversary gathers a threshold τ of shares, algebraic reconstruction is deterministic.
CNVS differs from this paradigm. Terminal fragments in CNVS do not carry polynomial shares of the native payload ($d \in D_\sigma$); they carry autonomous measurement grids ($I_{metadata}$). The global state is validated through observational convergence rather than algebraic threshold reassembly. Therefore, CNVS is not primarily exposed to polynomial-interpolation reconstruction in the same way as threshold-share schemes.

Demarcation from Secure Multi-Party Computation (SMPC)

Secure Multi-Party Computation allows joint function evaluation over private inputs without revealing the inputs themselves. While sharing the goal of privacy-preserving evaluation, SMPC traditionally operates within a cryptographic computation model and may require non-trivial cryptographic machinery (e.g., garbled circuits or homomorphic encryption) to compute a function securely. CNVS, by contrast, models verification through restricted local observation, randomized assignment, and hidden global binding. It uses external verifiers as restricted local observers and analyzes security through hidden-invariant residual non-inferability and bounded topological leakage.
This places CNVS in a different design space from SMPC, especially when verification involves physical or empirical observations.

Demarcation from Verifiable Computation (VC) and zk-SNARKs

In Verifiable Computation frameworks, such as zk-SNARKs, a prover mathematically demonstrates the correct execution of a function $f(x)$ without revealing the input x. While superficially similar in its privacy-preserving goals, CNVS operates under a different formal ontology. In CNVS, the external verifier is not a cryptographic prover generating a mathematical proof of a known computation; rather, it acts as a physical oracle executing a real-world measurement. The verifier in CNVS does not possess the hidden input to prove it. Consequently, CNVS security is not primarily modeled through proof-generation hardness,

but through restricted verifier knowledge, hidden invariant binding, and residual non-inferability.

Demarcation from Probabilistically Checkable Proofs (PCP)

The PCP theorem allows the verification of global proof validity by means of a randomized verifier that queries only a constant number of locations in an encoded proof string. While PCP techniques use local proof queries to certify global properties, the queried positions directly belong to the proof object itself; they are not external empirical observers and are not semantically blind in the CNVS sense. In contrast, the CNVS framework strictly enforces the Knowledge Restriction bound introduced in Section 6. The terminal fragment provides a measurement grid whose exposed information remains bounded and non-reconstructive with respect to the global semantic payload, in accordance with Lemma 10.

Demarcation from Blind Quantum Computing (BQC)

Blind Quantum Computing is conceptually adjacent to CNVS, as it allows a client to delegate a computation to a server without revealing the delegated circuit or the underlying data. However, the demarcation is structural, physical, and operational. First, BQC achieves blindness through the delegation of quantum states and rotational encryption requiring quantum hardware. CNVS operates within a classical verification setting and seeks restricted verifier knowledge through randomized assignment, structural non-uniformity, and hidden binding. Second, BQC servers act as passive computational executors with no localized verification; they compute functions blindly without checking the semantic alignment of their outputs. Conversely, CNVS nodes function as restricted local empirical observers: each terminal fragment enforces a local verification function (V_L) that requires a real-world empirical observation (obs) to satisfy the local convergence predicate defined by the measurement-grid constraints. Furthermore, CNVS natively integrates a Global Veto mechanism (V_G) over structural invariants (C), a holistic state-validation feature not inherently present in the purely computational delegation of BQC.

Demarcation from Classical Distributed Verification

Classical distributed verification often assumes that local nodes verify parts of a distributed state or computation. CNVS differs by making global admissibility explicitly non-reducible to local verification alone.

Even if all terminal fragments are locally admissible, the candidate state may still be globally rejected if relational consistency or invariant satisfaction fails. This is formalized by the Global Veto:

$V_G(S) = 1$

only when local admissibility, relational consistency, and global invariant satisfaction hold jointly.

Summary

CNVS should therefore be understood as a candidate formal class of closed native verification systems characterized by:

1. internal payloads not ordinarily disclosed to verifiers;
2. external measurement-grid based observation;
3. randomized assignment of terminal evaluative units;
4. hidden invariant binding and relational topology;
5. bounded topological leakage;
6. residual non-inferability of critical fragments;
7. global admissibility enforced by systemic veto.

The framework does not claim unconditional superiority over existing cryptographic or distributed verification systems. Its contribution is the formalization of a different verification architecture whose security properties are conditional on explicit assumptions: bounded leakage, hidden instantiated invariants, residual min-entropy, randomized assignment, and sub-unitary composite compromise probability.

20. Open Problems

While this paper establishes the foundational formal proofs of the CNVS architecture, several advanced vectors require further formalization:

1. Cryptographic Reductions: Formal mapping of the local knowledge restriction bounds to standard hard computational problems (e.g., Learning With Errors (LWE) or Discrete Logarithm).
2. Information-Theoretic Lower Bounds: Derivation of the absolute optimal adversarial allocation strategies and the corresponding tightest bounds for $I_{metadata}$ expansion.
3. Empirical Validation: Extensive stress-testing of the asymptotic bounds ($\mathbb{P}(Rec^{*}) \to 0$) via large-scale Monte Carlo systemic simulations under dynamically shifting adversarial assignment (A_t).

Appendix A. Minimal Formal Definition

A structure

$M = (\boldsymbol{\mathcal{S}}, E, R, C, D, A, V_L, V_G, Rec, \mathcal{K}(v, f))$

is a Closed Native Verification System if and only if:

1. $\boldsymbol{\mathcal{S}}$ is a typed finite-binary structural universe.
2. Raw structural membership belongs to the candidate state layer: an element s may belong to E_{cand} independently of its current verification status.
3. Terminal admissibility requires local verification: $Adm_L(s) = 1 \Leftrightarrow \pi_1(V_L(s)) = 1$.
4. Accepted state validity requires global verification: $S \in \Sigma^+ \Leftrightarrow V_G(S) = 1$.
5. Global verification requires terminal admissibility, relational consistency, and invariant satisfaction.
6. Decomposition is finite, recursive, and reconstructible.
7. Verifier knowledge is strictly restricted.
8. Terminal assignments are randomized.
9. Invalid candidate states are rejected from accepted state evolution; their rejection does not imply that their candidate elements were structurally non-existent.
10. The symbols V_L and V_G denote respectively the Local Verification Function and the Global Verification Function defined in this paper.

AI-Assistance Disclosure

The Author acknowledges the use of AI tools for editorial refinement, language optimization, formatting support, consistency checking, and assistance in the formal correction of notation, domains, and mathematical expressions. The conceptual architecture, core theoretical framework, axiomatic structure, original mathematical relations, intended formal meaning of the equations, and scientific claims of the CNVS framework were developed and determined by the author. The author reviewed, selected, and approved the final formal formulation and assumes full scientific responsibility for the content of this manuscript.

END DOCUMENT

Author:
Massimo Comitato, Milano (MI),
Independent Researcher,
massimocomitato@gmail.com
Italy, 13.06.2026