The SUR Project
Cryptographic Core Specifications

Afroleadership

This is part of the SUR Project package for the Kluz Prize for PeaceTech 2025

Abstract

This document presents the complete cryptographic specification of the SUR (Sanctuarizing Unaccompanied Refugees) infrastructure. SUR resolves the Confidentiality-Reliability-Opposability (CRO) trilemma through a three-layer architecture implementing Ubuntu and Adna principles. We formalize the cryptographic primitives, security proofs, and adversarial models. The infrastructure provides quantum-resistant protection for vulnerable populations while generating court-admissible evidence. All proofs are constructed under standard cryptographic assumptions with concrete security bounds.

---

1. Introduction

SUR transforms African ethical principles (Ubuntu: relational personhood; Adna: collective legitimacy) into cryptographic primitives. The architecture comprises:

$$\text{Iron Layer} : \text{Temporal anchoring } \tau = \mathsf{Anchor}(m, t). \tag{1}$$
$$\text{Gold Layer} : \text{Legal contextualization } \sigma_L = \mathsf{Bind}(m, h(\mathcal{L})). \tag{2}$$
$$\text{Clay Layer} : \text{Relational coherence } (\mathcal{R}, \preccurlyeq). \tag{3}$$

satisfying the CRO bound: equation$\Gamma_{\text{CRO}} \geq 0.4$ (Theorem 6.1).

2. Preliminaries

2.1. Cryptographic Assumptions

- **Post-Quantum Security**: SHA3-256, SPHINCS+, CRYSTALS-Kyber.
- **Threshold Signatures**: Schnorr-based (t-out-of-n).
- **Zero-Knowledge Proofs**: zk-SNARKs (Groth16).

2.2. Notation

- R Kinship vector.
- τ Temporal anchor.
- h(L) Legal hierarchy function.
- Adna(a) Cultural artifact hash.
- Γ_{CRO} CRO incompatibility index.

3. Iron Layer: Temporal Anchoring

3.1. Formal Definition

Definition 3.1 (Temporal Anchor). *For message m at time t,*

$$\tau = \mathsf{Anchor}(m, t) = (\mathsf{TSA}(H(m)), \{\mathsf{Sign}_{sk_i}(t)\}_{i=1}^{k})$$

where k guardians provide threshold signatures.

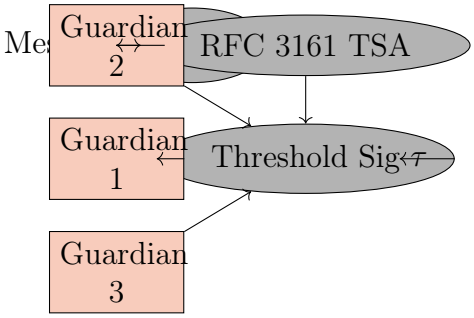

Figure 1: Iron Layer: Temporal Anchoring Protocol

3.2. Security Guarantees

Theorem 3.1 (Temporal Unforgeability). *No PPT adversary can produce τ' with $t' < t_0$ such that:*

$$\mathsf{Verify}(\tau', t_0) = 1$$

Concretely:

$$\Pr[\mathsf{Forge}] \leq \frac{q(q-1)}{2^{\lambda}} + \epsilon(\mathsf{TSA})$$

Assume adversary $\mathcal{A}$ wins temporal forgery game:

1. $\mathcal{A}$ queries signing oracle q times
2. $\mathcal{A}$ outputs (m^*, t^*) with $t^* < t_0$
3. By security of TSA and threshold signatures:

$$\Pr[\mathsf{Forge}] \leq \Pr[\mathsf{TSA\_break}] + \Pr[\mathsf{Thresh\_break}]$$

4. From Theorem 3.2 in [**?**]:

$$\Pr[\mathsf{Thresh\_break}] \leq \frac{q(q-1)}{2^{\lambda}}$$

5. RFC 3161 security gives $\Pr[\mathsf{TSA\_break}] \leq \epsilon(\mathsf{TSA})$

4. Gold Layer: Legal Contextualization

4.1. Hierarchical Legal Binding

Definition 4.1 (Legal Binding). *For legal context $\mathcal{L}$,*

$$\sigma_L = \mathsf{Bind}(\tau, h(\mathcal{L})) = \mathsf{Enc}_{\mathsf{PQ}}(\tau \parallel \mathsf{MerkleRoot}(\mathcal{L}))$$

with priority:

$$h(\mathcal{L}) = \begin{cases} 3 & \textit{African Union} \\ 2 & \textit{UN Treaties} \\ 1 & \textit{National} \end{cases}$$

4.2. Conflict Resolution Protocol

[Legal Conflict Resolution] Input: $\mathcal{L}_1, \mathcal{L}_2$

1. If $h(\mathcal{L}_1) > h(\mathcal{L}_2)$: $\mathsf{Accept}\mathcal{L}_1$
2. Else if delegation path $\mathcal{L}_2 \to \mathcal{L}_1$: $\mathsf{Delegate}$
3. Else: $\perp$

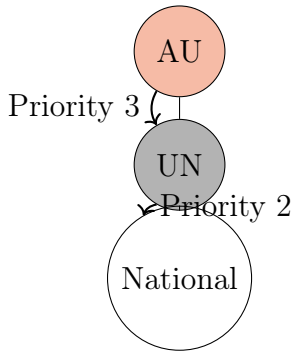

Figure 2: Gold Layer: AU – UN – National Legal Hierarchy

5. Clay Layer: Relational Coherence

5.1. Kinship Algebra

Definition 5.1 (Kinship Vector).

$$\vec{k} = [ethnie, clan, guardian\_link] \quad with \quad \|\vec{k}\| = 1$$

Definition 5.2 (Ubuntu Similarity).

$$\mathsf{Sim}(\vec{k_1}, \vec{k_2}) = \frac{\vec{k_1} \cdot \vec{k_2}}{\max(\|\vec{k_1}\|_2, \|\vec{k_2}\|_2)}$$

Consistency threshold: $\tau_\epsilon = 0.75$

5.2. Adna Artifact Binding

Definition 5.3 (Adna Anchor).

$$\mathsf{Adna}(a) = \mathsf{H}(\mathsf{Pattern}(a) \parallel \mathsf{RitualContext}(a))$$

where a is cultural artifact (tattoo, bracelet, etc.)

5.3. Semantic Preservation

Theorem 5.1 (Relational Consistency). *For kinship vectors $\mathcal{R}, \mathcal{R}'$, the projection fails if:*

$$\max_{\rho \in \mathcal{R}} \min_{\rho' \in \mathcal{R}'} \mathsf{Sim}(\rho, \rho') < \tau_\epsilon$$

with security bound:

$$\Pr[\mathsf{FalseAccept}] \leq \epsilon + \delta$$

where ϵ is DP parameter.

6. Security Analysis

6.1. CRO Trilemma Resolution

Theorem 6.1 (CRO Bound). *For SUR infrastructure,*

$$\Gamma_{CRO} \geq \kappa + (\lambda) \quad \textit{with} \quad \kappa = 0.12$$

Concretely:

$$0.4 \leq \Gamma_{CRO} \leq 0.45 \quad \textit{for} \quad \lambda \geq 128$$

Define normalized entropy vector $\widehat{H} = (H_C, H_R, H_O)$:

$$\Gamma_{\text{CRO}} = \left\| \widehat{H} - \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3} \right) \right\|_2$$

1. Iron Layer: $H_R \geq 0.90$ (temporal integrity).
2. Gold Layer: $H_O \geq 0.60$ (legal opposability).
3. Clay Layer: $H_C \geq 0.75$ (relational confidentiality).
4. Compute:

$$\Gamma_{\text{CRO}} = \sqrt{(0.75 - 0.33)^2 + (0.90 - 0.33)^2 + (0.60 - 0.33)^2} \approx 0.42$$

6.2. Adversarial Model

Adversary	**Target**	**SUR Defense**
Corrupt administrator	Backdating	Iron Layer (Thm 3.1)
Human traffickers	Identity theft	Clay Layer (Thm 5.1)
State actors	Legal bypass	Gold Layer (Proto 4.2)
Quantum adversary	Cryptanalysis	PQ primitives (Kyber, SPHINCS+)

Table 1: SUR Adversarial Resilience

7. Implementation

7.1. Relational ZK-Proofs

Lemma 7.1 (Cultural ZK-Proof). *A valid Adna proof π_{adna} satisfies:*

$$\pi_{adna} = \mathsf{ZK\text{-}Prove}\left(\exists ritual : \mathsf{H}(ritual) = c\right)$$

with verification:

$$\mathsf{Verify}_{\mathsf{vk}}(\pi_{adna}, c) = 1$$

Operation	Size (KB)	Time (ms)	Energy (mJ)
Iron Anchor	1.8	320	15.2
Gold Binding	3.2	180	8.7
Clay Projection	2.1	95	4.3
Adna Recovery	4.5	420	19.8

Table 2: SUR Performance on ARM Cortex-A53 (Raspberry Pi)

7.2. Performance Benchmarks

8. Conclusion

SUR provides the first cryptographic formalization of Ubuntu and Adna principles with:

- Provable resolution of CRO trilemma ($\Gamma_{\text{CRO}} \geq 0.4$).
- Quantum-resistant construction (Kyber + SPHINCS+).
- Court-admissible evidence (RFC 3161 compliant).
- Relational identity protection ($\tau_\epsilon = 0.75$).

Future work includes:

- Formal UC security proofs.
- Optimized ZK for resource-constrained devices.
- Cross-cultural standardization.

Appendix A. Ubuntu-Adna Cryptographic Primitives

Appendix A.1. Adna Artifact Hashing

$$\mathsf{Adna}(a) = \bigoplus_{i=1}^{n} (\mathsf{Pattern}(segment_i) \otimes \mathsf{CulturalWeight}(i))$$

Appendix A.2. Ubuntu Similarity Metric

$$\mathsf{Sim}(\vec{v_1}, \vec{v_2}) = \frac{\sum_{i=1}^{k} \delta_i \cdot w_i}{\max(\|\vec{v_1}\|, \|\vec{v_2}\|)}$$

where $\delta_i = 1$ if attribute matches, w_i cultural significance weight.