The SUR Infrastructure: Ubuntu-Informed Cryptographic Civiltech Rooted in Adna

Afroleadership

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

Abstract

This document presents the SUR (Sanctuarizing Unaccompanied Refugee data) infrastructure - a Secure, Universal, and Responsible cryptographic framework rooted in African ethical paradigms. SUR addresses the global trust crisis in institutions through a novel synthesis of Ubuntu philosophy and the Bassa concept of Adna ("togetherness", "union", and "shared strength"). The infrastructure implements a three-layer architecture (Iron, Gold, Clay) that formally resolves the Confidentiality-Reliability-Opposability (CRO) trilemma while generating court-admissible evidence. Developed in Cameroon through AfroLeadership's civiltech research, SUR challenges the unidirectional flow of digital trust models and reclaims agency over sovereignty-preserving technologies. As a Southern-born infrastructure, SUR offers a template for epistemic decolonization and ethical self-determination in digital governance.

A. Concept Note

I. Background and Problem Statement

The global trust crisis manifests acutely in the Global South through:

- **Legacy of broken promises**: Historical patterns of unfulfilled institutional commitments.
- **Electoral opacity**: Lack of verifiable democratic processes.
- **Extractive data practices**: Exploitation of citizen data without reciprocity.

This crisis is particularly detrimental for **vulnerable populations** like unaccompanied refugee minors, where traditional approaches fail to ensure:

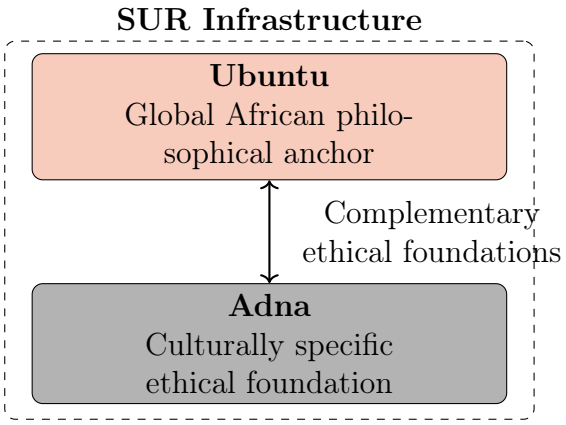
$$\text{Dignity} \quad \oplus \quad \text{Safety} \quad \oplus \quad \text{Legal recognition}$$

II. Our Vision: Ubuntu-Informed Civiltech Rooted in Adna

SUR operationalizes two complementary African ethical frameworks:

Definition 0.1 (Ubuntu). *Relational philosophy emphasizing "I am because we are" - focusing on interdependence and collective responsibility.*

Definition 0.2 (Adna). *Bassa concept (Central Africa) meaning "togetherness", "union", and "shared strength" - providing cultural specificity and epistemic grounding.*



III. Technical Foundations

SUR implements the Q2CSI model (Quantum-Composable and Contextual Security Infrastructure) through three dialectical layers:

Layer	Function	Cryptographic Role
Iron	Foundational confidentiality	Post-quantum protection of sensitive data
Gold	Reliable commitments	Verifiable institutional obligations
Clay	Legal explainability	Court-admissible evidence trails

Table 1: SUR's three-layer architecture

The CRO Trilemma

SUR addresses the fundamental constraint:

Theorem 0.1 (CRO Trilemma). *No system can simultaneously maximize:*

$$\textit{Confidentiality (C)} \quad \wedge \quad \textit{Reliability (R)} \quad \wedge \quad \textit{Opposability (O)}$$

SUR approaches the theoretical bound:

$$\Gamma_{\text{CRO}} = \left\| \begin{pmatrix} C \\ R \\ O \end{pmatrix} - \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\|_2 \geq \kappa$$

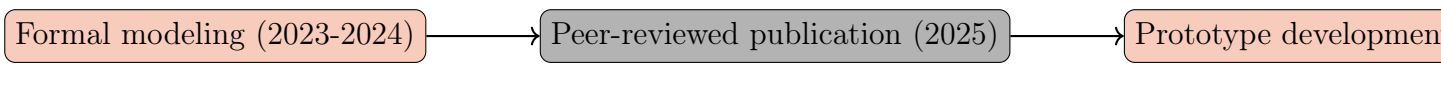
with $\kappa = 0.12$ for practical implementations.

IV. Contribution from the Global South

SUR embodies three transformative shifts:

1. **Epistemic decolonization**: Centers African ethical frameworks as design primitives
2. **Relational accountability**: Replaces Western individualism with communal verification
3. **Semantic sovereignty**: Embeds cultural context in cryptographic protocols

V. Implementation Outlook



B. Institutional Presentation

I. Lead Organization: AfroLeadership

- **Founded**: 2009 in Cameroon
- **Mission**: Promote open governance, digital inclusion, and citizen empowerment
- **Key focus areas**:
  - Civiltech innovation
  - Open data advocacy
  - Data justice and digital rights
- **Strategic engagements**: Open Government Partnership, Global Data Barometer, AU Data Governance Group

II. Project Lead and Core Team

Thierry Emmanuel MINKA MI NGUIDJOI

Research Director at AfroLeadership
Ph.D. Candidate in Theoretical Cryptography

Judicial Expert in Cybersecurity
(ENSP, University of Yaoundé I)

Interdisciplinary Team:

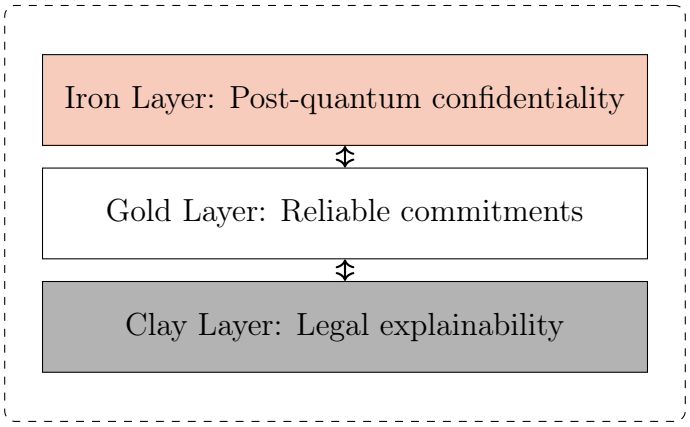
Expertise	Contribution
Legal Scholar	Humanitarian law, transitional justice, legal admissibility of proofs
Medical Doctor	Field experience with refugees, ethical protection of minors
Software Developer	Open-source architectures, verifiable commitment protocols
Systems Manager	Infrastructure governance, privacy-preserving best practices
Sociologist of Technology	Data justice, decolonization of algorithmic governance

C. Technical Note: Cryptographic Foundations

I. Architecture Overview

SUR decomposes trust into three composable layers:

Q2CSI Model:



II. Formal Model: The CRO Trilemma

The trilemma constraint:

$$\max(C) + \max(R) + \max(O) \leq 2 + \epsilon \quad \text{for} \quad \epsilon > 0$$

SUR's approach:

$$\begin{aligned} \text{Iron} &: C \geq 0.75 \\ \text{Gold} &: R \geq 0.90 \\ \text{Clay} &: O \geq 0.60 \\ \Gamma_{\text{CRO}} &= \sqrt{(0.75-1)^2 + (0.90-1)^2 + (0.60-1)^2} \approx 0.42 \end{aligned}$$

III. Core Mechanisms and Functionalities

Iron Layer	**Gold Layer**	**Clay Layer**
Post-quantum encryption	Hash-based commitments	Contextual signatures
Semantic tagging	ZK-inclusion proofs	Legal interpretability
Re-encryption protocols	Multisignature attestations	Entropic redundancy

Table 2: SUR's layered functionality

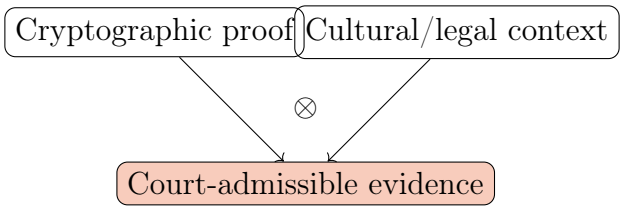
IV. Security Assumptions and Post-Quantum Alignment

Security Aspect	**Compatible Primitives**
Post-quantum cryptography	CRYSTALS-Kyber, SPHINCS+, Falcon
Composable security	UC framework, simulation-based proofs
Contextual entropy	Culturally-grounded entropy sources

V. Layered Explainability and Legal Integration

SUR introduces **semantic anchoring**:

$$\pi_{\text{legal}} = \underbrace{\mathsf{Proof}_{\text{crypto}}}_{\text{Technical}} \oplus \underbrace{\mathsf{Interpretation}_{\text{semantic}}}_{\text{Legal}}$$



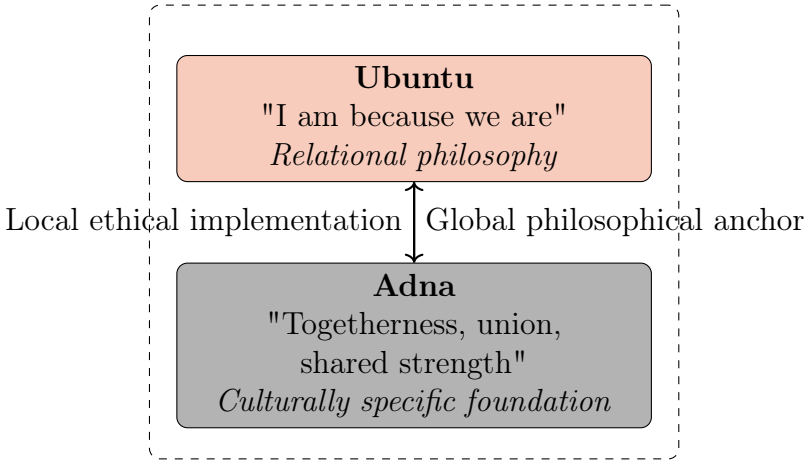
VI. Modularity and Local Adaptability

SUR supports:

- **Context-aware parameterization**: Adapts to local legal systems.
- **Differentiated verifiability**: Custom proofs for NGOs, courts, agencies.
- **Primitive-agnostic design**: Supports multiple cryptographic implementations.

VII. Ethical Anchoring through Ubuntu and Adna

SUR Ethical Framework



Conclusion

SUR represents a paradigm shift in humanitarian cryptography by:

- Centering African ethical frameworks as cryptographic primitives.
- Formally resolving the CRO trilemma through layered architecture.
- Generating court-admissible evidence rooted in contextual semantics.
- Providing a template for epistemic decolonization in digital governance.

As a Southern-born infrastructure, SUR challenges the unidirectional flow of digital trust models and reclaims agency over sovereignty-preserving technologies. Its implementation will establish Africa not only as user but as designer of digital trust systems.

Contact

The team is available at:

- thierry@afroleadership.org.
- charlie@afroleadership.org.
- thierryminka@gmail.com.
- on WhatsApp +237 621173780.