

Hachem Nasri

Protocol Engineer & Independent Researcher

 Portfolio |  github.com/Phig0r |  phigor.arc@gmail.com

Research Statement

Protocol Engineer & Independent Researcher architecting the infrastructure for Digital Integrity. I design secure, modular systems that solve the tension between privacy and transparency, engineering protocols that enforce verifiable correctness while overcoming fundamental constraints in scalability and identity.

Education

2022 - Present **Bachelor of Science in Computer Science**

Institut Supérieur d'Informatique et des Technologies de Communication de Sousse

Expected Graduation: June 2026


Research Projects

Attestation: Privacy-Preserving Airdrop Protocol  Source & Docs

- **The Problem:** Public ledger interactions expose user financial history (doxxing) and incur high gas costs for on-chain whitelist storage ($O(n)$ scaling).
- **The Solution:** Designed a privacy-first protocol using **Hierarchical Deterministic (HD) Keys** and **ZK-SNARKs**. Users prove ownership of a hidden key derived from an offline Master Key, decoupling the claim from their identity.
- **Key Engineering:** Implemented a custom **Circom** circuit for cryptographic ownership verification and used **Merkle Trees** for efficient storage, achieving $O(1)$ **verification cost** while maintaining cryptographically secure anonymity.

Provenance: Secure Digital Twin System  Source & Docs

- **The Problem:** Establishing a trusted "Digital Twin" is vulnerable to hardware cloning attacks, severing the link between a physical asset and its on-chain identity.
- **The Solution:** Engineered a cryptographically secure protocol using **PUF-hardware** challenges to bind physical items to the blockchain, ensuring unclonable authentication.
- **Key Engineering:** Architected the system using the **Diamond Standard (EIP-2535)** to modularize complex logic into infinite "Facets," overcoming the 24KB EVM contract size limit for scalability.

Decentralized Certificate System  Source & Docs

- **The Problem:** Digital credentials lack a standardized, trustless verification layer, making them susceptible to forgery and centralized data loss.
- **The Solution:** Engineered a credential protocol using **Soulbound Tokens (SBTs)** with overridden transfer logic to cryptographically bind assets to identity, preventing unauthorized transfers.
- **Key Engineering:** Implemented granular **Role-Based Access Control (RBAC)** for secure issuance and achieved **97% test coverage**, ensuring the integrity of the verification layer.

Technical Expertise

Languages	Solidity (Yul/Assembly), Circom, TypeScript, Python.
Cryptography	Zero-Knowledge Proofs (SNARKs), Merkle Trees, HD Wallets, PUFs.
Architecture	EIP-2535 (Diamond Standard), State Machine Design, RBAC Modeling.
Tooling	Hardhat, SnarkJS, Ethers.js, React.js, Git.
Research Focus	Privacy-Enhancing Technologies (PETs), Mechanism Design, Distributed Systems.