XHS1024 — Cryptographic Hash Function

Technical Specification v1.0

Author: Dominy Project
Algorithm Name: XHS1024
Hash Size: 1024 bits
Block Size: 2048 bits
Rounds: 256 (fixed)
Status: Experimental / Original Cryptographic Design
Origin: Brazil

---

1. Introduction

XHS1024 is a cryptographic hash function designed from first principles as part of the Dominy blockchain project.
It was developed entirely from scratch, without derivation, reuse, or structural dependency on the SHA family, NIST standards, or any existing hash construction.

The primary goals of XHS1024 are:

- Extreme internal state width (1024 bits)
- High resistance to classical cryptanalysis
- Practical resistance to quantum attacks, including Grover's algorithm
- Structural simplicity with strong mathematical diffusion
- Long-term cryptographic durability

XHS1024 is not a variant, extension, or fork of SHA-1, SHA-2, SHA-3, Keccak, Blake, or any NIST-standardized algorithm.

---

2. Design Philosophy

XHS1024 follows a **wide-pipe ARX-based design**, using only fundamental operations:

- XOR
- Addition modulo 21282^{128}2128
- Fixed circular rotations

The algorithm deliberately avoids:

- Lookup tables
- S-boxes
- Data-dependent memory access
- External primitives

This design minimizes side-channel attack surfaces and favors portability across architectures.

---

3. Mathematical Model

3.1 Word Definition

Let:

- W=Z2128W = \mathbb{Z}_{2^{128}}W=Z2128

All arithmetic is performed modulo 21282^{128}2128.

3.2 Internal State

The internal chaining state is defined as:

S=(S0,S1,S2,S3,S4,S5,S6,S7)S = (S_0, S_1, S_2, S_3, S_4, S_5, S_6, S_7)S=(S0,S1,S2,S3,S4,S5,S6,S7)

Where each Si∈WS_i \in WSi∈W.

Total state size: **1024 bits**

3.3 Message Block

Each message block consists of:

M=(M0,M1,…,M15)M = (M_0, M_1, \ldots, M_{15})M=(M0,M1,…,M15)

Where each Mi∈WM_i \in WMi∈W.

Block size: **2048 bits**

---

4. Padding Scheme

XHS1024 uses a strengthened Merkle–Damgård padding scheme.

Given a message of length LLL bits:

1. Append a single `1` bit
2. Append `0` bits
3. Append the original message length encoded as a **256-bit integer**

Such that the final message length is a multiple of 2048 bits.

This construction prevents length-extension attacks.

---

5. Iterative Structure

XHS1024 processes the padded message block-by-block using an iterative compression function:

Si+1=F(Si,Mi)S_{i+1} = F(S_i, M_i)Si+1=F(Si,Mi)

The final hash output is the full internal state after processing the last block.

---

6. Message Expansion

Each 2048-bit message block is expanded into **256 words**:

W0…W255W_0 \ldots W_{255}W0…W255

- For 0≤i<160 \leq i < 160≤i<16:
  Wi=MiW_i = M_iWi=Mi
- For i≥16i \geq 16i≥16:
  Wi=ROTL(Wi−16⊕Wi−7,r1)+ROTL(Wi−3,r2)+Ci(mod2128)W_i = \text{ROTL}(W_{i-16} \oplus W_{i-7}, r_1) + \text{ROTL}(W_{i-3}, r_2) + C_i \pmod{2^{128}}Wi=ROTL(Wi−16⊕Wi−7,r1)+ROTL(Wi−3,r2)+Ci(mod2128)

Where:

- CiC_iCi are fixed round constants
- r1,r2r_1, r_2r1,r2 are fixed rotation offsets

---

7. Compression Function

The compression function consists of **256 rounds**.

Each round applies:

- Modular addition
- XOR mixing
- Circular rotations
- A fixed permutation of the 8-word state

Every word influences every other word within a small number of rounds, ensuring full diffusion.

---

8. Permutation Layer

After each round, the internal state undergoes a fixed permutation:

(S0,S1,…,S7)→π(S)(S_0, S_1, \ldots, S_7) \rightarrow \pi(S)(S0,S1,…,S7)→π(S)

The permutation is static, publicly defined, and constant across all rounds.

---

9. Round Constants

Round constants CiC_iCi are derived from public, non-manipulable mathematical sources such as:

- Fractional parts of π, e, and √2
- Expanded to 128-bit words

This avoids hidden structure and eliminates the possibility of backdoored constants.

---

10. Security Considerations

10.1 Classical Security

- Collision resistance: approximately 25122^{512}2512
- Preimage resistance: approximately 210242^{1024}21024

The wide internal state significantly raises the complexity of generic attacks.

10.2 Quantum Resistance

Under Grover's algorithm, preimage resistance is reduced to approximately:

25122^{512}2512

Which remains computationally infeasible for any foreseeable quantum hardware.

The large state size and high round count further increase circuit depth requirements, making practical quantum attacks unrealistic.

---

11. Originality Statement

XHS1024 is an **entirely original cryptographic construction**, designed and implemented from scratch.

It does not reuse:

- SHA-family designs

- NIST standards
- Existing compression functions
- Reference implementations

All architectural decisions, parameters, and structures were independently defined.

---

12. Intended Use

XHS1024 is intended for use in:

- Blockchain consensus systems
- Block identification
- Proof-of-work and proof-of-validation mechanisms
- Long-term cryptographic commitments

---

13. Disclaimer

XHS1024 has not yet undergone public cryptanalysis.
Its security claims are based on design rationale and established cryptographic principles.

Public review and academic analysis are encouraged.

End of Specification — XHS1024 v1.0