XHS1024 — Função Hash Criptográfica

Especificação Técnica v1.0

Autor: Projeto Dominy
Nome do Algoritmo: XHS1024
Tamanho do Hash: 1024 bits
Tamanho do Bloco: 2048 bits
Rounds: 256 (fixo)
Status: Experimental / Projeto Criptográfico Original
Origem: Brasil

---

1. Introdução

XHS1024 é uma função hash criptográfica projetada do zero como parte do projeto de blockchain Dominy.
O algoritmo foi desenvolvido integralmente a partir de princípios próprios, sem derivação, adaptação ou dependência estrutural da família SHA, padrões NIST ou qualquer outro algoritmo existente.

Os principais objetivos do XHS1024 são:

- Estado interno extremamente amplo (1024 bits)
- Alta resistência a criptoanálise clássica
- Resistência prática a ataques quânticos, incluindo o algoritmo de Grover
- Difusão forte baseada em operações matemáticas fundamentais
- Durabilidade criptográfica de longo prazo

O XHS1024 **não é** variante, extensão ou fork de SHA-1, SHA-2, SHA-3, Keccak, Blake ou qualquer padrão NIST.

---

2. Filosofia de Projeto

O XHS1024 segue um design **wide-pipe baseado em ARX**, utilizando exclusivamente operações fundamentais:

- XOR
- Adição módulo 21282^{128}2128
- Rotações circulares fixas

O algoritmo evita deliberadamente:

- Tabelas de consulta (lookup tables)
- S-boxes
- Acessos à memória dependentes de dados
- Primitivas externas

Essa abordagem reduz superfícies de ataque por canais laterais e garante portabilidade entre arquiteturas.

---

3. Modelo Matemático

3.1 Definição da Palavra

Seja:

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

Todas as operações aritméticas são realizadas módulo 21282^{128}2128.

3.2 Estado Interno

O estado interno de encadeamento é definido como:

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)

Onde cada Si∈WS_i \in WSi∈W.

Tamanho total do estado: **1024 bits**

3.3 Bloco de Mensagem

Cada bloco de mensagem é composto por:

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

Onde cada Mi∈WM_i \in WMi∈W.

Tamanho do bloco: **2048 bits**

---

4. Esquema de Padding

O XHS1024 utiliza um esquema de padding do tipo Merkle–Damgård fortalecido.

Dada uma mensagem de comprimento LLL bits:

1. Adiciona-se um único bit `1`
2. Adicionam-se bits `0`
3. Adiciona-se o comprimento original da mensagem codificado como um inteiro de **256 bits**

De forma que o comprimento final seja múltiplo de 2048 bits.

Esse método previne ataques de extensão de comprimento.

---

5. Estrutura Iterativa

O XHS1024 processa a mensagem preenchida bloco a bloco usando uma função de compressão iterativa:

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

O hash final é o estado interno completo após o processamento do último bloco.

---

6. Expansão da Mensagem

Cada bloco de 2048 bits é expandido em **256 palavras**:

W0…W255W_0 \ldots W_{255}W0…W255

- Para 0≤i<160 \leq i < 160≤i<16:
  Wi=MiW_i = M_iWi=Mi
- Para 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)

Onde:

- CiC_iCi são constantes de round fixas
- r1,r2r_1, r_2r1,r2 são rotações fixas

---

7. Função de Compressão

A função de compressão consiste em **256 rounds**.

Cada round aplica:

- Adição modular
- Mistura por XOR
- Rotações circulares
- Uma permutação fixa do estado de 8 palavras

Cada palavra influencia todas as outras em poucos rounds, garantindo difusão total.

---

8. Camada de Permutação

Após cada round, o estado interno passa por uma permutação fixa:

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

A permutação é estática, pública e idêntica em todos os rounds.

---

9. Constantes de Round

As constantes CiC_iCi são derivadas de fontes matemáticas públicas e não manipuláveis, como:

- Partes fracionárias de π, e e √2
- Expandidas para palavras de 128 bits

Isso elimina estruturas ocultas e reduz o risco de backdoors.

---

10. Considerações de Segurança

10.1 Segurança Clássica

- Resistência a colisões: aproximadamente 25122^{512}2512
- Resistência a pré-imagem: aproximadamente 210242^{1024}21024

O estado interno amplo aumenta significativamente a complexidade de ataques genéricos.

10.2 Resistência Quântica

Sob o algoritmo de Grover, a resistência a pré-imagem é reduzida para aproximadamente:

25122^{512}2512

Valor ainda impraticável para qualquer hardware quântico previsível.

O alto número de rounds e o tamanho do estado aumentam a profundidade de circuito exigida, dificultando ataques quânticos reais.

---

11. Declaração de Originalidade

O XHS1024 é uma **construção criptográfica totalmente original**, projetada e implementada do zero.

Não reutiliza:

- Estruturas da família SHA

- Padrões NIST
- Funções de compressão existentes
- Implementações de referência

Todos os parâmetros e decisões arquiteturais foram definidos de forma independente.

---

12. Uso Pretendido

O XHS1024 é destinado ao uso em:

- Sistemas de consenso em blockchain
- Identificação de blocos
- Mecanismos de prova de trabalho ou validação
- Compromissos criptográficos de longo prazo

---

13. Aviso Legal

O XHS1024 ainda não passou por auditoria criptográfica pública.
As garantias de segurança baseiam-se em princípios de design e fundamentos matemáticos conhecidos.

Análise acadêmica e revisão pública são encorajadas.

Fim da Especificação — XHS1024 v1.0