Time-Differential Blake3 Initialization Vector Generation

1 Algorithm Definition

Let $\mathcal{T}$ be the set of system timestamps, and $\mathcal{P}$ be the set of prime numbers. The initialization vector $IV \in \mathbb{F}_{2^{32}}^8$ is generated through the following procedure:

1.1 Temporal Signature Collection

For a sequence of timestamps $t_i \in \mathcal{T}$, where $i \in \{1, \ldots, 8\}$, define:

$$\tau(t_i) = t_i \oplus (\nu_{\text{cpu}} \cdot i)$$

where ν_{cpu} represents the CPU frequency in Hz.

The composite temporal signature σ_t is defined as:

$$\sigma_t = \bigoplus_{i=1}^{8} \tau(t_i)$$

1.2 Prime Distance Calculation

For each temporal component, calculate the prime distance function δ_p:

$$\delta_p(x) = \min\{p - x \mid p \in \mathcal{P}, p > x\}$$

The prime distance vector $\Delta = (\delta_1, \ldots, \delta_8)$ is computed as:

$$\delta_i = \delta_p(\sigma_t + i \cdot \omega)$$

where ω is the word size (32 bits).

1.3 Entropy Mixing Function

Define the entropy mixing function $\mathcal{E} : \mathbb{F}_{2^{32}} \to \mathbb{F}_{2^{32}}$:

$$\mathcal{E}(x) = x \oplus \text{ROT}_r(x) \oplus \eta$$

where:

- ROT_r is a right rotation by r bits
- η is system-specific entropy
- $r = \lfloor \log_2(x) \rfloor \bmod 32$

1.4 Initialization Vector Generation

The final IV components are generated as:

$$IV_i = \mathcal{E}(\delta_i) \oplus \mathcal{H}(m_i)$$

where:

- $\mathcal{H}$ is an auxiliary hash function
- m_i represents system memory statistics

2 Security Properties

2.1 Entropy Bounds

The minimum entropy contribution from each source is bounded by:

$$H_{\min}(\tau) \geq \log_2(\nu_{\text{cpu}}) + \log_2(t_{\text{precision}})$$

where $t_{\text{precision}}$ is the system's temporal resolution.

2.2 Prime Distance Security

The prime distance function provides a minimum security margin σ defined as:

$$\sigma = \min_{x,y \in \mathbb{F}_{2^{32}}} \{\delta_p(x) - \delta_p(y)\}$$

This ensures a minimum differential security of σ bits.

3 Implementation Constraints

The algorithm must satisfy the following constraints:

1. Temporal Resolution:

$$t_{\text{precision}} \leq 10^{-9} \text{ seconds}$$

2. Prime Search Boundary:

$$\max_{x \in \mathbb{F}_{2^{32}}} \{\delta_p(x)\} \leq 2^{20}$$

3. Entropy Pool Size:

$$|\eta| \geq 64 \text{ bytes}$$

4 Compression Function Integration

The modified compression function G' incorporating the dynamic IV is defined as:

$$G'(h, m, t) = G(h \oplus IV(t), m, t)$$

where:

- h is the input chaining value
- m is the message block
- t is the current timestamp
- G is the original Blake3 compression function

The chaining value update function becomes:

$$h_{i+1} = G'(h_i, m_i, t_i)$$

5 Performance Considerations

The algorithm implements the following optimizations:

1. Prime Cache:
$$\mathcal{C}_p = \{(x, \delta_p(x)) \mid x \in \text{recent}(\mathcal{T})\}$$
2. IV Generation Rate Limit:
$$\text{rate}(IV) \leq \min(\nu_{\text{cpu}}/1000, 10^6 \text{ Hz})$$
3. Memory Complexity:
$$\mathcal{O}(\log_2(\max(\mathcal{T})) \cdot |\mathcal{C}_p|)$$

6 Thread Safety Constraints

For parallel execution, the following invariant must hold:

$$\forall t_1, t_2 \in \mathcal{T} : t_1 \neq t_2 \implies IV(t_1) \neq IV(t_2)$$

with probability:

$$P(IV(t_1) = IV(t_2)) \leq 2^{-256}$$

7 Error Bounds

The algorithm maintains the following error bounds:

1. Timing Precision Error:

$$\epsilon_t \leq 10^{-9} \text{ seconds}$$

2. Prime Distance Error:

$$\epsilon_p \leq 2^{-32}$$

3. Entropy Pool Depletion:

$$P(\text{entropy\_depletion}) \leq 2^{-64}$$