**Blake3 Hash Scheme Documentation**

**What is BLAKE3?**

BLAKE3 is a cryptographic hash function that is fast, widely supported, and does not have any variants unlike its previous version Blake2. Blake2 had many variants: Blake2bp, Blake2sp etc. While Blake2b was widely supported, it was not fast and Blake2bp, Blake2sp were fast, but not widely supported. Blake3 solves all these drawbacks.

**Overview of the Implementation**

Functions:

1. quarter\_round
2. blake3\_compress
3. blake3\_hash

**1. quarter\_round(a, b, c, d)**

The quarter\_round function is a main component of the hash function's mixing process. It takes four integers and performs a series of operations to mix them.

Parameters:

- a, b, c, d: Four integers to be mixed.

Returns:

- A tuple of four integers after mixing.

Explanation:

- The function adds, XORs, and rotates the bits of the input integers to ensure thorough mixing.

Example Usage:

a, b, c, d = quarter\_round(1, 2, 3, 4)

Preview:

Изображение выглядит как снимок экрана, текст

Автоматически созданное описание

**2. blake3\_compress(state)**

The blake3\_compress function applies the quarter\_round function repeatedly to compress the state.

Parameters:

- state: A list of integers representing the state.

Returns:

- A list of integers after compression.

Explanation:

- The function performs 12 rounds of mixing using the quarter\_round function on different parts of the state.

- It then adds the initial state to the final state to mix in the original values.

Example Usage:



Preview:

Изображение выглядит как снимок экрана, текст, Мультимедийное программное обеспечение, программное обеспечение

Автоматически созданное описание

**3. blake3\_hash(key, counter, message)**

The blake3\_hash function initializes the state with a key and counter, compresses the state, and produces a hash output.

Parameters:

- key: A byte string used as the key for hashing.

- counter: A counter value for domain separation.

- message: The message to be hashed.

Returns:

- A byte string representing the hash output.

Explanation:

- The function initializes the state with predefined constants, the key, and the counter.

- It calls blake3\_compress to process the state.

- Finally, it converts the state to a byte string to produce the hash output.

Example Usage:

Изображение выглядит как текст, Мультимедийное программное обеспечение, Шрифт, снимок экрана

Автоматически созданное описание

Preview:

Изображение выглядит как текст, Мультимедийное программное обеспечение, программное обеспечение, снимок экрана

Автоматически созданное описание

The whole code:

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Автоматически созданное описание

