## Analisis Kinerja Algoritma Hash pada Keamanan Data: Perbandingan Antara SHA-256, SHA-3, dan Blake2

Dalam analisis ini, kita akan membahas kinerja tiga algoritma hash utama: \*\*SHA-256\*\*, \*\*SHA-3\*\*, dan \*\*BLAKE2\*\*. Fokus utama adalah pada aspek keamanan dan efisiensi komputasi masing-masing algoritma, serta perbandingan mereka dalam konteks penggunaan yang berbeda, termasuk aplikasi dalam cryptocurrency dan sistem blockchain.

### 1. \*\*Deskripsi Algoritma Hash\*\*

- \*\*SHA-256\*\*: Bagian dari keluarga SHA-2, SHA-256 menghasilkan hash sepanjang 256 bit dan dikenal luas karena keamanannya yang tinggi. Algoritma ini telah menjadi standar dalam berbagai aplikasi, termasuk Bitcoin.

- \*\*SHA-3\*\*: Menangkap perhatian sebagai pemenang kompetisi NIST untuk algoritma hash baru, SHA-3 memiliki struktur yang berbeda dari SHA-2 dan dirancang untuk mengatasi potensi kerentanan yang mungkin ada pada SHA-2. SHA-3 juga mendukung panjang hash yang sama dengan SHA-2.

- \*\*BLAKE2\*\*: Dikenal karena kecepatan dan efisiensinya, BLAKE2 menawarkan keamanan setara dengan SHA-3 tetapi dengan performa yang lebih baik dalam banyak pengujian. Ini dirancang untuk menjadi lebih cepat dan lebih sederhana dibandingkan dengan algoritma lain.

### 2. \*\*Perbandingan Kinerja\*\*

Berdasarkan hasil eksperimen yang dilakukan pada ketiga algoritma ini, berikut adalah beberapa temuan kunci:

- \*\*Keamanan\*\*: Semua algoritma menunjukkan tingkat keamanan yang tinggi. Namun, BLAKE2 dan SHA-3 dirancang untuk mengatasi beberapa potensi serangan yang mungkin dapat mempengaruhi SHA-256 di masa depan[1][3].

- \*\*Efisiensi Komputasi\*\*:

- \*\*SHA-256\*\* dan \*\*BLAKE2\*\* menunjukkan waktu eksekusi yang lebih pendek dibandingkan dengan \*\*SHA-3\*\*, menjadikannya pilihan lebih baik dalam situasi yang memprioritaskan efisiensi[1][4].

- Dalam pengujian throughput, BLAKE2 sering kali lebih cepat daripada SHA-256, terutama pada platform 64-bit. Misalnya, BLAKE2 mencapai sekitar 5.2 siklus per byte, sedangkan SHA-256 sekitar 6.0 siklus per byte[3][5].

### 3. \*\*Analisis Hasil Eksperimen\*\*

Tabel berikut merangkum hasil kinerja dari ketiga algoritma berdasarkan pengujian yang dilakukan:

| Algoritma | Panjang Hash (bit) | Kecepatan (siklus/byte) | Keamanan |

|-------------|---------------------|-------------------------|------------------|

| SHA-256 | 256 | ~6 | Tinggi |

| SHA-3 | 224/256/384/512 | ~7 | Sangat Tinggi |

| BLAKE2 | 256/384/512 | ~5.2 | Setara dengan SHA-3 |

### 4. \*\*Kesimpulan\*\*

Dari analisis di atas, dapat disimpulkan bahwa:

- \*\*SHA-256\*\* tetap menjadi pilihan yang solid untuk aplikasi yang membutuhkan keamanan tinggi dengan efisiensi baik.

- \*\*SHA-3\*\* menawarkan keamanan tambahan dengan struktur yang berbeda tetapi mungkin kurang efisien dalam hal kecepatan.

- \*\*BLAKE2\*\* muncul sebagai alternatif menarik karena kombinasi kecepatan dan keamanan yang sebanding dengan SHA-3.

Ketika memilih algoritma hash untuk aplikasi tertentu, penting untuk mempertimbangkan kebutuhan spesifik terkait keamanan dan efisiensi komputasi. Dalam konteks blockchain dan cryptocurrency, BLAKE2 dan SHA-256 mungkin menjadi pilihan utama karena performa mereka yang superior dalam pengujian praktis[1][4][5].

Citations:

[1] http://arxiv.org/pdf/2408.11950.pdf

[2] https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=4068861

[3] https://www.ijcst.com/vol8/8.2/3-rohit-jones.pdf

[4] https://dergipark.org.tr/en/download/article-file/2304059

[5] https://ceur-ws.org/Vol-3550/paper7.pdf

[6] https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Makalah-UAS/Makalah-UAS-Kripto-2020%20(24).pdf

[7] https://www.researchgate.net/publication/271454097\_An\_FPGA\_implementation\_and\_comparison\_of\_the\_SHA-256\_and\_Blake-256

[8] https://www.semanticscholar.org/paper/An-FPGA-implementation-and-comparison-of-the-and-Kahri-Bouallegue/c033cdb0f38db8fba43365d480b416cc708bf441