ABSTRAK

Perkembangan komputasi kuantum memicu tantangan baru dalam keamanan data, terutama dalam mengatasi serangan yang dapat memecahkan masalah matematika yang kompleks dengan cepat. Sejumlah metode keamanan data berbasis hash telah diusulkan untuk mengatasi ancaman ini, termasuk Hash to Obtain Random Subset (HORS), Hash to Obtain Random Subset-Tree (HORST), dan Hash to Obtain Random Subset and Integer Composition (HORSIC). Akan tetapi, metode-metode ini memiliki kekurangan, seperti kelemahan keamanan pada HORS karena hanya menggunakan satu putaran hash dan panjang kunci publik yang besar pada HORST. HORSIC, meskipun menggabungkan komposisi bilangan bulat untuk meningkatkan keamanan, menambahkan waktu pemrosesan yang signifikan.

Penelitian ini mengusulkan sebuah metode baru, Modified Hash to Obtain Random Subset-Tree (MHORST), yang bertujuan untuk meningkatkan keamanan, mengurangi waktu pemrosesan, dan memperpendek panjang kunci pada metode-metode sebelumnya. MHORST menggunakan pohon Merkle dan hash SHA-256 untuk membangun kunci publik dan tanda tangan digital. Hasil penelitian menunjukkan bahwa waktu pembuatan kunci untuk HORST adalah sekitar 9 hingga 15 kali lebih cepat dibandingkan dengan HORSIC dan sekitar 1.2 hingga 1.6 kali lebih cepat dibandingkan dengan MHORST. Dalam hal penandatanganan, HORST mengurangi waktu sekitar 2.1 hingga 3.6 kali dibandingkan dengan HORSIC, sedangkan MHORST mengurangi waktu penandatanganan sekitar 3.3 hingga 6.6 kali dibandingkan dengan HORST. Untuk verifikasi, HORST menunjukkan pengurangan waktu 17 hingga 235 kali dibandingkan dengan HORSIC, sedangkan MHORST mengurangi waktu verifikasi sekitar 1.1 hingga 2.1 kali. Meskipun tingkat keamanan MHORST sedikit menurun dibandingkan dengan HORSIC, metode ini masih lebih unggul dibandingkan dengan HORST dalam hal mengurangi kemungkinan pemalsuan tanda tangan.

Kata kunci: Quantum Computing, HORS, HORST, HORSIC, SHA-256, pohon Merkle, tanda tangan digital, keamanan data