ABSTRACT

The development of quantum computing triggers new challenges in data security, particularly in addressing attacks that can solve complex mathematical problems on the fly. A number of hash-based data security methods have been proposed to deal with this threat, including Hash to Obtain Random Subset (HORS), Hash to Obtain Random Subset-Tree (HORST), and Hash to Obtain Random Subset and Integer Composition (HORSIC). However, these methods have drawbacks, such as the security weakness in HORS due to using only one hash round and the large public key length in HORST. HORSIC, while incorporating integer composition to improve security, adds significant processing time.

This research proposes a new method, Modified Hash to Obtain Random Subset-Tree (MHORST), which aims to improve security, reduce processing time, and shorten key length in previous methods. MHORST uses Merkle trees and SHA-256 hashes to build public keys and digital signatures. The results show that the key generation time for HORST is about 9 to 15 times faster than that of HORSIC and about 1.2 to 1.6 times faster than that of MHORST. In terms of signing, HORST reduces the time by about 2.1 to 3.6 times compared to HORSIC, while MHORST reduces the signing time by about 3.3 to 6.6 times compared to HORST. For verification, HORST shows a time reduction of 17 to 235 times compared to HORSIC, while MHORST reduces the verification time by about 1.1 to 2.1 times. Although the security level of MHORST decreases slightly compared to HORSIC, this method is still superior to HORST in terms of reducing the probability of signature forgery.

Keywords: Quantum Computing, HORS, HORST, HORSIC, SHA-256, Merkle tree, digital signature, data security