abtechchennai@gmail.com
www.abtechnologies.in
9840511458

# LATTICE BASED PRIVACY PRESERVING AND FORWARD SECURE CLOUD STORAGE PUBLIC AUDITING SCHEME

## ABSTRACT

Aiming at reducing the local storage burden and computational costs, numerous individuals and enterprises are willing to outsource their data to the cloud server. Meanwhile, due to the loss of the actual physical control over their data files once outsourced to the cloud server, how to guarantee the cloud server keep user's data integrity is an important security issue to be addressed urgently. Accordingly, multiple data integrity checking schemes based on the traditional cryptosystem have been proposed. However, with the advent and development of quantum computer, these existing data integrity checking schemes are no longer secure. Thus, it is necessary to study the new scheme which can resist quantum attack to adapt to the quantum era. In this project, we put forward a novel scheme named lattice based privacy preserving and forward secure cloud storage public auditing scheme (LB-PPFS). Our proposed scheme is not only quantum attack against, but also enjoys the privacy preserving and forward-secure property. In the proposed scheme, a curious auditor cannot learn any knowledge of user's data because the original data is encapsulated with a random number. In addition, the lattice basis delegation technique is adopted to achieve forward security for resisting key exposure attack. Based on the hardness assumptions of SIS problem from lattice, we prove that the proposed scheme can achieve formally provable security. Besides, the theoretical analysis and performance evaluation demonstrate that the proposed scheme is effective and feasible to guarantee the quantum security for the data integrity in cloud storage.