A New Secure Distributed Storage System for Cloud: Mathematical Framework, Design and Applications

Tan, Chih Wei

Cheong, Hou Teng

This project includes new insights about how principles of mathematics can be used to raise security of data in distributed storage and the results can be applied to design a user-end security cloud storage application and a door access system for group users. Firstly, we have defined an abstract framework of k bit (t,n) secret sharing framework for distributed storage. A successful implementation can provide protection to data when the storage is under attacks on confidentiality, integrity, and reliability. Furthermore, the system has equipped with encryption, error detection, location, and data rescue. We use Lagrange polynomials and take the advantages of the algebraic property “t distinct points on the plane can uniquely determine a polynomial function of degree t-1” to design a k bit (t,n) -secret sharing distributed storage (SSDS). We employ the set with unique factorization property (UFP) so that we simply need to calculate the y intercept of a Lagrange polynomial and then use a lookup table to recover a secret. Moreover, if the UFP set is minimal, the corresponding containers have minimum size. Besides, we can utilize the geometric facts “three non collinear points determine a unique circle and four non coplanar points determine a unique sphere” to construct k bit (3,n) and (4,n) SSDS respectively. Applying Chinese Remainder Theorem (CRT), we have designed k bit (t,n) SSDS and one of the designs can produce containers with smallest size but k is not arbitrary. We have implemented algebraic, geometric and the CRT methods in C. The performances of first two kinds are satisfactory. For the CRT case, it can produce half size containers rapidly. A user-end cloud storage application and a door access system for group users are implemented.