

**CHENNAI – PONDICHERRY**

**PROVABLY SECURE KEY-AGGREGATE CRYPTOSYSTEMS WITH BROADCAST AGGREGATE KEYS FOR ONLINE DATA**

**SHARING ON THE CLOUD**

**Abstract:**

Online data sharing for increased productivity and efficiency is one of the primary requirements today for any organization. The advent of cloud computing has pushed the limits of sharing across geographical boundaries, and has enabled a multitude of users to contribute and collaborate on shared data. However, protecting online data is critical to the success of the cloud, which leads to the requirement of efficient and secure cryptographic schemes for the same. Data owners would ideally want to store their data/files online in an encrypted manner, and delegate decryption rights for some of these to users, while retaining the power to revoke access at any point of time. An efficient solution in this regard would be one that allows users to decrypt multiple classes of data using a single key of constant size that can be efficiently broadcast to multiple users. Chu et al. proposed a key aggregate cryptosystem (KAC) in 2014 to address this problem, albeit without formal proofs of security. In this paper, we propose CPA and CCA secure KAC constructions that are efficiently implementable using elliptic curves and are suitable for implementation on cloud based data sharing environments. We lay special focus on how the standalone KAC scheme can be efficiently combined with broadcast encryption to cater to m data users and m' data owners while reducing the reducing the secure channel requirement from O(mm') in the standalone case to O(m + m').