Abstract

It is important to share data securely, efficiently and flexibly in cloud storage. We describe public-key encryption technique based on elliptic-curve theory which is used to create faster, smaller and more efficient cryptographic keys. This public-key cryptosystem produces constant size cipher texts and user can aggregate any set of secret keys and make them as compact as single and can decrypt any set of cipher texts by using that compact aggregate key but, files outside the set remain confidential. In this cryptosystem it is possible to efficiently assign decryption rights for the set of cipher texts to any users. The secret key holder can release a constant-size aggregate key for set of cipher texts and this compact aggregate key conveniently shared with others with very limited secure storage. In this paper, we study how to create a decryption key more powerful so that it can allows decryption of multiple cipher texts, without increasing key size.


**Index Terms**

Computer Science  
Distributed Systems

**Keywords**

Key-aggregate cryptosystem, Elliptic curve cryptography, public-key cryptosystem, Data sharing.