

**CHENNAI – PONDICHERRY**

**FULL VERIFIABILITY FOR OUTSOURCED DECRYPTION IN ATTRIBUTE BASED ENCRYPTION**

**Abstract:**

Attribute based encryption (ABE) is a popular cryptographic technology to protect the security of users’ data. However, the decryption cost and ciphertext size restrict the application of ABE in practice. For most existing ABE schemes, the decryption cost and ciphertext size grow linearly with the complexity of access structure. This is undesirable to the devices with limited computing capability and storage space. Outsourced decryption is considered as a feasible method to reduce the user's decryption overhead, which enables a user to outsource a large number of decryption operations to the cloud service provider (CSP). However, outsourced decryption cannot guarantee the correctness of transformation done by the cloud, so it is necessary to check the correctness of outsourced decryption to ensure security for users’ data. Current research mainly focuses on verifiability of outsourced decryption for the authorized users. It still remains a challenging issue that how to guarantee the correctness of outsourced decryption for unauthorized users. In this paper, we propose an ABE scheme with verifiable outsourced decryption (called full verifiability for outsourced decryption), which can simultaneously check the correctness for transformed ciphertext for the authorized users and unauthorized users. The proposed ABE scheme with verifiable outsourced decryption is proved to be selective CPA-secure in the standard model.