一种云存储下多授权访问控制及用户属性撤销方案

江泽涛 1,2，王伟峰 1,2

（1 桂林电子科技大学 广西图像图形处理智能处理重点实验室，广西 桂林 541004;
2 桂林电子科技大学 广西高校图像图形智能处理重点实验室, 广西 桂林 541004）

摘要： 云存储下已有基于属性加密的访问控制研究多是基于单授权中心来实现，该种方案在授权方不可信或遭受恶意攻击的情况下可能会造成密钥泄露.基于 CP-ABE 设计了一种多授权访问控制方案，引用代理服务器(Proxy Server,PS)，帮助用户承担大量解密操作；对用户属性撤销问题采用高效安全的算法进行处理；最后，利用双线性判定(Decision Bilinear Diffie-Hellman，DBDH)假设理论证明是选择明文攻击安全的.

关键词： 云存储；多授权中心；访问控制；CP-ABE；属性撤销

A Scheme of Multi-authorization Access Control and User Attribute Revocation in Cloud Storage

JIANG Ze-tao1,2，WANG Wei-feng1,2

（1 The Key Laboratory of Image and Graphic Intelligent Processing of Guangxi ,Guilin University of Electronic Technology, Guilin 541004， China;2 The Key Laboratory of Image and Graphic Intelligent Processing of Higher Education in Guangxi , Guilin University of Electronic Technology, Guilin 541004, China）

Abstract： The research of access control based on attribute encryption has been implemented in cloud storage, which is mostly based on single authorization center, may result in the leakage of key. Proposing a CP-ABE design of a multi access control scheme based on reference proxy server (Proxy Server, PS), to help users to undertake a large number of decryption operation; Problems with high security attributes revocation algorithm for processing; Finally, using the bilinear decision(Decision Bilinear Diffie-Hellman，DBDH) proved to be the chosen plaintext attack security.

Key words： cloud storage; multi-authorization center; access control; CP-ABE; attribute revocation

作者简介：

江泽涛男，（1961-），教授，博士生导师.研究方向为访问控制与信息安全及计算机视觉.
E-mail: 1459586819@qq.com.

王伟峰男，（1992-），硕士研究生.研究方向为访问控制与信息安全.