# Cryptology ePrint Archive: Report 2013/208

**CloudHKA: A Cryptographic Approach for Hierarchical Access Control in Cloud Computing**

*Yi-Ruei Chen and Cheng-Kang Chu and Wen-Guey Tzeng and Jianying Zhou*

**Abstract:** Cloud services are blooming recently. They provide a convenient way for data accessing, sharing, and processing. A key ingredient for successful cloud services is to control data access while considering the specific features of cloud services. The specific features include great quantity of outsourced data, large number of users, honest-but-curious cloud servers, frequently changed user set, dynamic access control policies, and data accessing for light-weight mobile devices. This paper addresses a cryptographic key assignment problem for enforcing a hierarchical access control policy over cloud data.

We propose a new hierarchical key assignment scheme CloudHKA that observes the Bell- LaPadula security model and efficiently deals with the user revocation issue practically. We use CloudHKA to encrypt outsourced data so that the data are secure against honest-but- curious cloud servers. CloudHKA possesses almost all advantages of the related schemes, e.g., each user only needs to store one secret key, supporting dynamic user set and access hierarchy, and provably-secure against collusive attacks. In particular, CloudHKA provides the following distinct features that make it more suitable for controlling access of cloud data. (1) A user only needs a constant computation time for each data accessing. (2) The encrypted data are securely updatable so that the user revocation can prevent a revoked user from decrypting newly and previously encrypted data. Notably, the updates can be outsourced by using public information only. (3) CloudHKA is secure against the legal access attack. The attack is launched by an authorized, but malicious, user who pre-downloads the needed information for decrypting data ciphertexts in his authorization period. The user uses the pre-downloaded information for future decryption even after he is revoked. Note that the pre-downloaded information are often a small portion of encrypted data only, e.g. the header- cipher in a hybrid encrypted data ciphertext. (4) Each user can be flexibly authorized the access rights of Write or Read, or both.

**Category / Keywords:** cryptographic protocols / access control, hierarchical key assignment, key management, Bell-LaPadula security model, outsourced data, cloud computing, proxy re-encryption

**Publication Info:** This paper was accepted by the 11th International Conference on Applied Cryptography and Network Security (ACNS'13) (this is the full version)

**Date:** received 10 Apr 2013

**Contact author:** jellystudio cs96g at gmail com

**Available formats:** PDF | BibTeX Citation

**Version:** 20130414:152852 (All versions of this report)

**Discussion forum:** Show discussion | Start new discussion

---

[ Cryptology ePrint archive ]