Cryptology ePrint Archive: Report 2011/529

Secure and Efficient Proof of Storage with Deduplication

Qingji Zheng and Shouhuai Xu

Abstract: Both security and efficiency are crucial to the success of cloud storage. So far, security and efficiency of cloud storage have been separately investigated as follows: On one hand, security notions such as Proof of Data Possession (\PDP) and Proof of Retrievability (\POR) have been introduced for detecting the tamperation of data stored in the cloud. One the other hand, the notion of Proof of Ownership (\POW) has also been proposed to alleviate the cloud server from storing multiple copies of the same data, which could substantially reduce the consumption of both network bandwidth and server storage space. These two aspects are seemingly quite to the opposite of each other. In this paper, we show, somewhat surprisingly, that the two aspects can actually co-exist within the same framework. This is possible fundamentally because of the following insight: {\em The public verifiability offered by \PDP/\POR\ schemes can be naturally exploited to achieve \POW}. This ``one stone, two birds'' phenomenon not only inspired us to propose the novel notion of Proof of Storage with Deduplication (\POSD),but also guided us to design a concrete scheme that is provably secure in the Random Oracle model based on the Computational Diffie-Hellman (CDH) assumption.

Category / Keywords: cryptographic protocols / cloud storage, outsourced storage, proof of storage, deduplication, integrity checking, proof of ownership, proof of data possession, proof of retrievability

Publication Info: in submission

Date: received 29 Sep 2011

Contact author: qzheng at cs utsa edu

Available formats: PDF | BibTeX Citation

Version: 20111001:031052 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]