Cryptology ePrint Archive: Report 2011/574

Towards Efficient Provable Data Possession

Jia XU and Ee-Chien CHANG

Abstract: Provable Data Possession (\PDP) allows data owner to periodically and remotely audit their data stored in a cloud storage, without retrieving the file and without keeping a local copy. Ateniese~\emph{et al.} (CCS 07) proposed the first {\PDP} scheme, which is very efficient in communication and storage. However their scheme requires a lot of group exponentiation operations: In the setup, one group exponentiation is required to generate a tag per each data block. In each verification, (equivalently) $(m + \ell)$ group exponentiations are required to generate a proof, where m is the size of a data block and ℓ is the number of blocks accessed during a verification. This paper proposed an efficient {\PDP} scheme. Compared to Ateniese~\emph{et al.} (CCS 07), the proposed scheme has the same complexities in communication and storage, but is more efficient in computation: In the setup, no group exponentiations are required. In each verification, only (equivalently) m group exponentiations are required to generate a proof. The security of the proposed scheme is proved under Knowledge of Exponent Assumption and Factoriztion Assumption.

Category / Keywords: cryptographic protocols / Cloud Storage, Provable Data Possession, Proofs of Retrievability, Remote Data Integrity Check, Homomorphic Authentication Tag, RSA Factorization Problem

Date: received 24 Oct 2011

Contact author: jiaxu2001 at gmail com

Available formats: PDF | BibTeX Citation

Note: 1. This is the full version of the PDP scheme described in the Appendix of Cryptology ePrint Archive, Report 2011/362. 2. The proposed scheme improves "Ateniese et al. CCS 07: Provable Data Possession at Untrusted Stores" in computation complexity, without sacrificing in communication or storage.

Version: 20111025:170723 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]