Cryptology ePrint Archive: Report 2011/362

Practically Efficient Proof of Retrievability in Cloud Storage

Jia XU and Ee-Chien CHANG

Abstract: Proofs of Retrievability ({\POR}) is a cryptographic method for remotely auditing the integrity of files stored in the cloud, without keeping a copy of the original files in local storage. In a {\POR} scheme, a user Alice backups her data file together with some authentication data to a potentially dishonest cloud storage server Bob. Later, Alice can periodically and remotely verify the integrity of her data stored with Bob using the authentication data, without retrieving back the data file during a verification. Besides security, performances in communication, storage overhead and computaton are major considerations. Shacham and Waters~\cite{CompactPOR} gave a fast scheme with $\mathcal{O}(s)$ communication bits and a factor of $1/s$ file size expansion. Although Ateniese~\emph{et al.}~\cite{PDP} achieves constant communication requirement with the same $1/s$ storage overhead, it requires intensive computation in the setup and verification. In this paper, we incorporate a recent construction of constant size polynomial commitment scheme into Shacham and Waters~\cite{CompactPOR} scheme. The resulting scheme requires constant communication bits (particularly, 720 bits if elliptic curve is used or 3312 bits if a modulo group is used) per verification and a factor of $1/s$ file size expansion, and its computation in the setup and verification is significantly reduced compared to Ateniese~\emph{et al.}~\cite{PDP}. Essentially, Ateniese~\emph{et al.}~\cite{PDP} requires one group multiplication per each bit of the data file in the setup, while the proposed scheme requires one group multiplication per each chunk of data bits (160 bits per chunk if elliptic curve is used or 1024 bits per chunk if modulo group is used). The experiment results show that our proposed scheme is indeed efficient and practical. Our security proof is based on Strong Diffie-Hellman Assumption.

Category / Keywords: Cloud Storage, Proofs of Retrievability, Remote Data Integrity Check, Homomorphic Authentication Tag, Polynomial Commitment, Provable Data Possession

Date: received 4 Jul 2011, last revised 15 Oct 2011

Contact author: jiaxu2001 at gmail com

Available formats: PDF | BibTeX Citation

Note: An efficient variant version of Ateniese's PDP scheme (CCS '07: Provable data possession at untrusted stores) is in the appendix, which requires no exponentiations in setup.

Version: 20111015:134219 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]