Cryptology ePrint Archive: Report 2011/362

Practically Efficient Proof of Retrievability in Cloud Storage

Jia XU

Abstract: Cloud storage, among other cloud computing services, is becomming more and more prevalent in the IT industry. In a secure cloud storage application, a user Alice outsources (backups) her data file together with some authentication data to a potentially untrusted Cloud Storage Server Bob. Later, Alice wants to periodically and remotely verify the integrity of her data stored with Bob using the authentication data, without keeping a local copy of the data file or retrieving back the data file during the verification.

We propose two secure and efficient methods that allow Bob to prove to Alice that he indeed keeps her data file intactly:

(1) Our first method is the first provable-secure Proof of Retrievability scheme constructed over integer domain, and has the same complexity as Shacham and Waters~\cite{CompactPOR}. (2) Our second method reduces the communication complexity of Shacham and Waters~\cite{CompactPOR} from O(s) to O(1), where keeping other aspects of complexity unchanged, using our new construction of a functional encryption scheme.

Category / Keywords: Cloud Storage, Proof of Retrievability, Remote Data Integrity Check, Homomorphic Authentication Tag, Functional Encryption

Date: received 4 Jul 2011, last revised 25 Jul 2011

Contact author: jiaxu2001 at gmail com