Cryptology ePrint Archive: Report 2011/021

Fully Secure Anonymous Hierarchical Identity-Based Encryption with Constant Size Ciphertexts

Jae Hong Seo and Jung Hee Cheon

Abstract: Efficient and privacy-preserving constructions for search functionality on encrypted data is important issues for data outsourcing, and data retrieval, etc. Fully secure anonymous Hierarchical ID-Based Encryption (HIBE) schemes is useful primitives that can be applicable to searchable encryptions [4], such as ID-based searchable encryption, temporary searchable encryption [1], and anonymous forward secure HIBE [9]. We propose a fully secure anonymous HIBE scheme with constant size ciphertexts.

Category / Keywords: cryptographic protocols / anonymity

Date: received 11 Jan 2011, last revised 16 Jan 2011

Contact author: jhsbhs at gmail com

Available formats: PDF | BibTeX Citation

Version: 20110117:041825 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]