Cryptology ePrint Archive: Report 2011/699

Public-Key Encryption with Cluster-Chain-based Keyword Search

Peng Xu and Hai Jin and Wei Wang and Deqing Zou

Abstract: It is widely acknowledged that the keyword search performance and the privacy of keywords are equally important for keyword searchable ciphertexts. To our knowledge, no public-key-encryption-based work in literature can accelerate the keyword search, while preserving semantic security of keywords under chosen keyword attacks. In this paper, we propose public-key encryption with cluster-chain-based keyword search (PCCS), which is an innovation of public-key encryption with keyword search (PEKS). PCCS not only has much more efficient keyword search, but also preserves the equal SS-CKA security with PEKS from computational bilinear Diffie-Hellman (CBDH) assumption. With such advantages, PCCS just slightly increases the size of public parameter and the space complexity of keyword searchable ciphertexts.

Category / Keywords: public-key cryptography /

Date: received 21 Dec 2011, last revised 6 Jan 2012, withdrawn 17 Feb 2012

Contact author: xupeng at mail hust edu cn

Available formats: (-- withdrawn --)

Version: 20120217:153459 (All versions of this report)