Cryptology ePrint Archive: Report 2011/645

Fully Homomorphic Encryption Based on Approximate Matrix GCD

Gu Chunsheng

Abstract: We first introduce approximate matrix GCD problem (AMGCD), and construct public key encryption schemes based on AMGCD. Then, we define a variant of AMGCD and design a new fully homomorphic encryption scheme (FHE) based on the variant AMGCD, whose security depends on the hardness assumption of the variant AMGCD problem.

Category / Keywords: Fully Homomorphic Encryption, Approximate Matrix GCD, Learning with Error, Approximate GCD

Date: received 29 Nov 2011, last revised 4 Dec 2011

Contact author: guchunsheng at gmail com

Available formats: PDF | BibTeX Citation

Note: We have found a security problem for previous version.

Version: 20111204:140034 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]