Cryptology ePrint Archive: Report 2011/471

Improved Key Generation For Gentry's Fully Homomorphic Encryption Scheme

P. Scholl and N.P. Smart

Abstract: A key problem with the original implementation of the Gentry Fully Homomorphic Encryption scheme was the slow key generation process. Gentry and Halevi provided a fast technique for 2-power cyclotomic fields. We present an extension of the Gentry--Halevi key generation technique for arbitrary cyclotomic fields. Our new method is roughly twice as efficient as the previous best methods. Our estimates are backed up with experimental data.

Category / Keywords:

Date: received 31 Aug 2011

Contact author: nigel at cs bris ac uk

Available formats: PDF | BibTeX Citation

Version: 20110906:040232 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]