Cryptology ePrint Archive: Report 2011/133

Fully Homomorphic SIMD Operations

N.P. Smart and F. Vercauteren

Abstract: At PKC 2010 Smart and Vercauteren presented a variant of Gentry's fully homomorphic public key encryption scheme and mentioned that the scheme could support SIMD style operations. The slow key generation process of the Smart--Vercauteren system was then addressed in a paper by Gentry and Halevi, but their key generation method appears to exclude the SIMD style operation alluded to by Smart and Vercauteren. In this paper, we show how to select parameters to enable such SIMD operations, whilst still maintaining practicality of the key generation technique of Gentry and Halevi. As such, we obtain a somewhat homomorphic scheme supporting both SIMD operations and operations on large finite fields of characteristic two. This somewhat homomorphic scheme can be made fully homomorphic in a naive way by recrypting all data elements seperately. However, we show that the SIMD operations can be used to perform the recrypt procedure in parallel, resulting in a substantial speed-up. Finally, we demonstrate how such SIMD operations can be used to perform various tasks by studying two use cases: implementing AES homomorphically and encrypted database lookup.

Category / Keywords: public-key cryptography

Date: received 15 Mar 2011, last revised 3 Aug 2011

Contact author: frederik vercauteren at gmail com

Available formats: Postscript (PS) | Compressed Postscript (PS.GZ) | PDF | BibTeX Citation

Note: Much improved exposition and algorithms.

Version: 20110803:143250 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]