Cryptology ePrint Archive: Report 2011/440

Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers

Jean-Sebastien Coron and David Naccache and Mehdi Tibouchi

Abstract: We describe a compression technique that reduces the public key size of van Dijk, Gentry, Halevi and Vaikuntanathan's (DGHV) fully homomorphic scheme over the integers from \lambda^7 to \lambda^5. Our variant remains semantically secure, but in the random oracle model. We obtain an implementation of the full scheme with a 10.1 MB public key instead of 802 MB using similar parameters as in \cite{cmnt2011}. Additionally we show how to extend the quadratic encryption technique of \cite{cmnt2011} to higher degrees, to obtain a shorter public-key for the basic scheme.

This paper also describes a new modulus switching technique for the DGHV scheme that enables to use the new FHE framework without bootstrapping from Brakerski, Gentry and Vaikuntanathan with the DGHV scheme. Finally we describe an improved attack against the Approximate GCD Problem on which the DGHV scheme is based, with complexity 2^\rho instead of 2^{3 \rho/2}.

Category / Keywords: public-key cryptography / Fully Homomorphic Encryption

Publication Info: An extended abstract of this paper appeared at Eurocrypt 2012. This is the full version.

Date: received 12 Aug 2011, last revised 18 Jan 2012

Contact author: jean-sebastien coron at uni lu