Cryptology ePrint Archive: Report 2011/441

Fully Homomorphic Encryption over the Integers with Shorter Public Keys

Jean-Sebastien Coron and Avradip Mandal and David Naccache and Mehdi Tibouchi

Abstract: At Eurocrypt 2010 van Dijk {\sl et al.} described a fully homomorphic encryption scheme over the integers. The main appeal of this scheme (compared to Gentry's) is its conceptual simplicity. This simplicity comes at the expense of a public key size in ${\cal \tilde O}(\lambda^{10})$ which is too large for any practical system. In this paper we reduce the public key size to ${\cal \tilde O}(\lambda^{7})$ by encrypting with a quadratic form in the public key elements, instead of a linear form. We prove that the scheme remains semantically secure, based on a stronger variant of the approximate-GCD problem, already considered by van Dijk {\sl et al}.

We also describe the first implementation of the resulting fully homomorphic scheme. Borrowing some optimizations from the recent Gentry-Halevi implementation of Gentry's scheme, we obtain roughly the same level of efficiency. This shows that fully homomorphic encryption can be implemented using simple arithmetic operations.

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

Publication Info: An extended abstract will appear at CRYPTO 2011

Date: received 12 Aug 2011

Contact author: jean-sebastien coron at uni lu