Cryptology ePrint Archive: Report 2013/075

Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme

Joppe W. Bos and Kristin Lauter and Jake Loftus and Michael Naehrig

Abstract: In 1996, Hoffstein, Pipher and Silverman introduced an efficient lattice based encryption scheme dubbed NTRUEncrypt. Unfortunately, this scheme lacks a proof of security. However, in 2011, Stehle and Steinfeld showed how to modify NTRUEncrypt to reduce security to standard problems in ideal lattices. At STOC 2012, Lopez-Alt, Tromer and Vaikuntanathan proposed a fully homomorphic scheme based on this modified system. However, to allow homomorphic operations and prove security, a non-standard assumption is required in their scheme. In this paper, we show how to remove this non-standard assumption via techniques introduced by Brakerski at CRYPTO 2012 and construct a new fully homomorphic encryption scheme from the Stehle and Steinfeld version based on standard lattice assumptions and a circular security assumption. The scheme is scale-invariant and therefore avoids modulus switching, it eliminates ciphertext expansion in homomorphic multiplication, and the size of ciphertexts is one ring element. Moreover, we present a practical variant of our scheme, which is secure under stronger assumptions, along with parameter recommendations and promising implementation results. Finally, we present a novel approach for encrypting larger input sizes by applying a CRT approach on the input space.

Category / Keywords: public-key cryptography / Leveled homomorphic encryption, fully homomorphic encryption, ring learning with errors

Date: received 15 Feb 2013, last revised 18 Feb 2013

Contact author: mnaehrig at microsoft com