Cryptology ePrint Archive: Report 2011/622

Homomorphic encryption from codes

Andrej Bogdanov and Chin Ho Lee

Abstract: We propose a new homomorphic encryption scheme based on the hardness of decoding under independent random noise from certain affine families of codes. Unlike in previous lattice-based homomorphic encryption schemes, where the message is hidden in the noisy part of the ciphertext, our scheme carries the message in the affine part of the transformation and applies noise only to achieve security. Our scheme can tolerate noise of arbitrary magnitude, as long as the noise vector has sufficiently small hamming weight (and its entries are independent).

Our design achieves "proto-homomorphic" properties in an elementary manner: message addition and multiplication are emulated by pointwise addition and multiplication of the ciphertext vectors. Moreover, the extremely simple nature of our decryption makes the scheme easily amenable to bootstrapping. However, some complications are caused by the inherent presence of noticeable encryption error. Our main technical contribution is the development of two new techniques for handling this error in the homomorphic evaluation process.

We also provide a definitional framework for homomorphic encryption that may be useful elsewhere.

Category / Keywords: public-key cryptography / homomorphic encryption, code-based cryptosystems

Date: received 18 Nov 2011

Contact author: andrejb at cse cuhk edu hk