Cryptology ePrint Archive: Report 2011/344

Efficient Fully Homomorphic Encryption from (Standard) LWE

Zvika Brakerski and Vinod Vaikuntanathan

Abstract: We present a fully homomorphic encryption scheme that is based solely on the (standard) learning with errors (LWE) assumption. Applying known results on LWE, the security of our scheme is based on the worst-case hardness of ``short vector problems'' on arbitrary lattices.

Our construction improves on previous works in two aspects:

1. We show that ``somewhat homomorphic'' encryption can be based on LWE, using a new {\em re-linearization} technique. In contrast, all previous schemes relied on complexity assumptions related to ideals in various rings.

2. We deviate from the ``squashing paradigm'' used in all previous works. We introduce a new {\em dimension-modulus reduction} technique, which shortens the ciphertexts and reduces the decryption complexity of our scheme, {\em without introducing additional assumptions}.

Our scheme has very short ciphertexts and we therefore use it to construct an asymptotically efficient LWE-based single-server private information retrieval (PIR) protocol. The communication complexity of our protocol (in the public-key model) is $k \cdot \polylog(k)+\log |DB|$ bits per single-bit query (here, k is a security parameter).

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

Date: received 26 Jun 2011, last revised 4 Aug 2011

Contact author: vinodv at alum mit edu