# Cryptology ePrint Archive: Report 2011/410

**Functional Encryption for Inner Product Predicates from Learning with Errors**

*Shweta Agrawal and David Mandell Freeman and Vinod Vaikuntanathan*

**Abstract:** We propose a lattice-based functional encryption scheme for inner product predicates whose security follows from the difficulty of the "learning with errors" (LWE) problem. This construction allows us to achieve applications such as range and subset queries, polynomial evaluation, and CNF/DNF formulas on encrypted data. Our scheme supports inner products over small fields, in contrast to earlier works based on bilinear maps.

Our construction is the first functional encryption scheme based on lattice techniques that goes beyond basic identity-based encryption. The main technique in our scheme is a novel twist to the identity-based encryption scheme of Agrawal, Boneh and Boyen (Eurocrypt 2010).

**Category / Keywords:** Public-key cryptography / predicate encryption, functional encryption, lattices, learning with errors

**Publication Info:** Extended abstract to appear in Asiacrypt 2011

**Date:** received 31 Jul 2011, last revised 16 Aug 2011

**Contact author:** vinodv at cs toronto edu