Cryptology ePrint Archive: Report 2013/060

On FHE without bootstrapping

Aayush Jain

Abstract: In this work we come up with two fully homomorphic schemes. First, we propose an IND-CPA secure symmetric key homomorphic encryption scheme using multivariate polynomial ring over finite fields. This scheme gives a method of constructing a CPA secure homomorphic encryption scheme from another symmetric deterministic CPA secure scheme. We base the security of the scheme on pseudo random functions and prove the scheme to be IND-CPA secure, rather than basing security on hard problems like Ideal Membership and Gr\"obner basis as seen in most polly cracker based schemes which also use multivariate polynomial rings. This scheme is not compact but has many interesting properties- It can evaluate circuits of arbitrary depths without bootstrapping for bounded length input to the algorithm. Second, we also describe another similar symmetric key scheme which is compact, fully homomorphic and doesn't require bootstrapping. The scheme is on the lines of the work of Albrecht et. al. (Asiacrypt-2011) and is proven to be bounded CPA secure. Proof is based on Ideal Membership/ Ideal Remainder/Gr\"obner basis problem.

Category / Keywords: Fully Homomorphic Encryption, Multivariate Polynomials, Bootstrapping, Symmetric Key Cryptography

Date: received 6 Feb 2013, last revised 18 Feb 2013

Contact author: aayushjainiitd at gmail com