Cryptology ePrint Archive: Report 2011/680

Better Bootstrapping in Fully Homomorphic Encryption

Craig Gentry and Shai Halevi and Nigel P. Smart

Abstract: Gentry's bootstrapping technique is currently the only known method of obtaining a "pure" fully homomorphic encryption (FHE) schemes, and it may offers performance advantages even in cases that do not require pure FHE (such as when using the new noise-control technique of Brakerski-Gentry-Vaikuntanathan).

The main bottleneck in bootstrapping is the need to evaluate homomorphically the reduction of one integer modulo another. This is typically done by emulating a binary modular reduction circuit, using bit operations on binary representation of integers. We present a simpler approach that bypasses the homomorphic modular-reduction bottleneck to some extent, by working with a modulus very close to a power of two. Our method is easier to describe and implement than the generic binary circuit approach, and is likely to be faster in practice. In some cases it also allows us to store the encryption of the secret key as a single ciphertext, thus reducing the size of the public key.

We also show how to combine our new method with the SIMD homomorphic computation techniques of Smart-Vercauteren and Gentry-Halevi-Smart, to get a bootstrapping method that works in time quasi-linear in the security parameter. This last part requires extending the techniques from prior work to handle arithmetic not only over fields, but also over some rings. (Specifically, our method uses arithmetic modulo a power of two, rather than over characteristic-two fields.)

Category / Keywords: public-key cryptography / Bootstrapping, Fully Homomorphic Encryption

Date: received 15 Dec 2011

Contact author: shaih at alum mit edu