Cryptology ePrint Archive: Report 2011/279

Fully Homomorphic Encryption without Squashing Using Depth-3 Arithmetic Circuits

Craig Gentry and Shai Halevi

Abstract: We describe a new approach for constructing fully homomorphic encryption (FHE) schemes. Previous FHE schemes all use the same blueprint from [Gentry 2009]: First construct a somewhat homomorphic encryption (SWHE) scheme, next "squash" the decryption circuit until it is simple enough to be handled within the homomorphic capacity of the SWHE scheme, and finally "bootstrap" to get a FHE scheme. In all existing schemes, the squashing technique induces an additional assumption: that the sparse subset sum problem (SSSP) is hard.

Our new approach constructs FHE as a hybrid of a SWHE and a multiplicatively homomorphic encryption (MHE) scheme, such as Elgamal. Our construction eliminates the need for the squashing step, and thereby also removes the need to assume the SSSP is hard. We describe a few concrete instantiations of the new method, including a "simple" FHE scheme where we replace SSSP with Decision Diffie-Hellman, an optimization of the simple scheme that let us "compress" the FHE ciphertext into a single Elgamal ciphertext(!), and a scheme whose security can be (quantumly) reduced to the approximate ideal-SIVP.

We stress that the new approach still relies on bootstrapping, but it shows how to bootstrap without having to "squash" the decryption circuit. The main technique is to express the decryption function of SWHE schemes as a depth-3 ($\sum \prod \sum$) arithmetic circuit of a particular form. When evaluating this circuit homomorphically (as needed for bootstrapping), we temporarily switch to a MHE scheme, such as Elgamal, to handle the $\prod$ part. Due to the special form of the circuit, the switch to the MHE scheme can be done without having to evaluate anything homomorphically. We then translate the result back to the SWHE scheme by homomorphically evaluating the decryption function of the MHE scheme. Using our method, the SWHE scheme only needs to be capable of evaluating the MHE scheme's decryption function, not its own decryption function. We thereby avoid the circularity that necessitated squashing in the original blueprint.

Category / Keywords: foundations / Fully-homomorphic encryption

Publication Info: Extended abstract in FOCS 2011, this is the full version

Date: received 29 May 2011, last revised 14 Sep 2011

Contact author: shaih at alum mit edu