Cryptology ePrint Archive: Report 2011/279

Fully Homomorphic Encryption without Squashing Using Depth-3 Arithmetic Circuits

Craig Gentry and Shai Halevi

Abstract: All currently known fully homomorphic encryption (FHE) schemes 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.

We describe a new approach that 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, obtaining the following results:

* A "simple" FHE scheme where we replace SSSP with Decision Diffie-Hellman.

* The first FHE scheme based entirely on worst-case hardness. Specifically, we describe a "leveled" FHE scheme whose security can be quantumly reduced to the approximate shortest independent vector problem over ideal lattices (ideal-SIVP).

* Some efficiency improvements for FHE. While at present our new method does not improve computational efficiency, we do provide an optimization that reduces the ciphertext length. For example, at one point, the entire FHE ciphertext may consist of a single Elgamal ciphertext!

Our new method does not eliminate the bootstrapping step. Whether this can be done remains an intriguing open problem. As in the previous blueprint, we can get "pure" (non-leveled) FHE by assuming circular security.

Our 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. We then translate the result back to the SWHE scheme by homomorphically evaluating the decryption function of the MHE scheme. (Due to the special form of the circuit, switching to the MHE scheme can be done without having to evaluate anything homomorphically.)

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

Date: received 29 May 2011

Contact author: shaih at alum mit edu