Fully Homomorphic Encryption from the ground up

Daniele Micciancio[1][0000−0003−3323−9985]

University of California, San Diego, Mail Code 0404, La Jolla, CA 92093, USA.
daniele@cs.ucsd.edu
http://cseweb.ucsd.edu/~daniele/

Abstract. The development of fully homomorphic encryption (FHE), i.e., encryption schemes that allow to perform arbitrary computations on encrypted data, has been one of the main achievements of theoretical cryptography of the past 20 years, and probably the single application that brought most attention to lattice cryptography. While lattice cryptography, and fully homomorphic encryption in particular, are often regarded as a highly technical topic, essentially all constructions of FHE proposed so far are based on a small number of rather simple ideas. In this talk, I will try highlight the basic principles that make FHE possible, using lattices to build a simple private key encryption scheme that enjoys a small number of elementary, but very useful properties: a simple decryption algorithm (requiring, essentially, just the computation of a linear function), a basic form of circular security (i.e., the ability to securely encrypt its own key), and a very weak form of linear homomorphism (supporting only a bounded number of addition operations.)
All these properties are easily established using simple linear algebra and the hardness of the Learning With Errors (LWE) problem or standard worst-case complexity assumptions on lattices. Then, I will use this scheme (and its abstract properties) to build in a modular way a tower of increasingly more powerful encryption schemes supporting a wider range of operations: multiplication by arbitrary constants, multiplication between ciphertexts, and finally the evaluation of arithmetic circuits of arbitrary, but a-priory bounded depth. The final result is a *leveled*[1] FHE scheme based on standard lattice problems, i.e., a scheme supporting the evaluation of arbitrary circuits on encrypted data, as long as the depth of the circuit is provided at key generation time. Remarkably, lattices are used only in the construction (and security analysis) of the basic scheme: all the remaining steps in the construction do not make any direct use of lattices, and can be expressed in a simple, abstract way, and analyzed using solely the weakly homomorphic properties of the basic scheme.

Keywords: Lattice-based cryptography · fully homomorphic encryption · circular security · FHE bootstrapping.

[1] The "leveled" restriction in the final FHE scheme can be lifted using "circular security" assumptions that have become relatively standard in the FHE literature, but that are still not well understood. Achieving (non-leveled) FHE from standard lattice assumptions is the main theoretical problem still open in the area.