Abstract

In 2009, Gentry proposed the first Fully Homomorphic Encryption (FHE) scheme, an extremely powerful cryptographic primitive that enables to perform computations, i.e., to evaluate circuits, on encrypted data without decrypting them first. This has many applications, particularly in cloud computing. In all currently known FHE schemes, encryptions are associated with some (non-negative integer) noise level. At each evaluation of an AND gate, this noise level increases. This increase is problematic because decryption succeeds only if the noise level stays below some maximum level L at every gate of the circuit. To ensure that property, it is possible to perform an operation called *bootstrapping* to reduce the noise level. Though critical, boostrapping is a time-consuming operation. This expense motivates a new problem in discrete optimization: minimizing the number of bootstrappings in a circuit while still controlling the noise level. In this paper, we (1) formally define the *bootstrap problem*, (2) design a polynomial-time L-approximation algorithm using a novel method of rounding of a linear program, and (3) show a matching hardness result: $(L - \epsilon)$-inapproximability for any $\epsilon > 0$.