Computer Science and Artificial Intelligence Laboratory
Technical Report

MIT-CSAIL-TR-2009-025 June 15, 2009

A Useful Homomorphic Encryption Method

Silvio Micali

massachusetts institute of technology, cambridge, ma 02139 usa — www.csail.mit.edu

A Useful Homomorphic Encryption Method

Silvio Micali
CSAIL, MIT
silvio@csail.mit.edu

June 15, 2009

In its full generality, homomorphic encryption (HE) is a form of encryption enabling the evaluation of a given function F on a plaintext by running another function F' on the ciphertext. The existence of such a general scheme was proved by Gentry at STOC 2009 based on lattice assumptions.

We consider HE as a way for a party A to run a secret program P of another party B on data of party A (and B). In essence this is so because F could be taken to be the universal Turing machine (or a suitable circuit version of it), the plaintext to be B's secret program P.

We now consider the useful choice of P: namely, the program that, on input x, outputs both $h(x)$ and the GMR signature of $h(x)$. Here h could be a collision-resistent function —e.g., one randomly chosen by B in a given family. By GMR signature we mean a non-existentially forgeable digital signature scheme under a chosen message attack. In essence P has embedded the secret signing key of the GMR scheme. The corresponding public key may or may not be made public. The same is true about function h.

We'll elaborate on the merits of this method later on.