Fully Homomorphic Encryption

Mohsen Toorani *

University of Bergen, Norway
mohsen.toorani@uib.no

Abstract. Fully homomorphic encryption schemes allow computing arbitrary functions over encrypted data. They make it possible to delegate processing of encrypted data without giving away access to the plain data. They seem to be interesting cryptographic tools for cloud computing applications. In this paper, we review homomorphic encryption schemes and their properties. We discuss relationships between bootstrappable encryption, somewhat homomorphic encryption, and fully homomorphic encryption.

* This project is co-funded by the EEA Grants and the state budget of the Slovak Republic from the EEA Scholarship Programme Slovakia.