İTÜ Matematik Seminerleri

Computing on Encrypted Data: Homomorphic Encryption

Mehmet Sabır Kiraz

TÜBİTAK BİLGEM UEKAE, Mathematical and Computational Sciences Labs

Abstract

Recent technological developments have increased the number of mobile devices and their usage. Mobile technologies have access to large data centers (in the cloud). Therefore, outsourcing computation securely to a cloud has become a very challenging though inevitable step. However, it is impossible to solve this challenge with the conventional symmetric/asymmetric cryptographic algorithms (e.g., AES, RSA). (Partial/Fully) Homomorphic Encryption is one of the best candidates to securely outsource any computation.

In this talk, we give a survey about the homomorphic encryption techniques and open problems.

Tarih: 5 Aralık 2014, Cuma

Saat: 14:30

Yer: Matematik Bölümü, B-326