Seminar Announcement

Speaker: Ali Aydın Selçuk
TOBB University, Ankara

Threshold Cryptography with Linear Secret Sharing Schemes

Abstract

Threshold cryptography deals with the problem of distributing a secret key or a secret function among a set of users such that only certain authorized subsets can evaluate the secret function together. Traditionally function sharing schemes have been based on the Shamir secret sharing scheme. In this talk, I will describe a method that allows conducting function sharing based on any linear secret sharing scheme, and will present an RSA signature sharing scheme as a practical example. If time permits, I will also describe another method based on the Chinese Remainder Theorem .

DATE: March 18, 2015
TIME: 15:40
PLACE: FEF 404 (Seminar Room)

All interested people are cordially invited.
After the seminar, some cookies and soft drinks will be served.