Abstract:

Secure computation is to do some computation on encrypted data without leaking any information on data. There are two schemes for such computation: (fully) homomorphic encryption and secret sharing. Secure computation is an interesting research topic which is related to many other areas such as external memory algorithms, parallel algorithms, communication complexity, and quantum algorithms. In this talk, we explain basic ideas and algorithms for secret sharing.