به نام خدا

جلسه ارائه هفتگی آزمایشگاه امنیت داده و شبکه

ساختارهای جدید رمزنگاری مبتنی بر مشبکه با استفاده از نمونه برداری گوسی گسسته

New Cryptographic Constructions based on Lattices using Discrete Gaussian Sampling

احمد بورقانی فراهانی

زمان: شنبه ۱۷ فروردین ماه ۱۳۹۲، ساعت ۹:۰۰ صبح

مکان: دانشکده مهندسی کامپیوتر، طبقه پنجم، آزمایشگاه امنیت داده و شبکه

نمونه‌برداری گوسی گسسته، انتخاب نقاط یک مشبکه یا نقاط گسسته دلخواه از فضاست، که بر اساس توزیع احتمال گوسی انجام می‌شود. استفاده از این گونه نمونه‌برداری، از گذشته در مطالعه ریاضی مشبکه‌ها مطرح بوده و در دهه‌ی گذشته نیز، برای بررسی سختی مسائل مشبکه به کار رفته است. در چند سال اخیر با استفاده از این تکنیک، ساختارهای رمزنگاری جدیدی چون توابع دریچه، امضای دیجیتال، و رمزنگاری مبتنی بر شناسه نیز ارائه شده است. در این ارائه به معرفی این ساختارها خواهیم پرداخت.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.