به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

بررسی مباحث جاری رمزشناسی با مروری بر کنفرانس ASIACRYPT'13

Current Trends in Cryptology: An ASIACRYPT'13 Review

احمد بورقانی فراهانی

زمان: شنبه ۷ دی ماه ۱۳۹۲ ساعت ۹ صبح

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

کنفرانس ASIACRYPT یکی از معتبرترین کنفرانس‌های مرتبط با رمزشناسی است. نوزدهمین دوره‌ی این کنفرانس در دسامبر ۲۰۱۳ در حالی برگزار شد که دو کارگاه مستقل «رمزنگاری مبتنی بر مشبکه» و «استفاده از رمزنگاری نوین در کاربرد» نیز در کنار آن ارائه شدند. در این کنفرانس، مباحث متنوعی درباره‌ی پروتکل‌های هیچ‌دانش، خم‌های بیضوی، رمزنگاری احراز اصالت شده، رمزنگاری متقارن، تحلیل رمز، انواع امضای دیجیتال، گمنامی، فرضیات فیزیکی، محاسبات چندطرفه، رمزنگاری مقاوم در برابر نشت، و ... ارائه شدند که می‌تواند معرف مباحث جاری پژوهشگران دنیا در حوزه رمزشناسی باشد. در این ارائه قصد داریم تا برخی عناوین، مفاهیم و نتایج مطرح شده در این کنفرانس را که بیشتر می‌تواند مورد توجه مخاطبین قرار گیرد، مرور کنیم.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.