به نام خدا

جلسه سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

بررسی مباحث جاری رمزنگاری متقارن با مروری بر کنفرانس FSE'15

Current Trends in Symmetric Cryptography: An FSE'15 Overview

احمد بورقانی

زمان: شنبه ۲۲ فروردین ماه ۱۳۹۴ ساعت ۹:۱۵

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهارم، سالن خوارزمی (۴۰۴)

کنفرانس Fast Software Encryption (FSE) یکی از معتبر کنفرانس‌های مرتبط با رمزشناسی است که توسط انجمن بین‌المللی رمزشناسی (IACR) برگزار شده و به طور اختصاصی به مباحث رمزنگاری متقارن اختصاص دارد. بیست و دومین دوره از این کنفرانس، مارس ۲۰۱۵ در ترکیه برگزار شد. ۲۷ مقاله با موضوعاتی چون تحلیل رمز خطی، تفاضلی و خطی-تفاضلی، حملات ملاقات در میانه (Meet-in-the-middle)، تحلیل رمز چرخشی، حمله بومرنگ و غیره روی شماهایی چون TWINE، CLEFIA، Camellia، PRINCE، PRESENT، ICEPOLE، JAMBU و شماهای مبتنی بر طراحی Even-Mansour در این کنفرانس ارائه شدند. بعلاوه یک سخنرانی مدعو و یک مقاله به برنامه جاسوسی فراگیر آمریکا و نقش و تلاش جامعه رمزنگاری برای مقابله با آن اختصاص یافته شد. 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.