دوره درسی

رمزنگاری پساکوانتومی کد-مبنا

عنوان درس:

مباحثی در رمزنگاری: رمزنگاری پساکوانتومی کد-مبنا

ارائه دهنده:

عمران احمدی (پژوهشکده ریاضیات)

خلاصه:

امنیت مهمترین سامانه‌های رمزنگاری کلید عمومی مورد استفاده کنونی مبتنی بر سختی تجزیه اعداد صحیح یا سختی حل مساله لگاریتم گسسته در گروه خم بیضوی تعریف شده بر روی یک میدان متناهی است. این در حالی است که در صورت ساخته شدن کامپیوترهای کوانتومی میتوان با استفاده از الگوریتم پیتر شر مسایل فوق را در زمان کوتاهی حل کرده و سیستمهای رمز مربوطه را شکست. با توجه به این مساله، شاخه‌ای جدید در رمزنگاری در دو دهه گذشته پدید آمده است که به آن رمزنگاری پساکوانتومی می‌گویند. یکی از زیر شاخه‌های مهم رمزنگاری پساکوانتومی، رمزنگاری کد-مبنا است. در این دوره‌ی درسی به بحث و بررسی آخرین تحولات این عرصه از رمزنگاری پرداخته می‌شود.

واحد: ۴ واحد درسی

پیش‌نیاز: جبرخطی، نظریه میدانهای متناهی.

مرجع اصلی:

A Survey on Code-based Cryptography: Violetta Weger, Niklas Gassner , and Joachim Rosenthal.

این درس برای دانشجویان دوره کارشناسی ارشد و دکتری می‌باشد.

(در صورت تمایل، دانشجویان کارشناسی با در نظر گرفتن پیش‌فرض‌ها می توانند در دوره شرکت کنند.)

اولین جلسه توجیهی:

دوشنبه ۱۴۰۳/۷/۲ ساعت ۱:۳۰ سالن ۱

جلسه توجیهی و کلاس درس به صورت حضوری برگزار می‌شود.

در صورت تمایل به شرکت در کلاس، به آدرس oahmadid@ipm.ir ایمیلی ارسال نمایید.

آدرس: میدان نیاوران، پژوهشگاه دانشهای بنیادی،
پژوهشکده ریاضیات، سالن ۱