دوره درسی

رمزنگاری پساکوانتومی مشبکه-مبنا

عنوان درس:

مباحثی در رمزنگاری: رمزنگاری پساکوانتومی مشبکه-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 مشبکه-مبنا است. در این دوره‌ی درسی به بحث و بررسی آخرین این عرصه از رمزنگاری پرداخته می‌شود.

واحد: ۴ واحد درسی

پیش‌نیاز: جبرخطی، میدانهای متناهی.

مرجع اصلی

Lattice-based Cryptography for beginners: Dong Chi, Jeong Choi, Jeong Kim and Taewan Kim

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)

ساعات برگزاری:

دو شنبه‌ها از ۱۴۰۳/۱۱/۱۵ ساعت ۹ الی ۱۲ سالن ۱

کلاس درس به صورت حضوری برگزار می‌شود.