کارگاه آموزشی

فرازهایی از رمزنگاری پساکوانتومی

Selected Areas in Post-quantum Cryptography

برگزارکنندگان:

- پژوهشکده الکترونیک، دانشگاه صنعتی شریف
- قطب علمی رمز
- انجمن رمز ایران
- شاخه دانشجویی انجمن رمز ایران در دانشگاه صنعتی شریف

مسئول برگزاری:

- دکتر ترانه اقلیدس

۲۴ و ۲۵ بهمن ماه ۱۳۹۷

دانشگاه صنعتی شریف، دانشکده مهندسی برق

سالن کهربا

نقشه‌ی دانشگاه صنعتی شریف

دانشگاه صنعتی شریف

جدول زمان‌بندی روز اول (چهارشنبه ۲۴ بهمن)

۹:۰۰–۹:۲۵	پذیرش و افتتاحیه
۹:۳۰–۱۰:۴۵	مقدمه‌ای بر رمزنگاری پساکوانتومی خانم دکتر ترانه اقلیدس
۱۰:۴۵–۱۱:۰۰	پذیرایی
۱۱:۰۰–۱۲:۱۵	رمزنگاری مشبکه مبنا، مسیری برای امنیت اثبات‌پذیر آقای دکتر حسن خدایی‌مهر
۱۲:۱۵–۱۳:۳۰	نماز و ناهار
۱۳:۳۰–۱۴:۴۵	امیدی تازه برای به‌کارگیری **LWE** در طراحی سامانه‌های رمز پساکوانتومی سبک وزن آقای دکتر حسن خدایی‌مهر
۱۴:۴۵–۱۵:۰۰	پذیرایی
۱۵:۰۰–۱۶:۱۵	امضاهای رقمی مبتنی بر توابع چکیده‌ساز (بخش اول) آقای دکتر رسول محمدی
۱۶:۱۵–۱۶:۳۰	پذیرایی
۱۶:۳۰–۱۷:۴۵	امضاهای رقمی مبتنی بر توابع چکیده‌ساز (بخش دوم) آقای دکتر رسول محمدی

جدول زمان‌بندی روز دوم (پنجشنبه ۲۵ بهمن ۹۷)

۹:۰۰–۹:۲۵	برنامه‌ی آغاز روز دوم
۹:۳۰–۱۰:۴۵	رمزنگاری پساکوانتومی مبتنی بر کدهای با متر همینگ خانم دکتر خدیجه باقری
۱۰:۴۵–۱۱:۰۰	پذیرایی
۱۱:۰۰–۱۲:۱۵	رمزنگاری پسا کوانتومی مبتنی بر کدهای با متر رتبه آقای مهندس وحید یوسفی‌پور
۱۲:۱۵–۱۲:۳۰	اختتامیه
۱۲:۳۰–۱۲:۴۵	تحویل فرم های ارزشیابی و دریافت گواهی شرکت در کارگاه

در مورد سخنرانان

خانم دکتر ترانه اقلیدس دانشیار پژوهشکده الکترونیک در دانشگاه صنعتی شریف، مدرک دکتری خود را در رشته ریاضی از دانشگاه گیسن آلمان در سال ۲۰۰۰ میلادی دریافت کرده است. ایشان، از بهمن ۱۳۸۰ تاکنون عضو هیئت علمی پژوهشکده الکترونیک در دانشگاه صنعتی شریف است. زمینه‌های علمی-پژوهشی مورد علاقه ایشان شامل مبانی رمزنگاری متقارن و نامتقارن، رمزنگاری پساکوانتومی به ویژه رمزنگاری کدمبنا و رمزنگاری مشبکه‌مبنا و به‌طور کلی مدل‌سازی ریاضی برای مسائل برخاسته از پدیده‌های دنیای واقعی است.

صفحه شخصی: http://sharif.ir/~teghlidos

خانم دکتر خدیجه باقری مدرک کارشناسی و کارشناسی ارشد خود را در رشته ریاضی کاربردی به ترتیب درسال‌های ۱۳۸۹ و ۱۳۹۱ دریافت کرده است. ایشان مدرک دکترای خود را در رشته ریاضی کاربردی (گرایش رمز و کد) از دانشگاه صنعتی امیرکبیر درسال ۱۳۹۶ دریافت کرده است. زمینه‌های علمی-پژوهشی مورد علاقه ایشان شامل رمزنگاری پساکوانتومی، طراحی سامانه‌های رمزگذاری متقارن و نامتقارن مبتنی بر کدهای تصحیح خطا، مشبکه‌ها و کدمشبکه‌ها، سامانه‌های توأم رمزگذاری-کدگذاری، سامانه‌های رمز جستجوپذیر و بلاک چین است.

آقای دکتر حسن خدایی مهر استادیار گروه علوم کامپیوتر و آمار دانشکده ریاضی در دانشگاه صنعتی خواجه نصیرالدین طوسی، مدرک دکتری خود را در رشته ریاضی از دانشگاه صنعتی امیرکبیر در سال ۲۰۱۷ میلادی دریافت کرده است. ایشان از سال ۱۳۹۶ تاکنون عضو هیئت علمی دانشگاه صنعتی خواجه نصیرالدین طوسی است. زمینه‌های علمی-پژوهشی مورد علاقه ایشان شامل کدگذاری و نظریه اطلاع، رمزنگاری، نظریه مشبکه و کاربردهای آن در مخابرات بی‌سیم، امنیت در مخابرات بی‌سیم و کاربرد مشبکه در امنیت لایه فیزیکی است.

آقای دکتر رسول محمدی دارای مدرک کارشناسی ارشد ریاضی از دانشگاه صنعتی شریف و مدرک دکترای ریاضی از دانشگاه تربیت مدرس (۹۷-۱۳۹۲) با موضوع کدهای خطی روی برخی خم‌های بیضین است. ایشان دارای بیش از ۸ سال سابقه حضور در صنایع الکترونیک کشور است. زمینه‌های تحقیقاتی مورد علاقه ایشان شامل رمزنگاری پساکوانتومی، رمزگذاری تمام‌همریخت و کدهای کلاسیک و کوانتومی مبتنی بر هندسه جبری است.

آقای مهندس وحید یوسفی‌پور مدرک کارشناسی خود را در رشته مهندسی برق، گرایش مخابرات از دانشگاه صنعتی امیرکبیر در سال ۱۳۹۳ و مدرک کارشناسی ارشد خود را در رشته مهندسی برق، گرایش مخابرات امن و رمزنگاری از دانشگاه صنعتی شریف در سال ۱۳۹۵ دریافت کرده است. وی در حال حاضر دانشجوی دکتری مهندسی برق در دانشگاه صنعتی شریف است. . زمینه‌های علمی-پژوهشی مورد علاقه ایشان بررسی ساختارهای رمزنگاری کلید عمومی مدرن کد مبنا و مشبکه مبنا برای برقراری امنیت در پروتکل های اینترنتی و رایانش ابری است.

کارگاه آموزشی

۲۴ و ۲۵ بهمن ماه ۱۳۹۷
دانشگاه صنعتی شریف، دانشکده مهندسی برق

کارگاه آموزشی فرازهایی از رمزنگاری پساکوانتومی

سامانه‌های رمز کلید همگانی مانند RSA، در حال حاضر در سراسر جهان برای حفاظت اطلاعات در بستر اینترنت و دیگر شبکه‌های ارتباطی کامپیوتری استفاده می‌شوند. با پیشرفت‌های موجود در حوزه محاسبات کوانتومی و ارائه الگوریتم کوانتومی Shor در سال ۱۹۹۴ برای حل مسئله تجزیه اعداد مرکب بزرگ و لگاریتم گسسته، امنیت سامانه‌های رمز کلید همگانی کلاسیک در حضور کامپیوترهای کوانتومی مورد تهدید قرار گرفته است. Shor بیان می‌کند که مسئله تجزیه اعداد مرکب بزرگ در یک کامپیوتر کوانتومی که شامل ده‌ها یا صدها هزار گیت باشد به سرعت قابل حل است. اگرچه امروزه کامپیوترهای کوانتومی با چنین اندازه‌ای وجود ندارد اما پروژه‌های بزرگی برای ساخت چنین کامپیوترهایی طی ۱۰ تا ۲۰ سال آینده وجود خواهند داشت. محققان زیادی به دنبال یافتن راهی برای ایجاد امنیت در عصر کوانتومی هستند. ماهیت حل این مسئله با دو رویکرد متفاوت درنظر گرفته می‌شود. روش نخست از مکانیک کوانتومی برای طراحی رمزنگاری مبتنی بر کوانتوم استفاده می‌کند که با توجه به اصول پایه‌ای مکانیک کوانتومی شکست‌ناپذیر خواهد بود. روش دوم بر این اساس است که الگوریتم‌های کلاسیک جدیدی، به نام رمزنگاری پساکوانتومی، طراحی شود که بر مبنای سختی تجزیه اعداد مرکب بزرگ نیستند و با استفاده از الگوریتم Shor یا هر الگوریتم کوانتومی دیگر شکسته نمی‌شوند.

هر دو رویکرد مزایا و معایبی دارد. رویکرد رمزنگاری پساکوانتومی تنها نیازمند تغییرات نرم‌افزاری است و در زیرساخت‌های موجود قابل پیاده‌سازی است. محققان در حال مطالعه روی الگوریتم‌های این رویکرد برای سال‌های آینده هستند تا تضمین کنند که هیچ راه شناخته شده‌ای برای حمله به آن‌ها از طریق محاسبات کلاسیک و کوانتومی وجود ندارد. اما هرگز نمی‌توان به‌طور قطعی در مورد امنیت آن‌ها اظهار نظر کرد. رویکرد رمزنگاری کوانتومی، که بر اصول بنیادین مکانیک کوانتومی استوار است، یک اطمینان ۱۰۰٪ برای شکست‌ناپذیر بودن الگوریتم‌های این حوزه ارائه می‌دهد، اما این رویکرد بسیار پرهزینه است زیرا بر زیرساخت‌های ارتباطی و سخت‌افزاری جدید تکیه دارد. رمزنگاری کوانتومی با احتمال زیاد توسط بخش‌های نظامی/ دولتی استفاده خواهد شد که در آن‌ها نیاز به اطمینان کامل از شکسته نشدن الگوریتم وجود دارد و پرهزینه بودن از درجه اهمیت کمتری برخوردار است. اما، برای بیشتر کاربردهای تجاری استاندارد مانند پردازش تراکنش‌های کارت‌های اعتباری در بستر اینترنت، رویکرد رمزنگاری پساکوانتومی مطلوب است.