آزمایشگاه تحقیقاتی رمزنگاری و سیستم های امن
دانشکده مهندسی برق

دکتر مجید نادری

هسته اولیه تاسپس آزمایشگاه تحقیقاتی رمزنگاری و سیستم های امن در سالهای اولیه ۱۳۸۰ همزمان با تعریف و تدوین برنامه آموزشی گروه مخابرات امن در فناوری اطلاعات بوجود آمد و این ایده بدلیل نیازمندیهای نوینی بود که در ایران بوجود آمده بود و در حال تکوین بود. رشد و تحول فناوری اطلاعات در دهه ۱۳۷۰ و بوجود آمدن نیازهای جدید IT و ICT در جهان و ایران و بوجود آمدن بنیاد های علمی جدید همانند E-Comerce، E-Government، E-Teaching ، E-Booking و E-Health و دهها پدیده فناوری جدید در دنیا و ایران ما را به فکر گرایش جدیدی در دانشکده مهندسی برق انداخت و بدنبال این نیاز اقدام به تدوین برنامه آموزش و تحقیقاتی در فناوری اطلاعات گردید و نتیجه این کوشش گروه مخابرات امن به تصویب و تایید دانشگاه علم و صنعت ایران و سپس وزارت علوم و فناوری اطلاعات منجر گردید. برای اینکه دانشجویان ارشد و دکترا این گروه جدید التاسیس ، آزمایشگاهی جهت تحقیقات و پژو هشهای علمی خود داشته باشند، آزمایشگاه تحقیقاتی رمزنگاری و سیستم های امن با همکاری و سرمایه گذاری معاونت محترم آموزشی،؛ پژوهشی و روابط بین المللی وزارت ارتباطات و فناوری اطلاعات طراحی و تصویب گردید و در سال تحصیلی ۱۳۸۲ این آزمایشگاه آماده سرویس دهی به دانشجویان دانشکده مهندسی برق گردید. توان علمی و عملیاتی این آزمایشگاه پژوهشی با خرید تجهیزات و امکانات خارجی در سالهای بعد روز به روز فزونتر گردید و در حال حاضر قادر است به کلیه دانشجویان مخابرات امن و سایر محققین و پژوهندگان نیازمند ، خدمات و سرویس های لازم را عرضه نماید.

در این آزمایشگاه سیستم کامپیوتر پردازش موازی شرکت سان (***SUN***) و بردهای FPGA سریع و قدرتمند برای تولید نمونه های سخت افزاری و نرم افزاری مدرن آماده و تهیه گردیده است. علاوه بر امکانات فوق ، آزمایشگاه تحقیقات رمزنگاری و سیستم های امن دارای شبکه یکپارچه کامپیوتری با سیستم عامل ویندوز و یونیکس می باشد و قادر است نیاز کلیه پژوهشگران این رشته را تامین نماید.

گروه آموزشی مخابرات امن با تنوع گروههای آموزشی خود قادر است علاوه بر آموزش های مصوبه رسمی خود، آموزش های تخصیصی زیر را برای پژوهشگران علاقمند به این رشته به صورت دوره های کوته مدت، میان مدت و دراز مدت رسمی ارائه و تعریف نماید.

۱- امنیت شبکه های کامپیوتری
۲- امنیت سیستم های مخابراتی
۳- سیستم های رمزنگاری
۴- سیستم های درهم ساز برای امن نمودن اسناد و مدارک

۵- طراحی سیستم های امن
۶- الگوریتم ها و امنیت بخشیدن به سیستم های جدید مخابراتی و شبکه های جدید ارتباطی

در سالهای قبل پروژه های پژوهشی وتحقیقاتی زیر در این آزمایشگاه انجام گردیده است:

الف: پروژه هایی که توسط دانشجویان دکتری انجام شده است:

۱.طراحی سوئیچ ATM یک به چند قابل توسعه: علیرضا حسام محسنی
۲. مدلسازی و طراحی ساختاری سیستم های پردازش موازی کلاستر بندی شده چند طبقه: هادی شهریار شاه حسینی
۳.مدل سازی زیر لایه دستیابی به کانال و اولویت بندی مبتنی بر منطق فازی در شبکه های اقتضایی: علی خیاط زاده ماهانی
۴ .طراحی و پیاده سازی شبکه های فیبر نوری خود ترمیم: یوسف صیفی کاویان
۵.طراحی و تحلیل توابع درهم ساز برای به کارگیری در ساختار سیستم های رمزنگاری : نصور باقری

ب: پروژه هایی که توسط دانشجویان کارشناسی ارشد انجام شده است:

۱. طیف نگاری حالت گذرای تراز های عمیق، طراحی و ساخت سیستم کامپیوتری DLTS: علی صدر
۲.طیف نگاری حالت گذرای تراز های عمیق، محاسبات فیزیکی و تولید سیگنالهای کنترلی: شعبانعلی گل
۳.طیف نگاری حالت گذرای تراز های عمیق، طراحی و ساخت سیستم کنترل الکترونیکی – کامپیوتری: علی اصغر اروجی
۴.سیستم تعیین وضعیت: محمد رضا صالحی
۵.مدلسازی ریاضی سیستم های مولتی پروسسور: کاوه فضلی
۶.تطبیق و بهبود عملکرد پروتکل TCP در شبکه های اقتضایی: سید روح ا... میر اکبری
۷.بهبود تخصیص منابع در شبکه های سلولی چند گامی: بهزاد کثیری مشهد
۸.طراحی الگوریتمی جهت مسیر یابی در شبکه های اقتضایی به صورت چند مسیره به منظور افزایش قابلیت تحمل پذیری خطا : شبنم واحدی
۹.امن سازی اسناد و مدارک با استفاده از توابع درهم ساز: معصومه صفخانی
۱۰.طراحی و شبیه سازی برد واسط و بوجود آوردن شبکه برای رمزنگاری و امنیت در مبادلات شبکه محلی اترنت : مریم دبردانی
۱۱.امنیت شبکه های محلی بی سیم: لیلی اسماعیلانی
۱۲.معماری،مدیریت کلید به منظور امن کردن مبادلات اطلاعات بین FPGA و واحدهای خارجی : صوفیا آهنج
۱۳.طراحی و شبیه سازی پردازنده سی و دو بیتی رمزنگاری RISC: ابوذر احسانی
۱۴.طراحی پردازنده ویژه برای الگوریتم های رمز قطعه ای: مژده مهاجرانی
۱۵.ارزیابی نقاط آسیب پذیر حاصل از سرریز بافرها و راههای مقابله با آنها: نازلی احمد خان بیگی

۱۶.طراحی و شبیه سازی هسته مرکزی پردازنده شبکه: بهرام غفاری

۱۷.طراحی واحد پایپ لاین یک پردازنده : علی مکنونی نژاد

۱۸.طراحی، شبیه سازی و سنتز یک کمک پردازنده برای انجام DCT/IDCT دو بعدی: علی خیاط زاده ماهانی

۱۹.طراحی یک تابع درهم ساز چند منظوره: زهرا حیدران داروقه

۲۰.تشخیص تعدی در مسیر یابی شبکه های سیار اقتضایی مبتنی بر الگوریتم SVM : سید علیرضا نیک زاد

۲۱.بهینه سازی پروتکل VGAP برای تامین کیفیت سرویس در شبکه های اقتضایی: خدیجه غافرین

۲۲.طراحی مدار مجتمع خروجی یک سیستم اتوماسیون صنعتی با استفاده از تکنولوژی CMOS: جمال غلامی آهنگران

۲۳.کنترل و مدیریت ازدحام در شبکه های کامپیوتری به کمک مدل سازی : رامین بلیوان

24.دیجیتایز کردن بلادرنگ تصویر و تقسیم آن برای ارسال روی باند باریک: بیتا ناصری

۲۵.ارزیابی نقاط آسیب پذیر حاصل از سر ریز بافرها و راههای مقابله با آنها: نازلی احمد خان بیگی

۲۶.شبیه سازی رمزنگاری کوانتومی با توزیع کلید کوانتومی: حسین شفیعی

۲۷.تحلیل نقص ناشی از حملات در الگوریتم های رمز رشته ای : سحر سادات فرنودی

برای دسترسی و اطلاع رسانی بیشتر می توانید به سایت WWW.CRYPTO.IUST.AC.IR مراجعه و مکاتبه نمایید.