دانشکده مهندسی برق (پردیس ولنجک)
Faculty of Electrical Engineering

بسمه تعالی

زمان نصب در تابلوی اعلانات:

☐ دفاع از رساله دکتری ☐ سمینار عمومي (Colloquium)

■ دفاع از پایان‌نامه کارشناسی‌ارشد ☐ سمینار تخصصي (Seminar)

☐ سمینار تخصصي و مشورتي (Informal Seminar)

عنوان : بهبود روش‌های جستجوی مشخصه‌ی تفاضلی در رمزهای متقارن

سخنران : حسین مقیمی

چکیده:

حمله‌ی تفاضلی منقطع یکی از روش‌های تحلیل رمزهای قالبی است. با وجودیکه زمان زیادی از معرفی این نوع حمله می‌گذرد، اما این تحلیل در سال‌های اخیر مورد توجه مجدد تحلیل‌گران قرار گرفته‌است و پیشرفت‌های قابل توجهی در کارایی آن حاصل شده‌است. از سوی دیگر، بررسی آسیب‌پذیری الگوریتم‌های رمزنگاری در برابر حملات مختلف امری بسیار ضروری در امنیت رمزها و در عین حال یک فرآیند زمان‌بر و مستعد خطا است. از این جهت برای ارزیابی میزان مقاومت الگوریتم‌های رمزنگاری، خودکارسازی حملات آن‌ها به جهت افزایش سرعت و دقت، از اهمیت بالایی برخوردار است. یکی از پرکاربردترین و در عین حال موثرترین روش‌های خودکارسازی، استفاده از ابزار مسئله‌ی برنامه‌ریزی عدد صحیح آمیخته (MILP) است.

در این پایان‌نامه نخست با ارائه چند قضیه به توسعه مبانی نظری حمله تفاضلی منقطع و نیز ارائه یک چارچوب کلی برای این حمله و روابط پیچیدگی زمانی و داده آن می‌پردازیم. سپس با استفاده از ابزار MILP برای دو خانواده رمز قالبی SAND-n و QARMA-n تحلیل‌های تفاضلی منقطع ارائه خواهیم کرد. با استفاده از مدل‌سازی انجام‌شده برای رمز قالبی SAND-n که n بیانگر طول قالب یعنی ۶۴ و ۱۲۸ بیت است، در مدل تک کلیدی به ترتیب مشخصه‌ی ۱۰ دوری و ۱۳ دوری، و برای مدل کلید مرتبط حمله‌ی به ترتیب ۱۵ و ۳۱ دوری یافت شد که اولین تحلیل تفاضل منقطع برای این رمز قالبی است. برای هر دو نسخه رمز قالبی QARMA-n نیز (که n=۶۴و ۱۲۸) نخست یک تمایزگر ۶ دوری و سپس با اتکا به آن یک حمله ۱۰ دوری با پیچیدگی داده و پیچیدگی زمانی به مراتب کمتری در مقایسه با کران بالای ادعاشده توسط طراحان این الگوریتم معرفی شد. این حمله بهترین حمله به این رمز در زمان نگارش این پایان‌نامه است.

تاریخ برگزاری: ۲۸ شهریور ۱۴۰۲

زمان برگزاری: ساعت ۱۳ الی ۱۵

مکان برگزاری: دانشکده مهندسی برق (پردیس ولنجک)، اتاق ۲۰۰ (دفاعیه)