به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

بررسی هفت ساختار رمز قالبی امن قابل اثبات از منظر حمله تفاضلی

Seven New Block Cipher Structures With Provable Security Against Differential Cryptanalysis

فرید زرین خط

زمان: شنبه ۲۱ دی ماه ۱۳۹۲ ساعت ۹ صبح

مکان: دانشکده مهندسی کامپیوتر، طبقه پنجم، آزمایشگاه امنیت داده و شبکه

ساختارهای رمز دارای امنیت قابل اثبات، خانواده مهمی از رمزکننده‌های قالبی را تشکیل می‌دهند. در این میان هفت ساختار مطرح در رمزکننده‌های موجود عبارتند از انواع ساختار فیستلی(Feistel)، رمزکننده CLEFIA، زیر ساختار های متنوع FO برای الگوریتم رمز MISTY، و ..... .

از دیگر سو حملات تفاضلی یکی ابزارهای مهم تحلیل و شکست الگوریتم‌های رمز به شمار می‌روند. در این ارائه کران‌های مناسب پارامترهای موثر اجرای این حمله (از جمله متوسط احتمال تفاضلی و ...) تشریح خواهند شد.

شرکت در این جلسه برای تمامی دانشجویان علاقه مند آزاد است.