انجمن رمز ایران
شاخه دانشجویی دانشگاه شهید بهشتی

پژوهشکده فضای مجازی

مهندسی رمزنگاری خم بیضوی

سرکار خانم دکتر راضیه سالاری فرد
دکتری رشته معماری کامپیوتر از دانشگاه صنعتی شریف

چکیده

رمزنگاری مبتنی بر خم بیضوی به دلیل سطح امنیت یکسان ولی طول کلید کوچکتر در مقایسه با سایر روش‌های کلاسیک رمزنگاری نامتقارن، بسیار مورد توجه قرار گرفته است. ضرب نقطه‌ای اساسی‌ترین عمل در محاسبات رمزنگاری خم بیضوی است. بدین ترتیب معماری‌های با سرعت بالا و پیچیدگی کم آن موجب طراحی سامانه‌های رمزنگاری کارا می‌شود. یکی از خم‌های امن که محاسبات سبکی نیز دارد، خم۲۵۵۱۹ است. این خم امروزه بسیار مورد توجه قرار گرفته است و از جمله کاربردهای آن می‌توان به پیام‌رسان WhatsApp و آخرین نسخه استاندارد TSL اشاره کرد. در این ارائه، به شیوه طراحی و پیاده‌سازی یک ضرب نقطه‌ای با تاخیر و پیچیدگی کم روی خم۲۵۵۱۹ به همراه راه‌کارهای ضد حملات DPA پرداخته می‌شود. به منظور ارزیابی این معماری با کارهای پیشین به شیوه‌های ارزیابی معماری و معیارهای مرسوم نیز پرداخته می‌شود.

درباره‌ی سخنران :

راضیه سالاری فرد سه مقطع کارشناسی، کارشناسی ارشد و دکتری را در دانشکده کامپیوتر دانشگاه شریف و در گرایش معماری کامپیوتر گذرانده است. همچنین سه سال در شرکت نادشریف که حوزه امینت کار می کند سابقه کار دارد. حوزه پژوهش دوره دکتری وی پیاده سازی کارای رمزنگاری خم بیضوی بوده است که از ماحصل آن سه مقاله در مجله tcas1 چاپ شده است.

زمان: سه شنبه ۳۰ مهرماه ساعت ۱۲:۳۰ الی ۱۳:۳۰

مکان : سالن کنفرانس پژوهشکده فضای مجازی، ساختمان شهدا، دانشگاه شهید بهشتی