معرفی پنجاهمین وبینار تخصصی انجمن رمز ایران
زمان سخنرانی ۲ دی ماه ۱۴۰۴ ساعت ۱۵

معرفی سخنران:

آقای مهندس کسری عباس‌زاده مدرک کارشناسی خود را در رشته مهندسی برق از دانشگاه صنعتی شریف در سال ۱۴۰۰ دریافت کرده است. ایشان در حال حاضر در مقطع دکتری، در رشته علوم کامپیوتر و در دانشگاه مریلند مشغول به تحصیل هستند. پژوهش‌های ایشان در سال‌های اخیر متمرکز بر سامانه‌های اثبات ناتراوا و کابردهای آنها بوده‌است.

عنوان سخنرانی:

Recursive Zero-Knowledge Arguments and Applications

اثبات‌های ناتراوای بازگشتی و کاربردهای آن

چکیده سخنرانی:

اثبات‌های ناتراوا[1] این امکان را فراهم می‌کنند که بتوان درستی یک گزاره را بدون در اختیار گذاشتن اطلاعاتی درباره شاهد گزاره تایید کرد. در سال‌های اخیر، با بهبود عملکرد و کاهش پیچیدگی، این سامانه‌های اثبات، کاربردهای گسترده‌ای در زمینه‌های متنوع پیدا کرده‌اند و بعنوان نمونه از زنجیره های قالبی و فناوری‌های حفظ حریم خصوصی می توان یاد نمود. اثبات‌های ناتراوای بازگشتی[2] گروه خاصی از اثبات‌های ناتراوا هستند که برای احراز درستی محاسبات تکرار شونده به صورت فشرده و بهینه استفاده می‌شوند. در این ارائه به معرفی دو کاربرد نوین برای اثبات‌های بازگشتی خواهیم پرداخت. کاربرد اول یادگیری ماشین وارسی‌پذیر است که به طور خاص نشان می‌دهیم چگونه توسط اثبات‌های بازگشتی می‌توان آموزش یک شبکه عصبی را به صورت بهینه احراز کرد. کابرد دوم پروتکل‌های تجمیع امن[3] است که در یادگیری فدرال و تحلیل محرمانه داده استفاده می‌شود. در این قسمت از ارائه، ابتدا لزوم استفاده از اثبات‌های ناتراوا در پروتکل‌های تجمیع امن را بررسی می‌کنیم و سپس نشان می‌دهیم چگونه به کمک اثبات‌های بازگشتی می‌توان هزینه‌ی راستی‌آمازیی یک تجمیع امن را برای کاربرها به حداقل رساند.

[1] Zero-Knowledge Arguments
[2] Recursive Zero-Knowledge Arguments
[3] Secure Aggregation