

به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه



محرمانگی الگویی دسترسی به داده با استفاده از ماشین فراموش کار

Confidential Access to the Data With Using Oblivious RAM

الهه سادات نجم آبادی

زمان: شنبه ۶ اردیبهشت ماه ۱۳۹۳ ساعت ۳ بعد از ظهر

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهارم، سالن ۴۰۴

با رشد روزافزون تمایل صاحبان داده به برون سپاری آنها، چالش‌های امنیتی مرتبط با آن بسیار مورد توجه و تحقیق قرار گرفته است. در اکثر پژوهش‌های مرتبط با این موضوع، دو مبحث محرمانگی محتوای داده برون سپاری شده و همچنین کنترل دسترسی به آنها مورد بررسی قرار گرفته است ولی تحقیقات کمتری پیرامون محرمانگی الگویی دسترسی و محرمانگی دسترسی به داده‌ها انجام گرفته است. در مواردی نیاز است که علیرغم اعمال مطلوب کنترل دسترسی، محتوای پرس‌وجو و حتی الگویی دسترسی به داده‌ها از دید کاربر مخفی بماند. یکی از روش‌های موجود برای انجام این مهم استفاده از ماشین فراموش کار است. ماشین فراموش کار قدرت مخفی کردن دسترسی و الگویی دسترسی برای تمامی داده ساختارها در تمام سطوح (فایل سیستم، پایگاه داده و ...) را داراست.

در این ارائه به تعریف فراموش کاری، ماشین فراموش کار ساده، ماشین فراموش کار بهسازی شده خواهیم پرداخت.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.