به نام خدا

جلسه ارائه هفتگی آزمایشگاه امنیت داده و شبکه


# تصدیق اصالت مشبکه‌مبنای امن-اثبات‌پذیر

# On Lattice-based Provably-secure Authentication

**احمد بورقانی**

زمان: شنبه ۲۹ شهریور ماه ۱۳۹۳ ساعت ۳ عصر

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

رمزنگاری مشبکه‌مبنا، به عنوان یکی از مهم‌ترین گزینه‌ها برای رمزنگاری پَساکوانتمی، توجه ویژه‌ای را به خود اختصاص داده است. تصدیق اصالت مشبکه‌مبنا یکی از بخش‌های مهم از این نوع رمزنگاری را تشکیل می‌دهد و پژوهش‌های قابل توجهی در این حوزه انجام شده است. در این ارائه که مشابه جلسه دفاع از پیشنهاد پژوهشی اینجانب نیز می‌باشد، ما دو ایده برای نوآوری در تصدیق اصالت مشبکه‌مبنا ارائه می‌کنیم. ایده اول، ارائه پروتکل‌های تصدیق اصالت مشبکه‌مبنایی به منظور استفاده در کاربرد و مناسب برای محدود-سخت‌افزارها می‌باشد که از آن جمله می‌توان به کارت‌های هوشمند و میکروکنترلرها اشاره کرد. ایده‌ی دوم ارائه‌ی طرح‌هایی از شِمای رمزنگاری تصدیق اصالت شده (AE) مبتنی بر مشبکه می‌باشد که تاکنون در ادبیات موضوع به آن اشاره نشده است.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.