



بیستمین کنفرانس ملی سالانه انجمن کامپیوتر ایران  
سمپوزیوم بین المللی هوش مصنوعی و پردازش سیگنال انجمن کامپیوتر ایران

کارگاه‌های آموزشی CSICC 2015 و AISP 2015

کد کارگاه	WR1506
عنوان کارگاه	شبیه سازی و پیاده سازی الگوریتم ها و پروتکل های کوانتومی
چکیده	<p>دو مفهوم توزیع کلید کوانتومی و الگوریتم های کوانتومی نقشی اساسی در تبادل اطلاعات و امنیت ارتباطات دارد. با آغاز رایانش کوانتومی این موضوع روند جدیدی به خود گرفته است. به طور مثال پروتکل BB84 و دیگر پروتکل های الهام گرفته از این ساختار دارای امنیت بلاشرط می باشند و با چشم پوشی از نواقص سخت افزاری در راه پیاده سازی این پروتکها، می توان این ابزار ارتباطی را به عنوان تکیه گاه مناسبی برای دنیای ارتباطات امن در نظر گرفت. از طرف دیگر موضوعی که دنیای رمزنگاری کنونی را تهدید می کند ظهور الگوریتم های کوانتومی مانند الگوریتم شور و الگوریتم گراور می باشد که توانسته امنیت سیستم های رمزنگاری را با چالشهای بزرگی مواجه کند. اما با تمام مزیت هایی که این ابزارهای محاسباتی در اختیار ما قرار داده است، پیاده سازی عملیاتی آنها به علت ضعف های سخت افزاری کوانتومی با مشکل روبه رو می باشد. لذا می توان با شبیه سازی این الگوریتمها و پروتکلها به کمک کامپیوتر های کلاسیک تا اندازه ای به نتایج محاسباتی دست یافت که در تحلیل سیستم های امنیتی نقش موثری داشته باشد.</p>
زبان ارائه کارگاه	فارسی
زمان برگزاری	یک شنبه ۱۰ اسفند ۱۳۹۳ - ساعت ۸ الی ۱۸ - (۸ ساعت)
مخاطبان	سازمانهای دفاعی - سازمانهای امنیتی - متخصصین دفاع سایبری - فعالین بازارها و تجارت الکترونیک - متخصصین بانکداری الکترونیک (امضای دیجیتال) - دانشجویان رشته های نرم افزار و سخت افزار کامپیوتر، رمز و فیزیک کوانتوم.
ارائه دهندگان	دکتر مجید فرهادی - مهندس علی عامری مهر - مهندس احد روانشاد - مهندس محمد علی خندان - مهندس آرمان گودرزی - مهندس علی محمودی نهرانی
پیش نیازهای کارگاه	مفاهیم جبر خطی زبان های برنامه نویسی شبیه سازی، C , JAVA , Linux Programming
هزینه	۱۰۰۰۰۰۰ ریال
توضیحات	گواهی نامه حضور در کارگاه برای شرکت کنندگان صادر می شود.



بیستمین کنفرانس ملی سالانه انجمن کامپیوتر ایران  
سمپوزیوم بین المللی هوش مصنوعی و پردازش سیگنال انجمن کامپیوتر ایران

کارگاه‌های آموزشی CSICC 2015 و AISP 2015

سرفصل کارگاه:

- مقدمات مکانیک و محاسبات کوانتومی
- زبان های برنامه نویسی کوانتومی
- پیاده سازی آزمایشگاهی QKD
- شبیه سازی الگوریتم گراور
- شبیه سازی الگوریتم شور
- پیاده سازی الگوریتم گراور
- پیاده سازی الگوریتم شور