کارگاه W1-QKE

کامپیوتر کوانتومی و توزیع کلید کوانتومی

فهیمه سالاری سه دران، محمد صادق طالعی، حسین گرجی زاده و ابوالفضل ابراهیمی

دانشگاه صنعتی شریف، مرکز کوانتوم شریف

چکیده

از ابتدای تاریخ، مخابره اطلاعات حساس همراه با حفظ محرمانگی با چالش مواجه بوده است. تلاش برای شکستن رمز و دسترسی به اطلاعات محرمانه تاثیر فراوانی بر روی سرنوشت تاریخ به خصوص در جنگ‌های جهانی داشته است. امروزه رمزنگاری با زندگی روزمره انسان‌ها گره خورده و امنیت الگوریتم‌های رمزنگاری نقش مهمی در زندگی جوامع دارد. الگوریتم‌های رمزنگاری حال حاضر عموما بر پایه حل مسائل سخت ریاضی که با کامپیوترهای کلاسیک قابل حل نباشند استوار هستند. با ظهور ایده کامپیوترهای کوانتومی و افزایش قابل ملاحظه سرعت محاسبات، امنیت بسیاری از الگوریتم‌های رمزنگاری کلاسیک به مخاطره افتاده است، چرا که محدود بودن سرعت محاسبات در اثبات امنیت تمامی الگوریتم‌های کلاسیک جز مفروضات به حساب می‌آید. به طوری که در حال حاضر بسیاری به امید ساخت کامپیوتر کوانتومی در آینده در حال ذخیره‌سازی اطلاعات رمزگذاری شده هستند تا در زمان ساخته شدن کامپیوتر کوانتومی بتوانند به آن اطلاعات دست یابند.

دستیابی به مخابرات و ارتباطات امن یکی از نیازهای اساسی در جوامع بشری امروز است. پیشرفت سیستم‌های رمزنگاری باید از کامپیوترهای کوانتومی پیشی بگیرد، زیرا با تجاری شدن کامپیوترهای کوانتومی، سیستم‌های رمزنگاری کلاسیکی بلا استفاده می‌شوند. با پیشرفت فناوری کوانتومی و استفاده از منطق کوانتومی برای توزیع کلیدها، می‌توان از این تهدیدات جلوگیری نمود. به طور کلی، استفاده از رمزنگاری کوانتومی منجر به برقراری امنیت کامل در ارتباطات کوتاه برد و بلند برد خواهد گردید. در توزیع کلید کوانتومی از درجات آزادی مختلف نور مانند چارک‌های میدان، قطبش، فاز و ... می‌توان استفاده کرد. در این ارائه ضمن معرفی اصول کار پروتکل‌های توزیع کلید کوانتومی، به بررسی مسیر پیشرفت پروتکل‌های مختلف از جمله پروتکل‌های توزیع کلید متغیر گسسته، متغیر پیوسته و دور برد خواهیم پرداخت.

در این ارائه در ابتدا به معرفی منطق کوانتومی و علت جهش سرعت در کامپیوترهای کوانتومی نسبت به کامپیوترهای کلاسیک می‌پردازیم. در ادامه با مرور مختصر تاریخچه رمزنگاری کلاسیک، به الگوریتم‌های کوانتومی که منجر به شکستن رمزهای کلاسیک می‌شوند اشاره خواهیم کرد. سپس به معرفی رمزنگاری کوانتومی و تفاوت آن با رمز نگاری کلاسیک و رمزنگاری پساکوانتومی خواهیم پرداخت. در انتهای ارائه نیز به دورنمای ساخت کامپیوترهای کوانتومی در جهان و افق‌های پیش رو در این حوزه اشاره خواهد شد.

دستاوردهای علمی و عملی شرکت کنندگان

- آشنایی با مکانیک کوانتومی
- آشنایی با اهمیت توزیع کلید کوانتومی و نحوه به اشتراک‌گذاری کلید کوانتومی
- آشنایی با برخی از پروتکل‌های توزیع کلید کوانتومی
- آشنایی با کامپیوترهای کوانتومی

- آشنایی با الگوریتم‌های کوانتومی و نقش آن‌ها در شکستن رمزهای کلاسیک
- آشنایی با وضعیت کنونی ساخت و سخت‌افزار کامپیوترهای کوانتومی و چشم‌انداز آینده

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی با مفاهیم اولیه رمزنگاری

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	- توزیع کلیدکوانتومی راه حلی برای افزایش امنیت سیستم‌های رمزنگاری - مقدمات کوانتومی توزیع کلید کوانتومی - مروری بر تاریخ پیشرفت توزیع کلید کوانتومی - بررسی پروتکل‌های مهم متغیر گسسته و پیاده‌سازی‌های مهم آنها	۴۰ دقیقه
۲	- بررسی پروتکل‌های مهم متغیر پیوسته و پیاده‌سازی‌های مهم آنها - وضعیت فعلی جهان در توزیع کلید کوانتومی - جمع‌بندی	۴۰ دقیقه
۳	الگوریتم‌های کوانتومی	۶۰ دقیقه
۴	معرفی سخت‌افزار کامپیوترهای کوانتومی	۴۰ دقیقه

بیوگرافی ارائه دهندگان

فهیمه سالاری سه دران

- فارغ التحصیل دکترای فیزیک، دانشگاه صنعتی شریف
- دانشگاه صنعتی شریف، مرکز کوانتوم شریف، پژوهشگر

محمد صادق طالعی

- دانشجوی دکترای فیزیک، دانشگاه صنعتی شریف
- دانشگاه صنعتی شریف، مرکز کوانتوم شریف، پژوهشگر

حسین گرجی زاده

- فارغ التحصیل دکترای فیزیک، دانشگاه شهید باهنر کرمان
- دانشگاه صنعتی شریف، مرکز کوانتوم شریف، پژوهشگر پسادکترا

ابولفضل ابراهیمی

- دانشجوی دکترای فیزیک، دانشگاه صنعتی شریف
- دانشگاه صنعتی شریف، مرکز کوانتوم شریف، پژوهشگر

پیوست تکمیلی: دارد.

کارگاه W2-Fo-Android

جرم یابی اندروید

قادر ابراهیم پور، زهرا آخودداد و محمدرضا دارابی

پژوهشگاه توسعه فناوری‌های پیشرفته، پژوهشکده افتا

چکیده

امروزه با پیشرفت روزافزون تکنولوژی در حوزه تلفن‌های همراه، بررسی امنیتی این دستگاه‌ها نیز از اهمیت ویژه‌ای برخوردار است. از این روی شاخه‌ای از علم جرم‌یابی دیجیتال که مربوط به جرم‌یابی تلفن‌های همراه است رونق پیدا کرده است. جرم‌یابی دیجیتال مبتنی بر سیستم عامل اندروید یکی از شاخه‌های اصلی جرم‌یابی دیجیتال در دستگاه‌های تلفن همراه است، به این دلیل که سیستم عامل اندروید یک سیستم عامل پرطرفدار در بازار فروش تلفن‌های همراه است. بررسی راهکارها و روش‌های اجرای فرآیندهای جرم‌یابی دیجیتال در این حوزه اهمیت به‌سزایی دارد. در این کارگاه به بررسی علمی و عملی این فرآیندها مبتنی بر به‌روزترین رویکردهای حال حاضر پرداخته می‌شود.

دستاوردهای علمی و عملی شرکت کنندگان

- آشناایی با مفاهیم پیشرفته جرم‌یابی سیستم عامل اندروید
- آشنایی با ابزارهای تخصصی در حوزه جرم‌یابی اندروید

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی با مفاهیم اولیه جرم‌یابی دیجیتال
- آشنایی ابتدایی با سیستم عامل اندروید

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مفاهیم اولیه جرم‌یابی اندروید	۳۰ دقیقه
۲	آشنایی با ساختار سیستم عامل اندروید	۶۰ دقیقه
۳	ابزارهای تخصصی در حوزه تحلیل سیستم عامل اندروید (یوفد، اکسیژن و غیره)	۶۰ دقیقه
۴	مفاهیم پیشرفته در تحلیل سیستم عامل اندروید	۶۰ دقیقه
۵	جمع‌بندی	۳۰ دقیقه

بیوگرافی ارائه دهندگان

قادر ابراهیم پور

- فارغ التحصیل دکترا امنیت اطلاعات دانشگاه تهران، سازمان مدیریت صنعتی تهران۱۳۹۵
- پژوهشگاه توسعه فناوری‌های پیشرفته، پژوهشکده افتا، مدیر گروه امنیت زیرساخت از ۱۳۹۹

زهرا آخودداد

- فارغ التحصیل کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار دانشگاه صنعتی شریف، ۱۳۸۹
- پژوهشگاه توسعه فناوری‌های پیشرفته، رییس پژوهشکده افتا

محمدرضا دارابی

- فارغ التحصیل کارشناسی مهندسی کامپیوتر- نرم‌افزار دانشگاه خواجه نصیرالدین توسی، ۱۴۰۰
- پژوهشگاه توسعه فناوری‌های پیشرفته، پژوهشکده افتا، پژوهشگر از ۱۳۹۹

پیوست تکمیلی: دارد.

کارگاه W3-GRC

حکمرانی، ریسک و انطباق

علیرضا قهرود و مر ضیه بهرامی

شرکت کمان امن دیاکو

چکیده

به دلیل پیچیدگی روزافزون محیط‌های کسب وکار و الزامات قانونی، سازمان‌ها نیازمند رویکردی جامع برای مدیریت ریسک‌ها، بهبود حکمرانی و انطباق با استانداردها و الزامات بالادستی هستند. GRC-Governance Risk and Compliance چارچوبی است که به سازمان‌ها امکان می‌دهد این سه حوزه را به‌صورت یکپارچه مدیریت کنند، ریسک‌های امنیت سایبری را کاهش دهند، و شفافیت و کارآمدی تصمیم‌گیری‌ها را بهبود بخشند. عدم پیاده‌سازی صحیح GRC می‌تواند به ضعف حکمرانی، افزایش ریسک‌های غیرقابل کنترل و نقض الزامات قانونی منجر شود. در این کارگاه، اصول و چارچوب های GRC، نقش آن در مدیریت ریسک، تقویت حکمرانی و انطباق با مقررات بررسی می‌شود.

دستاوردهای علمی و عملی شرکت کنندگان

- آشنایی با مفاهیم کلیدی GRC
- نحوه استفاده از این چارچوب برای مدیر یت مؤثر ریسک ها و انطباق با استانداردهای بین المللی
- پیاده سازی موثر GRC در سازمان‌ها

پیش نیازها و ملزومات شرکت کنندگان

- تخصص در حوزه کلان امنیت و فناوری های وابسته (ترجیحاً شاغلین این حوزه)

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مقدمه ای برای معرفی مفاهیم GRC	۳۰ دقیقه
۲	تشریح کامل هر یک از اجزای چارچوب GRC	۳۰ دقیقه
۳	پیاده سازی صحیح GRC در سناریو ۱	۳۰ دقیقه
۴	پیاده سازی صحیح GRC در سناریو ۲	۳۰ دقیقه

بیوگرافی ارائه دهندگان

علیرضا قهرود

- فارغ التحصیل کارشناسی ارشد مدیریت تجارت الکترونیک، سازمان مدیریت صنعتی تهران
- مدیر دپارتمان راهکارهای امنیت سایبری، شرکت کمان امن دیاکو

مرضیه بهرامی

- دکترای کامپیوتر گرایش نرم افزار آزاد اسالمی واحد قزوین – ایران
- مدیر پروژه، شرکت کمان امن دیاکو

پیوست تکمیلی: دارد.

کارگاه W4-Risk-Asses

اندازه‌گیری ریسک امنیت سایبری به روش کمی: تبدیل داده‌ها به تصمیمات عملی

الناز عبادی و سعید کاظمی

شرکت تپسی

چکیده

در عصر افزایش تهدیدات سایبری و حملات پیچیده، رویکردهای سنتی ارزیابی ریسک کیفی اغلب عملکرد ضعیفی نشان می‌دهند. درجدیدترین مقالات و تحقیقات حوزه ارزیابی ریسک مشخص شده است که خطاهای شناختی و کمبودهای ذاتی مدل‌های ارزیابی ریسک کیفی، منجر به عملکرد کاملا غلط آن‌ها می‌شوند. این کارگاه به روش‌های کمی پیشرفته می‌پردازد که ارزیابی ریسک امنیت سایبری را از یک هنر به یک علم تبدیل می‌کند. شرکت‌کنندگان با تکنیک‌های پیشرفته‌ای برای اندازه‌گیری و کمی‌سازی ریسک سایبری، آشنا خواهند شد و همچنین ضعف‌ها و کمبودهای مدل‌های کیفی که سالیان سال است در همه سازمان‌ها به کار می‌رود را خواهد شناخت.

از طریق جلسات تعاملی و تمرین‌های عملی، شرکت کنندگان یاد می‌گیرند که:

- تهدیدات انتزاعی سایبری را به معیارهای مالی ملموس ترجمه کنند.
- از مدل‌های احتمالی برای ارزیابی و اولویت بندی ریسک‌ها استفاده کنند.
- از تکنیک‌های اندازه گیری پیشرفته برای عوامل امنیتی به ظاهر غیرقابل اندازه گیری استفاده کنند.
- استراتژی‌های داده محور برای تخصیص منابع و کاهش ریسک را توسعه دهند.

این کارگاه شکاف بین امنیت سایبری و تصمیم‌گیری برای مدیران ارشد و میانی امنیت را پر می‌کند و شرکت‌کنندگان را با ابزارهایی برای برقراری ارتباط موثر ریسک با ذینفعان و هدایت سرمایه‌گذاری‌های امنیتی آگاهانه مجهز می‌کند. شرکت کنندگان چه یک CISO، مدیر ریسک، یا متخصص امنیت باشند، بینش‌های ارزشمندی برای ارتقای شیوه‌های ارزیابی ریسک سازمان خود و همسو کردن تلاش‌های امنیتی با اهداف کسب و کار به دست خواهند آورد.

دستاوردهای علمی و عملی شرکت کنندگان

- آشنایی با روش‌های ارزیابی ریسک کمی
- تقویت مهارت تصمیم گیری برای مدیران امنیت
- تکنیک‌های اندازه گیری ریسک امنیتی
- توسعه استراتژی داده محور

پیش نیازها و ملزومات شرکت کنندگان

شرکت برای عموم آزاد است ولی دانش ابتدایی آمار و احتمالات به برداشت دقیق و علمی از مفاهیم کارگاه کمک خواهد کرد. البته مخاطب اصلی این کارگاه کارشناسان، مدیران میانی و ارشد امنیت اطلاعات در سازمان‌ها هستند.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	کمبودها و علل ناکارآمدی متدهای ارزیابی ریسک کیفی	۳۰ دقیقه
۲	مقدمه ای بر روش‌های ارزیابی ریسک کمی	۳۰ دقیقه
۳	روش‌های جمع آوری و آنالیز داده ها	۳۰ دقیقه
۴	بررسی case study	۳۰ دقیقه

بیوگرافی ارائه دهندگان

الناز عبادی

- فارغ التحصیل کارشناسی ارشد مهندسی برق - مخابرات، دانشگاه تهران، ۱۴۰۰
- کارشناس نرم افزار و متخصص امنیت اطلاعات – شرکت تپسی از ۱۴۰۰

سعید کاظمی

- فارغ التحصیل دکترای مدیریت بازرگانی، موسسه مدیریت صنعتی ایران، ۱۳۹۷
- مدیر امنیت – شرکت تپسی از ۱۴۰۲

پیوست تکمیلی: دارد.

کارگاه W5-Econ-Eval

کمی سازی ابعاد اقتصادی زیان حملات سایبری در سیستم‌های سایبرفیزیکی مبتنی بر الگوی فعالیت کسب و کار

محمدرضا جمالی

شرکت مهندسی نبض افزار

چکیده

هزینه مناسب بین امنیت و زیان ناشی از حملات سایبری در سیستم‌های سایبرفیزیکی از مسایل چالش بر انگیز در سال‌های اخیر است که فعالیت‌های تحقیقاتی زیادی در این زمینه صورت گرفته است. توجه شود که با توسعه دیجیتالی سیستم‌ها و اتصال سیستم‌های مختلف با یکدیگر و با توجه به اثر سلسله وار، حمله به یک سیستم می‌تواند باعث اختلال در سیستم‌های دیگر و در نتیجه فرآیندهای اجتماعی و سایبر فیزیکی شود که محاسبه زیان‌های اقتصادی حمله را با توجه به انتشار آن پیچیده تر می‌کند. این پیچیدگی و عدم امکان محاسبه مناسب ریسک و زیان عملیاتی باعث می‌شود که طراحی درستی در توافق نامه‌های سطح خدمات صورت نگیرد و نه تنها اندازه گیری ابعاد ریسک، بلکه مشخص کردن ابعاد اقتصادی و ایجاد بازی مناسب بین ارایه دهندگان خدمت و دریافت کنندگان خدمت در گراف‌های خدمت وجود ندارد. عدم امکان ارزیابی مناسب از زیان حمله باعث اتلاف منابع و یا عدم اختصاص منابع لازم برای برقراری امنیت می‌شود.

شرکت نبض افزار رایان اندیش با شناسایی، مدلسازی، شبیه سازی و همچنین بازسازی الگوی فعالیت کسب و کار با استفاده از روش‌های آماری، تحلیل دادگان بزرگ و همچنین پردازش هوشمند داده ها، نرم افزارها و داشبوردهایی دقیق در مقیاس بزرگ تولید کرده است که با اندازه گیری شاخص‌های اساسی سنجش کیفیت مانند دسترس پذیری، قابلیت اعتماد و دسترسی پذیری حس شده می‌تواند میزان زیان ناشی از حمله‌های سایبری در سیستم‌های سایبرفیزیکی را با کمترین میزان هشدار اشتباه و هشدار از دست رفته محاسبه کند.

در این کارگاه تجربیات و نتایج حاصل از فعالیت‌های موفق شرکت نبض افزار در طی ۱۷ سال فعالیت تحقیق و توسعه، تهیه بیش از ۲۰۰۰ گزارش و انجام بیش از ۱۵۰ قرارداد و بیش از ۲۰ مقاله علمی و تحقیقاتی در سطح ملی و جهانی، در اندازه گیری اخلال‌های ناشی از حملات سایبری و همچنین اختلالات تداوم عملیات در حوزه‌های سایبرفیزیکی مانند دوربین‌های نظارت شهری، شرکت‌های پرداخت، بانک ها، خدمات بهداشتی ارایه شده است. همچنین زیان مالی با توجه به ارزش کسب و کار محاسبه شده است و روش‌های مناسب طراحی توافق نامه سطح خدمات در این فعالیت‌ها ارایه شده است. نتایج حاصله می‌تواند در حوزه‌های مختلف دیگر به کار گرفته شود و باعث کاهش زیان و ریسک عملیاتی شرکت ها، سازمان‌ها و بهبود کیفیت ارایه خدمات مختلف شود.

دستاوردهای علمی و عملی شرکت کنندگان

- آشنایی با روش بدست آوردن الگوی کسب و کار در سیستم‌های سایبری و سایبرفیزیکی
- آشنایی با شاخص‌های اساسی سنجش کیفیت و روش سنجش کیفیت سیستم‌های سایبری
- آشنایی با ریسک و زیان عملیاتی و چگونگی محاسبه آن برای حملات سایبری
- آشنایی با توافق نامه سطح خدمات و چگونگی اندازه گیری آن

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی با آمار و احتمالات
- آشنایی با پردازش سیگنال دیجیتال

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	سیستم‌های سایبرفیزیکی و صنعت ۴,۰	۴۵ دقیقه
۲	ریسک عملیاتی در سیستم‌های سایبرفیزیکی	۳۰ دقیقه
۳	الگوی فعالیت کسب و کار	۳۰ دقیقه
۴	شاخص‌های اساسی سنجش کیفیت	۳۰ دقیقه
۵	توافق نامه سطح خدمات	۴۵ دقیقه
۶	نمونه فعالیت‌های صورت گرفته	۴۵ دقیقه
۷	مقالات و فعالیت‌های تحقیقاتی صورت گرفته و چشم انداز تحقیقاتی مسیر	۱ ساعت
۸	سیستم‌های سایبرفیزیکی و تبدیل(تحول) دیجیتال	۳۰ دقیقه

بیوگرافی ارائه دهنده

محمدرضا جمالی

- فارغ التحصیل دکترای هوش مصنوعی و رباتیک، دانشگاه تهران، ۱۳۹۰
- مدیرعامل شرکت نبض افزار، ۱۲ سال

پیوست تکمیلی: دارد.

کارگاه W6-QI

ارتباطات امن کوانتومی: از شبکه‌های توزیع کلید کوانتومی تا اینترنت جهانی کوانتومی

سارا توفیقی

پژوهشگاه ارتباطات و فناوری اطلاعات

چکیده

امروزه در میانه انقلاب دوم کوانتومی، شاهد ظهور کامپیوترهای کوانتومی هستیم. کامپیوترهای کوانتومی با سرعت پردازش بسیار بالا و ورای ابرکامپیوترهای کلاسیکی، باعث سریعتر شدن حل محاسبات پیچیده ریاضی می‌شوند. محاسبات کوانتومی علاوه بر اینکه فرصت پردازش داده‌های عظیم را فراهم می‌کند، امنیت ارتباطات کلاسیک را نیز به خطر می‌اندازد. فناوری ارتباطات کوانتومی بر مبنای اصول موضوعه مکانیک کوانتومی، راه حلی برای ایجاد مخابرات کاملاً امن ارائه داده است. در این کارگاه، پس از معرفی مبانی مکانیک کوانتومی و تبیین ضرورت ارتباطات کوانتومی، اصول کار ارتباطات کوانتومی و زیرشاخه‌های آن تشریح می‌شود. هدف نهایی در ارتباطات کوانتومی ایجاد اینترنت کوانتومی است که در آن رایانه‌های کوانتومی از طریق شبکه ارتباطات کوانتومی به یکدیگر متصل می‌شوند. اولین گام در دستیابی به اینترنت کوانتومی ایجاد شبکه توزیع کلید کوانتومی است. بخش انتهایی کارگاه به معرفی اصول کار شبکه توزیع کلید کوانتومی و اینترنت کوانتومی اختصاص دارد.

دستاوردهای علمی و عملی شرکت کنندگان

- آشنایی با اصول کار فناوری نوظهور ارتباطات کوانتومی

پیش نیازها و ملزومات شرکت کنندگان

- شرکت برای عموم آزاد است.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مبانی مکانیک کوانتومی	۱۰ دقیقه
۲	تبیین ضرورت ارتباطات کوانتومی	۳۰ دقیقه
۳	معرفی ارتباطات کوانتومی و زیرشاخه‌های آن	۳۰ دقیقه
۴	معرفی اصول کار شبکه‌های توزیع کلید کوانتومی	۳۰ دقیقه
۵	معرفی اصول کار اینترنت کوانتومی	۲۰ دقیقه

بیوگرافی ارائه دهندگان

سارا توفیقی

- فارغ التحصیل دکترای فیزیک – گرایش فوتونیک و اپتیک، دانشگاه صنعتی شریف ۱۳۹۴
- مدیر پروژه – پژوهشگاه فناوری ارتباطات و اطلاعات از ۱۴۰۲

پیوست تکمیلی: دارد.

کارگاه W7-Cipher-Eval

تحلیل رمز الگوریتم‌های متقارن سبک وزن به کمک یادگیری ماشین

صادق صادقی

پژوهشگاه توسعه فناوری‌های پیشرفته

چکیده

در عصر گسترش روزافزون اینترنت اشیاء (IoT) و دستگاه‌های کم‌مصرف، الگوریتم‌های رمزنگاری سبک وزن به دلیل کارایی بالا و مصرف کم منابع، اهمیت ویژه‌ای پیدا کرده‌اند. در همین راستا، پیشرفت‌های چشمگیر در حوزه هوش مصنوعی و به‌ویژه یادگیری عمیق، فرصت‌های جدیدی را برای تحلیل و بهبود این الگوریتم‌ها فراهم کرده است. کارگاه پیشنهادی به بررسی نقش یادگیری عمیق در شناسایی و رفع نقاط ضعف امنیتی رمزهای متقارن سبک وزن می‌پردازد. اهداف اصلی کارگاه شامل معرفی رمزهای سبک وزن، معرفی حمله‌های مطرح در این زمینه، توضیح مبانی یادگیری عمیق، تحلیل و بهبود امنیت رمزهای متقارن با استفاده از تکنیک‌های یادگیری عمیق، و ارائه مطالعات موردی و تجربیات عملی است. این کارگاه با ارائه مفاهیم نوین و کاربردهای آن، می‌تواند نقش مؤثری در افزایش آگاهی و توانمندی پژوهشگران و علاقه‌مندان در این زمینه ایفا کند.

دستاوردهای علمی و عملی شرکت کنندگان

- آشنایی با مفاهیم اولیه و پایه الگوریتم‌های رمزنگاری سبک وزن
- آشنایی با مبانی اولیه یادگیری عمیق
- تحلیل امنیتی الگوریتم‌های رمزنگاری سبک وزن و شناسایی نقاط ضعف امنیتی با استفاده از تکنیک‌های یادگیری عمیق
- بررسی و تحلیل مطالعات موردی در استفاده از یادگیری عمیق برای تحلیل رمزهای سبک وزن
- بررسی و آشنایی با حملات مطرح علیه الگوریتم‌های رمزنگاری سبک وزن

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی با مبانی رمزنگاری
- دانش پایه‌ای در زمینه الگوریتم‌های رمزنگاری، به‌ویژه رمزنگاری متقارن.
- آشنایی با مفاهیم اولیه امنیت اطلاعات

داشتن دانش در موارد زیر می‌تواند به درک بهتر مفاهیم کمک کند ولی در صورت آشنا نبودن سعی بر این است تا در کارگاه دید اولیه نسبت به مسائل زیر داده شود:

- ❖ آشنایی با مبانی یادگیری ماشین و یادگیری عمیق:
  - درک اولیه از اصول یادگیری ماشین و یادگیری عمیق
  - آشنایی با مفاهیم شبکه‌های عصبی مصنوعی
- ❖ تجربه برنامه‌نویسی:
  - تجربه برنامه‌نویسی در یکی از زبان‌های برنامه‌نویسی مورد استفاده در یادگیری ماشین (مانند پایتون)

- **قابلیت استفاده برای عموم:** کارگاه به‌طور عمومی قابل استفاده برای عموم علاقه‌مندان به حوزه‌های رمزنگاری و یادگیری ماشین است. با این حال، شرکت‌کنندگانی که دارای پیش‌نیازهای فوق باشند، بهره‌وری بیشتری از مطالب کارگاه خواهند داشت. به‌منظور اطمینان از بهرمندی بهتر شرکت‌کنندگان، توصیه می‌شود قبل از حضور در کارگاه، مبانی ذکر شده را مطالعه و مرور نمایند.
- این موارد به شرکت‌کنندگان کمک می‌کند تا بتوانند به‌صورت مؤثرتری در کارگاه شرکت کرده و از محتوای آموزشی آن بهره‌مند شوند.

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	آشنایی با رمزهای متقارن سبک وزن	یک ساعت
۲	آشنایی با حمله‌های مطرح در زمینه رمزنگاری سبک	یک ساعت
۳	مبانی یادگیری ماشین و یادگیری عمیق	یک ساعت و نیم
۴	استفاده از یادگیری عمیق در تحلیل رمزهای متقارن سبک وزن	دو ساعت
۵	پرسش و پاسخ و جمع‌بندی	نیم ساعت

بیوگرافی ارائه دهندگان

صادق صادقی

- فارغ التحصیل دکترای مهندسی برق- مخابرات امن، دانشگاه صنعتی شریف ۱۳۹۹
- عضو هیات علمی دانشگاه تحصیلات تکمیلی علوم پایه زنجان، دانشکده ریاضی

مرضیه وحید دستجردی

- فارغ التحصیل دکترای ریاضیات- نظریه گراف- مخابرات امن، دانشگاه صنعتی اصفهان ۱۳۹۹
- پژوهشگاه توسعه فناوری‌های پیشرفته، عضو هیات علمی از ۱۴۰۰

ایمان میرزاعلی

- فارغ التحصیل کارشناسی ارشد مهندسی برق- مخابرات امن، دانشگاه تربیت دبیر شهید رجایی ۱۴۰۳
- پژوهشگاه توسعه فناوری‌های پیشرفته، پژوهشگر از ۱۴۰۲

پیوست تکمیلی: دارد.

کارگاه W8-PostQ

رمزنگاری پساکوانتومی

محمود سلماسی زاده*، ترانه اقلیدس*، معصومه کوچک شوشتری* و راضیه سالاری فرد**

دانشگاه صنعتی شریف، پژوهشکده الکترونیک*

دانشگاه شهید بهشتی، دانشکده مهندسی و علوم کامپیوتر**

چکیده

ظهور کامپیوترهای کوانتومی در مقیاس بزرگ تهدیدی جدی برای زیرساخت امنیتی فعلی اطلاعات به ویژه در بخش اعتمادسازی در جهان است. رمزنگاری کلید عمومی از جمله RSA و رمزنگاری مبتنی بر خم‌های بیضوی و پروتکل‌های امضای دیجیتال، که امروزه به‌طور گسترده‌ای در اینترنت و انواع سامانه‌ها استفاده می‌شود، به مسائل سخت ریاضی وابسته هستند که به‌راحتی توسط یک کامپیوتر کوانتومی در مقیاس بزرگ شکسته خواهند شد. در این کارگاه آموزشی قصد داریم به معرفی الگوریتم‌ها و استانداردهای رمزنگاری بپردازیم که در برابر حملات کوانتومی مقاوم هستند و جنبه‌های امنیتی و کارآیی آنها را بررسی نماییم.

دستاوردهای علمی و عملی شرکت کنندگان

- آشنایی با پیشرفت‌های اخیر در زمینه رمزنگاری پساکوانتومی

پیش نیازها و ملزومات شرکت کنندگان

- آشنایی با مفاهیم اولیه رمزنگاری و امنیت

سرفصل مطالب کارگاه

ردیف	سرفصل	زمان
۱	مقدمه‌ای بر رمزنگاری پساکوانتومی	۹۰ دقیقه
۲	رمزنگاری مشبکه مبنا و طرح‌های رمزنگاری مشبکه مبنای فراخوان NIST	۹۰ دقیقه
۳	پیاده‌سازی نرم‌افزاری-سخت‌افزاری الگوریتم‌های رمزنگاری پساکوانتومی NIST	۹۰ دقیقه
۴	رمزنگاری کدمبنا و طرح‌های رمزنگاری کدمبنای فراخوان NIST	۹۰ دقیقه

بیوگرافی ارائه دهندگان

حسین پیلارام

- فارغ التحصیل دکترای مخابرات امن، دانشگاه صنعتی شریف
- دانشیار پژوهشکده الکترونیک، دانشگاه صنعتی شریف

ترانه اقلیدس

- فارغ التحصیل دکترای ریاضی – دانشگاه گیسن، آلمان
- دانشیار پژوهشکده الکترونیک، دانشگاه صنعتی شریف

معصومه کوچک شوشتری

- فارغ التحصیل دکترای مهندسی برق-مخابرات، دانشگاه صنعتی خواجه نصیرالدین توسی
- عضو هیات علمی پژوهشکده الکترونیک، دانشگاه صنعتی شریف

راضیه سالاری فرد

- فارغ التحصیل دکترای مهندسی کامپیوتر، دانشگاه صنعتی شریف
- عضو هیات علمی دانشکده مهندسی و علوم کامپیوتر، دانشگاه شهید بهشتی

پیوست تکمیلی: دارد.