

چهارشنبه ۲۵ مهرماه ۱۴۰۳ (۱۶ اکتبر ۲۰۲۴)

محل نشست	پایان	شروع	مستوف نشست	جزئیات نشست	عنوان نشست	ردیف
سالن اصلی (شهید اتابکی)	۹:۴۵	۸:۴۵		سرود ملی و تلاوت قرآن کریم خوش آمدگویی رئیس کنفرانس (دکتر سجاد ازگلی) سخنرانی معاون پژوهشی دانشگاه تربیت مدرس (دکتر محمد جوان) سخنرانی رئیس پژوهشکده امنیت پژوهشگاه ارتباطات و فناوری اطلاعات (دکتر رضا کلانتری) گزارش دبیر علمی و اعلام برنامه کنفرانس (دکتر مهدی آبادی)	مراسم افتتاحیه	۱
	۱۰:۳۰	۹:۴۵	دکتر محسن رمضان یارزندی	سخنران کلیدی: دکتر رسول جلیلی، هیأت علمی دانشگاه صنعتی شریف و عضو شورای عالی فضای مجازی تقاعد چالش‌های امنیت سایبری کشور با برنامه هفتم پیشرفت	سخنرانی کلیدی ۱	۲
	۱۱:۱۵	۱۰:۳۰		پذیرایی و بازدید از نمایشگاه		
سالن اصلی (شهید اتابکی)	۱۲:۰۰	۱۱:۱۵	دکتر محمدحسام تدین	<b>Keynote Speaker: Dr. Reza Shokri, National University of Singapore (NUS), Singapore</b> <b>Memorization in Machine Learning</b>	سخنرانی کلیدی ۲	۳
	۱۳:۳۰	۱۲:۰۰		نماز و ناهار		

چهارشنبه ۲۵ مهرماه ۱۴۰۳ (۱۶ اکتبر ۲۰۲۴)

محل نشست	پایان	شروع	مسئول نشست	جزئیات نشست	عنوان نشست	ردیف
H1 سالن	۱۵:۳۰	۱۳:۳۰	دکتر ترانه اقلیدس و دکتر محمدرضا هوشمند اصل	سخنران مدعو: دکتر نرجس محسنی فر، دانشگاه آزاد اسلامی، واحد شهرکرد ساخت ابتکاری ماتریس‌های MDS با استفاده از ماتریس‌های کوشی تعمیم‌یافته	نشست ۱ - مبانی رمزشناسی	۴
				Farnoosh Hamednejad, Javad Mohajeri, and Mohammad Reza Aref <b>Attacking Two Pairing-free Ciphertext-policy Attribute-based Encryption Schemes</b>		
				Atiyeh Mirzaie, Siavash Ahmadi, and Mohammad Reza Aref <b>Division Property-based Integral Attack on Reduced-round SAND-128</b>		
				Masroor Hajari, Mahmoud Salmasizadeh, Javad Mohajeri, Siavash Ahmadi, et al. <b>Impossible Differential Cryptanalysis of Reduced-round mCrypton-64</b>		
H2 سالن	۱۵:۳۰	۱۳:۳۰	دکتر فاطمه دلدار و دکتر حسین قرایی	سخنران مدعو: دکتر علی احمدیان رمکی، فارغ‌التحصیل دکتری، دانشگاه فردوسی مشهد حملات APT: مرز دانش، چالش‌ها و راه‌کار تشخیص مؤثر	نشست ۲ - امنیت شبکه	۵
				فاطمه پیش داد و رضا ابراهیمی آتانی پیشگیری و تشخیص حملات بات‌نت در اینترنت اشیا با استفاده از روش‌های یادگیری ترکیبی		
				Hossein Shadabfar, Moteharez Dehghan, and Babak Sadeghian <b>DSRL-APT-2023: A New Synthetic Dataset for Advanced Persistent Threats</b>		
				Amir Hossein Hadavi, Mohammad Mahdi Mojahedian, and Mohammad Reza Aref <b>Over-the-Air Federated Adaptive Data Analysis: Preserving Accuracy via Opportunistic Differential Privacy</b>		
				Mojtaba Shirinjani, Mojtaba Amiri, Amirhosein Salehi, Pouria Arefijamal, Rasoul Khazaei, et al. <b>Spotting and Mitigating DDoS Attacks Using Deep Learning for Online Traffic Analysis</b>		

چهارشنبه ۲۵ مهرماه ۱۴۰۳ (۱۶ اکتبر ۲۰۲۴)

محل نشست	پایان	شروع	مسئول نشست	جزئیات نشست	عنوان نشست	ردیف
سالن H3	۱۵:۳۰	۱۳:۳۰	دکتر رضا ابراهیمی آثانی و دکتر طلا تفضلی	سخنران مدعو: دکتر سعید بنائیان فر، پژوهشگر پسادکتری، دانشگاه یزد بررسی روش‌های ارائه امنیت و حفاظت از حریم خصوصی در بلاکچین‌های لایه سوم: چالش‌ها و افق‌های آینده	نشست ۳ - مدیریت امنیت و حریم خصوصی	۶
				ابوذر عرب سرخی و طلا تفضلی تحلیل موضوعات راهبردی در قلمرو مقررات حفاظت از داده‌های عمومی		
				فروش کریمی، بهروز ترک لادانی و بهروز شاه‌قلی قهفرخی هوشمندسازی اجرای سناریوهای تمرین در میدان سایبری با استفاده از روش‌های یادگیری ماشین		
				فاطمه غلامی سبزواری و معصومه صفحانی نقض خاصیت یکپارچگی در یک پروتکل حافظ حریم خصوصی انتها به انتها در سامانه‌های پایش سلامت مبتنی بر اینترنت اشیا		
				آرین عرب نوری، سهیل عیسی‌زاده و علیرضا شفیعی‌نژاد سامانه لاگ حسابرسی‌پذیر امن مبتنی بر زنجیره قالب		
	۱۶:۰۰	۱۵:۳۰		پذیرایی و بازدید از نمایشگاه		
سالن اصلی (شهید اتابکی)	۱۷:۳۰	۱۶:۰۰	دکتر محمدحسام تدین	نشست تخصصی: چالش ظرفیت‌سازی و تربیت نیروی انسانی امنیت سایبری با حضور ذینفعان کلیدی از دستگاه‌های اجرایی، سازمان‌ها و شرکت‌های مرتبط	نشست تخصصی	۷

## پنجشنبه ۲۶ مهرماه ۱۴۰۳ (۱۷ اکتبر ۲۰۲۴)

محل نشست	پایان	شروع	مسئول نشست	جزئیات نشست	عنوان نشست	ردیف
سالن H1	۱۰:۰۰	۸:۰۰	دکتر علی جهانیان و دکتر هادی سلیمانی	سخنران مدعو: دکتر نوید وفائی، پژوهشگر، پژوهشکده فضای مجازی دانشگاه شهید بهشتی رونمایی از حملات خطا: رویکردی آماری بر آسیب‌پذیری‌های رمزنگاری	نشست ۴ - پیاده‌سازی الگوریتم‌های رمزنگاری و حملات مرتبط	۱
				Hossein Naderi Varandi and Raziye Salarifard <b>A Lightweight General Modular Multiplier for Kyber PQC</b>		
				Narges Mokhtari, Navid Vafaei, Sadegh Sadeghi, and Nasour Bagheri <b>Differential Fault Analysis of the BIPBIP Block Cipher</b>		
				کیوان خورمهر، جواد علیزاده و محسن جهانبانی بررسی حمله تحلیل توان روی رمز قالبی SPEEDY و مقاوم‌سازی آن با استفاده از روش نقاب‌گذاری مبتنی بر دامنه (DOM)		
				عماد محمدزاده وطن‌چی، محبوبه هوشمند و منیره هوشمند بهبود هزینه ارتباطات برای محاسبات امن کوانتومی توزیع شده چندبخشی با استفاده از الگوریتم نهنگ کوانتومی		

پنجشنبه ۲۶ مهرماه ۱۴۰۳ (۱۷ اکتبر ۲۰۲۴)

محل نشست	پایان	شروع	مسئول نشست	جزئیات نشست	عنوان نشست	ردیف
سالن H2	۱۰:۰۰	۸:۰۰	دکتر بهروز ترک لادانی، دکتر حسین همایی و دکتر مرجان گودرزی	سخنران مدعو: دکتر محمدعلی جمشیدی، استادیار دانشگاه صنعتی خواجه نصیرالدین طوسی آموزش ماشین با داده‌های محرمانه: آخرین دستاوردها در حفظ حریم خصوصی و تحلیل داده از دور	نشست ۵ - هوش مصنوعی در رمزنگاری و امنیت سایبری	۲
				سخنران مدعو: دکتر فاطمه دلدار، استادیار دانشگاه صنعتی اصفهان یادگیری عمیق در تشخیص و طبقه‌بندی بدافزارهای روز صفر		
				Maryam Azadmanesh <b>A Fine-grained Hybrid Inversion-based Membership Inference Attack against GANs</b>		
				Elahe Farshadfar, Amir Mahdi Sadeghzadeh Mesgar, and Rasool Jalili <b>Divergent Twins Fencing: Protecting Deep Neural Networks Against Query-based Black-box Adversarial Attacks</b>		
سالن H3	۱۰:۰۰	۸:۰۰	دکتر ابودر عرب سرخی و مهندس هاشم حبیبی، دکتر محمدحسن مجیدی،	سخنران مدعو: مهندس سبحان علی‌آبادی راهبردهای مقابله با حملات و رخدادهای سایبری در سطح ملی	نشست ۶ - علم و صنعت افتا	۳
				Amirhosein Salehi, Siavash Ahmadi, and Mohammad Reza Aref <b>A Lightweight Online Intrusion Detection and Localization Framework for Industrial Control Systems</b>		
				مرتضی اسدی، محمدرضا زمانی و فاطمه زکیزاده پیااده‌سازی استاندارد احراز اصالت امن FIDO بر روی سرویس مدیریت منابع شبکه اکتیو دایرکتوری (مقاله علمی-صنعتی)		
				سمیه سلطانی، رسول رمضانیان، محمدرضا فاتحی‌نیا و هاشم حبیبی سیستم مدیریت رویدادها و اطلاعات امنیتی مبتنی بر هوش مصنوعی مولد (GAI-SIEM) (مقاله علمی-صنعتی)		

پنجشنبه ۲۶ مهرماه ۱۴۰۳ (۱۷ اکتبر ۲۰۲۴)

محل نشست	پایان	شروع	مسئول نشست	جزئیات نشست	عنوان نشست	ردیف
				رسول رمضانیان، وجیهه مبشری، محمدرضا فاتحی‌نیا، سمیه سلطانی و هاشم حبیبی دانا یار: همراه امن و هوشمند دولت و مدیران سازمان در تحلیل و تصمیم‌گیری مبتنی بر داده‌های سازمانی (مقاله علمی - صنعتی)		
	۱۰:۳۰	۱۰:۰۰		پذیرایی و بازدید از نمایشگاه		
سالن اصلی (شهید اتابکی)	۱۱:۱۵	۱۰:۳۰	دکتر ترانه اقلیدس	Keynote Speaker: Dr. Amin Sakzad, Monash University, Melbourne, Australia Lattice-based Optimization Techniques and Algorithms and Evaluations	سخنرانی کلیدی ۳ و ۴	۴
	۱۲:۰۰	۱۱:۱۵		سخنران کلیدی: دکتر منصور باقری، دانشگاه تربیت دبیر شهید رجایی Fault Attack on Symmetric Ciphers		۵
	۱۳:۳۰	۱۲:۰۰		نماز و ناهار		
سالن اصلی (شهید اتابکی)	۱۴:۱۵	۱۳:۳۰	دکتر صادق دری نوگرانی و دکتر هاله امین طوسی	Keynote Speaker: Dr. José L. Muñoz-Tapia, Universitat Politècnica de Catalunya, Barcelona, Spain Zero Knowledge Proofs in Blockchain	سخنرانی کلیدی ۵	۶
سالن اصلی (شهید اتابکی)	۱۵:۲۰	۱۴:۲۰	دکتر راضیه سالاری فرد و دکتر طلا تقضلی	Invited Speaker: Dr. Hanif Rahbari, Assistant Professor, Rochester Institute of Technology (RIT), New York, USA On the Requirements of Quantum-resistant Algorithms Beyond Cryptography (Case Study: Connected Vehicles)	نشست ۷ - سخنرانان مدعو	۷
				Invited Speaker: Dr. Simin Ghesmati, Researcher, SBA Research, Vienna, Austria Classification and Evaluation of Bitcoin Privacy Techniques		



پنجشنبه ۲۶ مهرماه ۱۴۰۳ (۱۷ اکتبر ۲۰۲۴)

محل نشست	پایان	شروع	مسئول نشست	جزئیات نشست	عنوان نشست	ردیف
سالن H1	۱۵:۵۰	۱۴:۲۰	مهندس جواد مهاجری و دکتر فرخ‌لقا معظمی	سخنران مدعو: دکتر مهدی مهدوی علیائی، فارغ‌التحصیل دکتری، دانشگاه شهید بهشتی مقدمه‌ای بر محاسبات روی داده‌های رمزنگاری شده	نشست ۸ - پروتکل‌های امنیتی	۸
				Mehrad Jaber, Hamid Mala, and Seyedeh Marzieh Sadat Madani <b>Cryptanalysis of Two Authenticated Key Agreement Protocols in Multi-server Environments</b>		
				قدسیه کریمی، مرتضی عادل و محمدعلی هادوی تحلیل امنیتی یک پروتکل سبک وزن انتقال مالکیت اشیا در سامانه‌های RFID		
				مهناز نوروزی و عطیه صادقی تحلیل امنیت یک طرح رمزگذاری قابل جستجوی احراز اصالت شده فاقد گواهی‌نامه		
سالن H3	۱۵:۵۰	۱۴:۲۰	دکتر سمانه مشهدی و دکتر شقایق نادری	Mohammad Amin Sarzaem, Seyed Reza Hoseini Najarkolaei, and Mohammad Reza Aref <b>Shapley-value for Federated Learning: A Distributed and Fair Framework</b>	نشست ۹ - پنهان‌سازی اطلاعات	۹
				Zahra Saeidi and Samaneh Mashhadi <b>A New Scheme based on (t,n)-Secret Image Sharing with Steganography based on Joseph's Problem and HLR</b>		
				Ebrahim Raeisian Dashtaki and Shahrokh Ghaemmaghani <b>A New Bit-wise Approach for Image-in-Audio Steganography Using Deep Learning</b>		
				سید حسام‌الدین هاشمی و محمدحسن مجیدی رمزنگاری تصویر IEPS: رمزنگاری بر مبنای نگاشت آشوبی PWLCM و تابع چکیده‌ساز SHA-512		
	۱۶:۲۰	۱۵:۵۰		پذیرایی و بازدید از نمایشگاه		

## پنجشنبه ۲۶ مهرماه ۱۴۰۳ (۱۷ اکتبر ۲۰۲۴)

محل نشست	پایان	شروع	مسئول نشست	جزئیات نشست	عنوان نشست	ردیف
سالن اصلی (شهید اتابکی)	۱۷:۴۵	۱۶:۲۰		سرود ملی و تلاوت قرآن کریم گزارش برگزاری کنفرانس توسط دبیر اجرایی (دکتر صادق دری نوگورانی) بیانیه پایانی و معرفی میزبان کنفرانس بیست و دوم سخنرانی ریاست محترم انجمن رمز ایران (دکتر محمدرضا عارف) اعلام برگزیدگان و تقدیر از تیم اجرایی توسط مسؤول محترم دبیرخانه دائمی کنفرانس (دکتر منصور باقری)	مراسم اختتامیه	۱۰