برنامه بیستمین کنفرانس بین‌المللی انجمن رمز ایران

روز اول – ۸ شهریور ۱۴۰۲

ردیف	عنوان برنامه	جزئیات برنامه	آغاز	پایان	محل برگزاری
۱		پذیرش	۸:۰۰	۸:۴۵	سالن ابوریحان
۲	مراسم آغازین	تلاوت قرآن، سرود ملی و کلیپ معرفی کنفرانس سخنرانی معاون محترم وزیر علوم، تحقیقات و فناوری و ریاست سازمان پژوهش‌های علمی و صنعتی ایران و رئیس کنفرانس (دکتر حسن زمانیان) سخنرانی دبیر محترم کنفرانس (دکتر شروین امیری)	۸:۴۵	۹:۱۵	سالن ابوریحان
۳	سخنرانی کلیدی ۱ مسئول: دکتر محمود سلماسی‌زاده	**واژه‌گزینی: چرائی، مبانی علمی، اصول و ضوابط، فرآیندها، تاریخچه، و گزارشی از اقدامات انجام‌شده در انجمن رمز ایران** دکتر جواد مهاجری، دانشگاه صنعتی شریف	۹:۱۵	۱۰:۱۵	
		استراحت، پذیرایی و بازدید از نمایشگاه	۱۰:۱۵	۱۰:۴۵	
۴	سخنرانی کلیدی ۲ مسئول نشست: مهندس حبیب رستمی	**هک رمزکننده صوتی راکال و کشف پیام‌های رمز دشمن در دفاع مقدس** مهندس کوروس حمزه، جهاد دانشگاهی صنعتی شریف	۱۰:۴۵	۱۱:۴۵	سالن ابوریحان
		نماز، ناهار و بازدید از نمایشگاه	۱۱:۴۵	۱۳:۳۰	
۵	سخنرانی کلیدی ۳ مسئول نشست: دکتر هادی سلیمانی	**Fast, Furious and Insecure: Passive Keyless Entry and Start Systems in Modern Supercars** Dr. Benedikt Gierlichs, KU Leuven, Belgium	۱۳:۳۰	۱۴:۲۰	سالن ابوریحان
۶		استراحت	۱۴:۲۰	۱۴:۳۰	

برنامه بیستمین کنفرانس بین‌المللی انجمن رمز ایران

روز اول – ۸ شهریور ۱۴۰۲

ردیف	عنوان برنامه	جزئیات برنامه	آغاز	پایان	محل برگزاری
۷	نشست S1 الگوریتم‌های رمزنگاری و نهان‌نگاری مسئول: دکتر شهرام خزایی، دکتر ترانه اقلیدس	جستجوی خودکار تمایزگرهای تفاضلی و تفاضل‌ناممکن رمزهای ARX سید آرش عظیمی، دانشگاه صنعتی شریف (سخنران مدعو ۱)	۱۴:۳۰	۱۵:۰۰	سالن ابوریحان
۸		Integral Cryptanalysis of Reduced-Round SAND-64 Based on Bit-Based Division Property عطیه میرزایی، سیاوش احمدی و محمدرضا عارف	۱۵:۰۰	۱۵:۲۰	
۹		New Directions in Design of Binary Matrices for SPN Block Ciphers سید مهدی سجادیه، آرش میرزایی	۱۵:۲۰	۱۵:۴۰	
۱۰		بررسی جامع کارایی روش نهان‌کاوی مبتنی بر یادگیری عمیق در کشف روش‌های حوزه مکان وجیهه ثابتی، مهدیه سمیعی	۱۵:۴۰	۱۶:۰۰	
۱۱					
۱۲	نشست S2 امنیت و سخت افزار مسئول: دکتر علی جهانیان، دکتر بیژن علیزاده	Unleashing the Shield: Empowering Hardware Security Through CAD Tools for Hardware Trojan Detection احمد شعبانی، دانشگاه تهران (سخنران مدعو ۲)	۱۴:۳۰	۱۵:۰۰	سالن ۱
۱۳		پیاده‌سازی کارای ضرب چندجمله‌ای‌های روی حلقه در الگوریتم رمزنگاری پساکوانتومی NTRU Prime برروی FPGA رضا رشیدیان، راضیه سالاری‌فرد، ریحانه خوارزمی، علی جهانیان	۱۵:۰۰	۱۵:۲۰	
۱۴		Cross-Device Deep Learning Based Side-Channel Attack Using the Filter and Autoencoder Functions مریم طبایی‌فرد، علی جهانیان	۱۵:۲۰	۱۵:۴۰	
۱۵		HyLock: Hybrid Logic Locking Based on Structural Fuzzing for Resisting Learning-Based Attacks محمد مرادی شاه‌میری، بیژن علیزاده	۱۵:۴۰	۱۶:۰۰	
۱۶		استراحت	۱۶:۰۰	۱۶:۳۰	

برنامه بیستمین کنفرانس بین‌المللی انجمن رمز ایران

روز اول – ۸ شهریور ۱۴۰۲

ردیف	عنوان برنامه	جزئیات برنامه	آغاز	پایان	محل برگزاری
۱۷	جایزه فناوری دکتر برنجکوب	گزارش رویداد (شرکت مهندسی پیام‌پرداز) ارائه شرکت فناور برتر	۱۶:۳۰	۱۶:۵۰	سالن ابوریحان
۱۸	میزگرد تخصصی مسئول: دکتر محمدحسام تدین	ظرفیت‌سازی و توسعه‌ی نیروی انسانی در حوزه‌ی امنیت سایبری در کشور	۱۷:۰۰	۱۸:۳۰	سالن ابوریحان

برنامه بیستمین کنفرانس بین‌المللی انجمن رمز ایران

روز دوم- ۹ شهریور ۱۴۰۲

ردیف	عنوان برنامه	جزئیات برنامه	آغاز	پایان	محل برگزاری
۱۸		تلاوت قرآن و اعلام برنامه روز دوم کنفرانس	۸:۱۵	۸:۳۰	سالن ابوریحان
۱۹	سخنرانی کلیدی ۴ مسئول: دکتر هاله امین‌طوسی	**Cybersecurity in the Era of ChatGPT** Dr. Hadis Karimipour, University of Calgary, Canada	۸:۳۰	۰۹:۳۰	
۲۰	سخنرانی کلیدی ۵ مسئول: دکتر نصور باقری	**Understanding the Duplex and Its Security** Dr. Bart Mennink, Radboud University, Nijmegen, the Netherlands	۹:۳۰	۱۰:۳۰	
۲۱		استراحت، پذیرایی و بازدید از نمایشگاه	۱۰:۳۰	۱۱	
۲۲	نشست S3 مبانی رمزشناسی مسئول: دکتر ترانه اقلیدس دکتر مهدی سجادیه	Quantum Multiple Access Wiretap Channel: On the One-Shot Achievable Secrecy Rate Regions هادی آقایی و بهاره اخباری	۱۱:۰۰	۱۱:۲۰	سالن ابوریحان
۲۳		New Variations of Discrete Logarithm Problem مهدی مهدوی علیایی، سحر خالقی‌فرد، زهرا احمدیان	۱۱:۲۰	۱۱:۴۰	
۲۴		Post Quantum Digital Signature Based on the McEliece Cryptosystems with Dual Inverse Matrix فرشید حیدری ماکویی، Thomas Aaron Gulliver و محمد دخیل‌علیان	۱۱:۴۰	۱۲:۰۰	
۲۵	نشست S4 پروتکل‌های امنیتی ۱ مسئول: دکتر معصومه صفخانی، دکتر محمدعلی اخایی	سیستم احرازهویت با سیگنال ضربان قلب برمبنای یادگیری عمیق سجاد ملکی، اکرم بیگی و نصور باقری	۱۱:۰۰	۱۱:۲۰	سالن ۱
۲۶		A Lightweight RFID Grouping Proof Protocol with Forward Secrecy and Resistant to Reader Compromised Attack فاطمه بُرجَل بیاتیانی، حمید مَلا	۱۱:۲۰	۱۱:۴۰	
۲۷		On the Security of an Access Control Scheme for Wireless Body Area Networks پریچهر دادخواه، محمد دخیل‌علیان و پروین رستگاری	۱۱:۴۰	۱۲:۰۰	
۲۸		نماز و ناهار	۱۲:۰۰	۱۳:۳۰	

برنامه بیستمین کنفرانس بین‌المللی انجمن رمز ایران

روز دوم- ۹ شهریور ۱۴۰۲

ردیف	عنوان برنامه	جزئیات برنامه	آغاز	پایان	محل برگزاری
۲۹	نشست S5 پروتکل‌های امنیتی ۲ مسئول: دکتر نصور باقری، دکتر فرخ‌لقا معظمی	حفظ حریم خصوصی در خدمات مبتنی بر مکان داخلی برای شهرهای هوشمند وحیده مقتدایی، دانشگاه شهید بهشتی (سخنران مدعو۳)	۱۳:۳۰	۱۴:۰۰	سالن ابوریحان
۳۰		An Efficient Scheme for Secure Medical Data Sharing in the Cloud ایمان جعفریان و سیاوش خرسندی	۱۴:۰۰	۱۴:۲۰	
۳۱		Privacy-Preserving Dataset Publishing Using Autoencoders محمدعلی جمشیدی، محمدمهدی مجاهدیان و محمدرضا عارف	۱۴:۲۰	۱۴:۴۰	
۳۲		پایگاه داده‌ی وارسی‌پذیر با قابلیت جستجوی بازه‌ای سید حسین تهامی و حمید مَلا	۱۴:۴۰	۱۵:۰۰	
۳۳		تحلیل رویکردهای جهانی در ارائه چارچوب‌های آموزش و به‌کارگیری متخصصان امنیت سایبری احمد راهداری و محمدحسام تدین	۱۵:۰۰	۱۵:۲۰	
۳۴	نشست S6 امنیت شبکه و رایانش مسئول: دکتر هاله امین‌طوسی دکتر مهدی آبادی	تحلیل آسیب‌پذیری برنامه‌های اندروید و ارتباطات آن‌ها به روش مهندسی معکوس مدل‌رانده عاطفه نیرومند، دانشگاه اصفهان (سخنران مدعو ۴)	۱۳:۳۰	۱۴:۰۰	سالن ۱
۳۵		Using ChatGPT as a Static Application Security Testing Tool عطیه بخشنده، عبدالصمد کرامت‌فر، امیر نوروزی و مهدی چکیده‌خون	۱۴:۰۰	۱۴:۲۰	
۳۶		A Semi-Supervised IDS for Cyber-Physical Systems Using a Deep Learning Approach امیرحسین صالحی، سیاوش احمدی، محمدرضا عارف	۱۴:۲۰	۱۴:۴۰	
۳۷		Private Federated Learning: An Adversarial Sanitizing Perspective مجتبی شیرین‌جانی، سیاوش احمدی، ترانه اقلیدس، محمدرضا عارف	۱۴:۴۰	۱۵:۰۰	
۳۸		محصول ParsZTNA: یک مدل امنیتی اعتمادصفر جهت رفع چالش‌های امنیتی سازمان‌ها رسول رمضانیان، سمیه سلطانی و امیر ذوالفقاری	۱۵:۰۰	۱۵:۲۰	
۳۹		استراحت و پذیرایی	۱۵:۲۰	۱۵:۵۰	

برنامه بیستمین کنفرانس بین‌المللی انجمن رمز ایران

روز دوم- ۹ شهریور ۱۴۰۲

ردیف	عنوان برنامه	جزئیات برنامه	آغاز	پایان	محل برگزاری
۴۰	نشست S7 پروتکل‌های امنیتی ۳ مسئول نشست: دکتر جواد مهاجری، راضیه سالاری‌فرد	حمله کشف کلید عملی روی پروتکل احراز اصالت و توافق کلید SecAuthUAV در شبکه پهپادها و ارائه یک پروتکل بهبود یافته جواد علیزاده و سید هادی نورانی اصل	۱۵:۵۰	۱۶:۱۰	سالن ابوریحان
۴۱		یک طرح احراز هویت و توافق کلید امن مناسب شبکه‌هایLoRaWAN زهرا جعفری، سحر پَلیمی، محمدامین صبائی، رحمان حاجیان، سید حسین عرفانی	۱۶:۱۰	۱۶:۳۰	
۴۲		Designated-Server Hierarchical Searchable Encryption in Identity-Based Setting دانیال شیرالی، نصرالله پاک‌نیت و زیبا اسلامی	۱۶:۳۰	۱۶:۵۰	
۴۳		A Lightweight Mutual Authentication Scheme for VANETs between Vehicles and RSUs محمدرضا امانی، جواد مهاجری، محمود سلماسی‌زاده	۱۶:۵۰	۱۷:۱۰	
۴۴	نشست S8 زنجیره قالب‌ها مسئول: دکتر صادق دری و دکتر مجید بیات	امنیت زنجیره‌های قالبی در فضای سایبری سید مرتضی پورنقی، دانشگاه جامع امام حسین(ع) (سخنران مدعو ۵)	۱۵:۵۰	۱۶:۲۰	سالن ۱
۴۵		یک طرح مخلوط کردن جدید برای بهبود حریم خصوصی در تراکنش‌های رمزارز بیتکوین هادی نوروزی چلچه، سلمان نیک‌صفت	۱۶:۲۰	۱۶:۴۰	
۴۶		مدیریت انگیزه‌ها در رمزارز ثابت‌قیمت پارسه رسول رمضانیان، محمدرضا فاتحی‌نیا و امیر ذوالفقاری	۱۶:۴۰	۱۷:۰۰	
		استراحت		۱۷:۱۵	
۴۷	مراسم پایانی	سخنرانی رئیس محترم انجمن رمز ایران (دکتر محمدرضا عارف)	۱۷:۱۵	۱۸:۰۰	سالن ابوریحان
۴۹		تقدیر و تشکر از حامیان، برگزارکنندگان و شرکت‌کنندگان			
۵۰		تقدیر از داوران برترکنفرانس و مجلات انجمن، مسئول محور برتر، رساله و پایان نامه برتر، مقاله برتر، شاخه دانشجویی برتر			
۵۱		قرائت بیانیه پایانی کنفرانس (مهندس حبیب رستمی)			
		پایان			