

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 رئیس محترم 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: چرایی، 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	سالن ابوریحان
		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
		ناهار و نماز 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

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

برنامه بیستمین کنفرانس بین‌المللی انجمن رمز ایران

روز اول - ۸ شهریور ۱۴۰۲

محل برگزاری	پایان	آغاز	جزئیات برنامه	عنوان برنامه	ردیف
	۱۶:۳۰	۱۶:۰۰	استراحت		۱۶
سالن ابوریحان	۱۶:۵۰	۱۶:۳۰	ارائه شرکت فناور برتر و اعطای جایزه	جایزه دکتر برنجکوب: دکتر محمود مدرس هاشمی	۱۷
سالن ابوریحان	۱۸:۳۰	۱۷:۰۰	ظرفیت‌سازی و توسعه‌ی نیروی انسانی در حوزه‌ی امنیت سایبری در کشور	میزگرد تخصصی مسئول: دکتر محمدحسام تدین	۱۸

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	
۱۹	سخنرانی کلیدی ۴ مسئول: دکتر هاله امین‌طوسی	Cybersecurity in the Era of ChatGPT Dr. Hadis Karimpour, University of Calgary, Canada	۸:۳۰	۰۹:۳۰	سالن ابوریحان
۲۰	سخنرانی کلیدی ۵ مسئول: دکتر زهرا احمدیان	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:	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 خالقی فرد، 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:	سیستم احراز هویت با سیگنال ضربان قلب بر مبنای یادگیری عمیق سجاد ملکی، اکرم بیگی و منصور باقری	۱۱:۰۰	۱۱:۲۰	سالن ۱
۲۶		A Lightweight RFID Grouping Proof Protocol with Forward Secrecy and Resistant to Reader Compromised Attack فاطمه بُرجل بیاتبانی، حمید ملا	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		ناهار و نماز	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:	حفظ حریم خصوصی در خدمات مبتنی بر مکان داخلی برای شهرهای هوشمند وحیده مقتدایی، دانشگاه شهید بهشتی (سخنران مدعو ۳)	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 واری‌پذیر با قابلیت جستجوی بازه‌ای سید حسین تهامی و حمید ملا	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:	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

محل برگزاری	پایان	آغاز	جزئیات برنامه	عنوان برنامه	ردیف
سالن ابوریحان	۱۶:۱۰	۱۵:۵۰	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	نشست S7 پروتکل‌های امنیتی ۳ مسئول نشست:	۴۰
	۱۶:۳۰	۱۶:۱۰	یک طرح احراز هویت و توافق کلید امن مناسب شبکه‌های LoRaWAN زهره جعفری، سحر پلیمی، محمدامین صباغی، رحمان حاجیان، سید حسین عرفانی		۴۱
	۱۶:۵۰	۱۶:۳۰	Designated-Server Hierarchical Searchable Encryption in Identity-Based Setting دانیال شیرالی، نصرالله پاک‌نیت و زیبا اسلامی		۴۲
	۱۷:۱۰	۱۶:۵۰	A Lightweight Mutual Authentication Scheme for VANETs between Vehicles and RSUs محمد رضا امانی، جواد مهاجری، محمود سلماسی زاده		۴۳
سالن ۱	۱۶:۲۰	۱۵:۵۰	امنیت زنجیره‌های قالبی در فضای سایبری سید حسین پورنقی، دانشگاه جامع امام حسین (ع) (سخنران مدعو ۵)	نشست S8 زنجیره قالبها مسئول: دکتر صادق دری و دکتر محمدعلی اخایی	۴۴
	۱۶:۴۰	۱۶:۲۰	یک طرح مخلوط کردن جدید برای بهبود حریم خصوصی در تراکنش‌های رمز ارز بیتکوین هادی نوروزی چلچله، سلمان نیک‌صفت		۴۵
	۱۷:۰۰	۱۶:۴۰	مدیریت انگیزه‌ها در رمز ارز ثابت‌قیمت پارسه رسول رمضانیان، محمد رضا فاتحی‌نیا و امیر ذوالفقاری		۴۶
	۱۷:۱۵		استراحت		
سالن ابوریحان	۱۸:۰۰	۱۷:۱۵	سخنرانی رئیس محترم انجمن رمز ایران (دکتر محمد رضا عارف)	مراسم پایانی	۴۷
			تقدیر و تشکر از حامیان، برگزار کنندگان و شرکت کنندگان		۴۹
			تقدیر از داوران برتر، مسئول محور برتر، رساله و پایان نامه برتر، مقاله برتر		۵۰
			قرائت بیانیه پایانی کنفرانس (مهندس حبیب رستمی)		۵۱
پایان					