به نام خدا

برنامه زمان‌بندی شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران

تاریخ	عنوان برنامه	زمان	
چهارشنبه ۹۸/۶/۶	پذیرش	۸	۸:۳۰
	مراسم آغازین کنفرانس	۸:۳۰	۹:۳۰
	سخنرانی کلیدی: درس‌ها و تجربه‌هایی از توسعه توانمندی‌های ملی در حوزه سیستم‌های مخابرات نوری *سخنران: دکتر مهدی پاکروان، دانشگاه صنعتی شریف* *مسئول نشست: دکتر رسول جلیلی*	۹:۳۰	۱۰:۳۰
	پذیرایی و بازدید از نمایشگاه	۱۰:۳۰	۱۱
	سخنرانی کلیدی: رمزنگاری در عصر کوانتوم *سخنران: دکتر ترانه اقلیدس، دانشگاه صنعتی شریف* *مسئول نشست: دکتر محمود احمدیان عطاری*	۱۱	۱۲
	اقامه نماز و صرف ناهار	۱۲:۰۰	۱۳:۳۰
	مجمع عمومی انجمن رمز ایران	۱۳:۳۰	۱۴:۳۰
	نشست ۱: امنیت اینترنت اشیاء و سامانه‌های صنعتی، جرم‌یابی سخنرانی مدعو: امنیت شهر هوشمند *سخنران: دکتر حسین قرائی، پژوهشگاه ارتباطات و فناوری اطلاعات*	۱۴:۳۰	۱۶
	نشست ۲: پروتکل‌های امنیتی ۱	۱۴:۳۰	۱۶
	پذیرایی و بازدید از نمایشگاه	۱۶	۱۶:۳۰
	نشست ۳: امنیت شبکه سخنرانی مدعو: شکار تهدیدات در شبکه‌های با پهنای باند بالا *سخنران: مهندس مرتضی نوفرستی، دانشگاه صنعتی شریف*	۱۶:۳۰	۱۸
	نشست ۴: پروتکل‌های امنیتی ۲	۱۶:۳۰	۱۸
	میزگرد «مسائل مدیریتی، قانون‌گذاری و سیاست‌گذاری در امنیت زیرساخت‌های حیاتی کشور»	۱۸	۱۹:۳۰

مشهد، میدان آزادی، پردیس دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر
تلفن: ۳۸۸۰۶۱۲۶-۰۵۱ نمابر: ۳۸۸۰۷۱۸۱-۰۵۱
http://iscisc2019.um.ac.ir 2019@isc.org.ir

به نام خدا

تاریخ	عنوان برنامه	زمان	
پنجشنبه ۹۸/۶/۷	نشست ۵: مبانی رمزنگاری، پیاده‌سازی الگوریتم‌ها و پروتکل‌های رمزنگاری و حملات مرتبط سخنرانی مدعو: معماری کارا و سریع ضرب نقطه‌ای روی خم ۲۵۵۱۹ *سخنران: دکتر راضیه سالاری فرد، دانشگاه صنعتی شریف*	۸:۳۰	۱۰
	نشست ۶: نهان سازی اطلاعات	۸:۳۰	۱۰
	مسابقه و ارزیابی ماراتن عمومی‌سازی امنیت و رمز	۸:۳۰	۱۰
	پذیرایی و بازدید از نمایشگاه	۱۰	۱۰:۳۰
	نشست ارائه‌های پوستری *مسئول نشست: دکتر محمدرضا هوشمند*	۱۰:۳۰	۱۲:۳۰
	نشست طرح مساله «امنیت سامانه های صنعتی و اینترنت اشیاء»	۱۰:۳۰	۱۲:۳۰
	رویداد شاخه‌های دانشجویی انجمن رمز ایران (گردهم‌آیی سالانه شاخه‌های دانشجویی)	۱۰:۳۰	۱۲:۳۰
	اقامه نماز و صرف ناهار	۱۲:۳۰	۱۴
	نشست ۷: مبانی رمزنگاری سخنرانی مدعو: روند پژوهش‌های دانش رمزنگاری در سطح بین‌الملل *سخنران: دکتر محمدعلی ارومیه‌چی‌ها، پژوهشگاه خواجه نصیر طوسی*	۱۴	۱۵:۳۰
	نشست ۸: امنیت رایانش	۱۴	۱۵:۳۰
	پذیرایی	۱۵:۳۰	۱۶
	مراسم پایانی کنفرانس و تقدیر	۱۶	۱۷:۳۰

مشهد، میدان آزادی، پردیس دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر
تلفن: ۳۸۸۰۶۱۲۶-۰۵۱ نمابر: ۳۸۸۰۷۱۸۱-۰۵۱
http://iscisc2019.um.ac.ir 2019@isc.org.ir

به نام خدا

جدول ارائه مقاله‌های شفاهی

* مدت زمان ارائه هر مقاله، ۲۰ دقیقه (۱۵ دقیقه ارائه + ۵ دقیقه پرسش و پاسخ) می‌باشد.

** مدت زمان سخنرانی مدعو ۳۰ دقیقه می‌باشد.

شماره نشست	عنوان نشست	تاریخ/زمان	مسئول نشست	عنوان مقاله
۱	امنیت اینترنت اشیاء و سامانه‌های صنعتی و جرم‌یابی	چهارشنبه ۹۸/۶/۶ ۱۶-۱۴:۳۰	دکتر محمدرضا هوشمند دکتر رضا ابراهیمی آتانی	طرح زنجیره قالب با قابلیت تغییرپذیری تراکنشها
				ارزیابی مجموعه حملات نشأت گرفته شده از حمله مرد میانی در شبکه های کنترل صنعتی با نگاه ویژه به پروتکل DNP۳
				Blind Multipurpose Image Watermarking Based on Secret Sharing
۲	پروتکل‌های امنیتی ۱	چهارشنبه ۹۸/۶/۶ ۱۶-۱۴:۳۰	دکتر هادی سلیمانی دکتر محمود احمدیان	Improvement of Digest Based Authentication for Biometric Verification
				GSLHA: Group-based Secure Lightweight Handover Authentication Protocol for M2M Communication
				A New RF-PUF Based Authentication of Internet of Things Using Random Forest Classification
				An Ultra-Lightweight RFID Mutual Authentication Protocol
۳	امنیت شبکه	چهارشنبه ۹۸/۶/۶ ۱۸-۱۶:۳۰	دکتر مرتضی امینی دکتر حمید ملا	Investigating the Streaming Algorithms Usage in Website Fingerprinting Attack Against Tor Privacy Enhancing Technology
				فانوس: راهکار مقابله با حملات انگشت نگاری وب سایت
				شناسایی روبات های وب با استفاده ازترکیب رویکردهای مبتنی بر ماشین های بردار پشتیبان فازی

مشهد، میدان آزادی، پردیس دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر
تلفن: ۳۸۸۰۶۱۲۶-۰۵۱ نمابر: ۳۸۸۰۷۱۸۱-۰۵۱
http://iscisc2019.um.ac.ir 2019@isc.org.ir

به نام خدا

شماره نشست	عنوان نشست	تاریخ/زمان	مسئول نشست	عنوان مقاله
۴	پروتکل‌های امنیتی ۲	چهارشنبه ۹۸/۶/۶ ۱۸-۱۶:۳۰	مهندس جواد مهاجری دکتر نصور باقری	A Lightweight Anonymous Authentication Protocol for IoT Wireless Sensor Networks
				ارزیابی عملکرد روشهای تشخیص شبکه های بات در مقابل حملات تقلیدی
				یک تمایزگر تفاضلی برای دو دور الگوریتم رمزگذاری احرازاصالت شده π-Cipher
				ارائه مدل عملی حفظ حریم خصوصی در قراردادهای هوشمند مبتنی بر زنجیره بلوکی با کاهش سربار
۵	مبانی رمزنگاری، پیاده‌سازی الگوریتم‌ها و پروتکل‌های رمزنگاری و حملات مرتبط	پنجشنبه ۹۸/۶/۷ ۱۰-۸:۳۰	دکتر محمود احمدیان دکتر زهرا احمدیان	یک طرح تسهیم راز مقاوم در برابر تقلب مبتنی بر گراف
				Cryptanalysis of sp۲das and ۳PDA, Two Data Aggregation Schemes for Smart Grid
				ارائه و پیاده سازی حمله ی زمانی برنشتاین بهبود یافته بدون داشتن دسترسی ریشه
۶	نهان‌سازی	پنجشنبه ۹۸/۶/۷ ۱۰-۸:۳۰	دکتر محمدعلی اخایی دکتر رضا ابراهیمی آتانی	A Novel Steganography Algorithm Using Edge Detection and MPC Algorithm
				Blind Image Watermarking Based on Area Quantization
				کاربرد یادگیری عمیق و شبکه عصبی پیچشی در نهانکاوی
۷	مبانی رمزنگاری	پنجشنبه ۹۸/۶/۷ ۱۴-۱۵:۳۰	دکتر هادی سلیمانی دکتر محمود احمدیان	Lightweight Involutive Components for Symmetric Cryptography
				Cryptanalysis of a Certificateless Signcryption Scheme
۸	امنیت رایانش	پنجشنبه ۹۸/۶/۷	دکتر بهروز ترک لادانی	Ransomware Detection Using Process Mining and Classification Algorithms

مشهد، میدان آزادی، پردیس دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر
تلفن: ۳۸۸۰۶۱۲۶-۰۵۱ نمابر: ۳۸۸۰۷۱۸۱-۰۵۱
http://iscisc2019.um.ac.ir 2019@isc.org.ir

به نام خدا

شماره نشست	عنوان نشست	تاریخ/زمان	مسئول نشست	عنوان مقاله
		۱۴-۱۵:۳۰	دکتر علیرضا کشاورز	Inferring API Correct Usage Rules: A Tree-based Approach
				An Anonymous Attribute-based Access Control System Supporting Access Structure Update

مشهد، میدان آزادی، پردیس دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر
تلفن: ۳۸۸۰۶۱۲۶-۰۵۱ نمابر: ۳۸۸۰۷۱۸۱-۰۵۱
http://iscisc2019.um.ac.ir 2019@isc.org.ir

دانزدهمین کنفرانس بین المللی انجمن رمز ایران
۶ و ۷ شهریور ۱۳۹۸
دانشگاه فردوسی مشهد
Sponsored and Indexed by CIVILICA We Respect the Science

به نام خدا

جدول ارائه مقاله‌های پوستری

تاریخ / زمان: پنج‌شنبه ۹۸/۶/۷ – ساعت ۱۲:۳۰-۱۰:۳۰

مسوول نشست: دکتر محمدرضا هوشمند

عنوان مقاله
Threat Extraction in IoT-Based Systems Focusing on Smart Cities
Classical-Quantum Multiple Access Wiretap Channel
Fault tolerant non-linear techniques for scalar multiplication in ECC
IoT-Based Anonymous Authentication Protocol Using Biometrics in Smart Homes
system for cloud-based IoTs An efficient secret sharing-based storage
Ransomware Detection Analysis of Machine Learning Techniques for
CRT-Based Robust Data Hiding Method by Extracting Features in DCT Domain
News Using Blockchain SANUB: A new method for Sharing and Analyzing
ارزیابی امنیت و کارایی طرح‌های توام رمزنگاری و فشرده‌سازی تصویر به منظور ارائه رویکردهای جدید در ارتباطات بی‌سیم
طراحی شبکه امن با یکسوسازی و کنترل جریان داده‌ها
محدودسازی حمله سیاهچاله در شبکه‌های متحرک اقتضایی با استفاده از روش یادگیری Q
تحلیل و بهبود "طرح احرازاصالت با حفظ مشروط حریم خصوصی CPPA" در شبکه‌های خودرویی
ارزیابی امنیتی بستر ابری اوپن استک در مقابل حملات از کاراندازی سرویس
دسته‌بندی مشتریان شرکت‌های ارائه‌دهنده سرویس‌های پرداخت با استفاده از تارنمای فروشگاهی آنان به کمک روش‌های داده‌کاوی
پیاده‌سازی حمله لغت‌نامه‌ای به گذرواژه‌ها بر روی GPU
تشخیص تروجان سخت‌افزاری بر مبنای تحلیل توان مصرفی، با استفاده از الگوریتمPCA و شبکه عصبی مصنوعی MLP
آزمایش و مقایسه سامانه تشخیص نفوذsuricata در تعامل با بهترین سامانه‌های انتقال سریع بسته
سیستم‌های رای‌گیری الکترونیکی مبتنی بر بلاکچین

مشهد، میدان آزادی، پردیس دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر
تلفن: ۳۸۸۰۶۱۲۶-۰۵۱ نمابر: ۳۸۸۰۷۱۸۱-۰۵۱
http://iscisc2019.um.ac.ir 2019@isc.org.ir

پنجمین کنفرانس بین‌المللی انجمن رمز ایران
۶ و ۷ شهریور ۱۳۹۸
دانشگاه فردوسی مشهد
Sponsored and Indexed by CIVILICA We Respect the Science