

برنامه زمان بندی شانزدهمین کنفرانس بین المللی انجمن رمز ایران

زمان		عنوان برنامه	تاریخ
۸:۳۰	۸	پذیرش	چهارشنبه ۹۸/۶/۶
۹:۳۰	۸:۳۰	مراسم آغازین کنفرانس (قرائت قرآن کریم، سرود ملی، سخنرانی دبیر کنفرانس، ...)	
۱۰:۳۰	۹:۳۰	سخنرانی کلیدی: درس‌ها و تجربه‌هایی از توسعه توانمندی‌های ملی در حوزه سیستم‌های مخابرات نوری سخنران: آقای دکتر مهدی پاکروان، دانشگاه صنعتی شریف مسئول نشست: آقای دکتر رسول جلیلی	
۱۱	۱۰:۳۰	پذیرایی و بازدید از نمایشگاه	
۱۲	۱۱	سخنرانی کلیدی: رمزنگاری در عصر کوانتوم سخنران: خانم دکتر ترانه اقلیدس، دانشگاه صنعتی شریف مسئول نشست: آقای دکتر محمود احمدیان عطاری	
۱۳:۳۰	۱۲:۰۰	اقامه نماز و صرف ناهار	
۱۴:۳۰	۱۳:۳۰	مجمع عمومی انجمن رمز ایران	
۱۶	۱۴:۳۰	نشست ۱: امنیت اینترنت اشیاء و سامانه‌های صنعتی، جرم یابی سخنرانی مدعو: چالش‌های امنیتی شهر هوشمند سخنران: آقای دکتر حسین قرائی، پژوهشگاه ارتباطات و فناوری اطلاعات نشست ۲: پروتکل‌های امنیتی	
۱۶:۳۰	۱۶	پذیرایی و بازدید از نمایشگاه	
۱۸	۱۶:۳۰	نشست ۳: امنیت شبکه سخنرانی مدعو: شکار تهدیدات در شبکه‌های با پهنای باند بالا سخنران: آقای مهندس مرتضی نوفرستی، دانشگاه صنعتی شریف نشست ۴: پروتکل‌های امنیتی	
۲۰	۱۸	میزگرد «مسائل مدیریتی، قانون‌گذاری و سیاست‌گذاری در امنیت زیرساخت‌های حیاتی کشور»	

انجمن رمز ایران
شانزدهمین کنفرانس بین‌المللی
سازمان

۶ و ۷ شهریور ۱۳۹۸
دانشگاه فردوسی مشهد



مرکز استنادی علوم اسلامی جهان و فناوری



Sponsored and Indexed by
CIVILICA
We Respect the Science

مشهد، میدان آزادی، پردیس دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر

تلفن: ۰۵۱-۳۸۸۰۶۱۲۶ شماره: ۰۵۱-۳۸۸۰۷۱۸۱

<http://iscisc2019.um.ac.ir> 2019@isc.org.ir



۶ و ۷ شهریور ۱۳۹۸
دانشگاه فردوسی مشهد



Sponsored and Indexed by
CIVILICA
We Respect the Science

زمان		عنوان برنامه	تاریخ
۹:۳۰	۸	مسابقه و ارزیابی مارتن عمومی سازی امنیت و رمز	پنجشنبه ۹۸/۶/۷
۱۰:۳۰	۹:۳۰	سخنرانی کلیدی: Recent Designs in Symmetric Cryptography Prof. Gregor Leander: Ruhr University, Bochum Germany مسئول نشست: آقای دکتر منصور باقری	
۱۱	۱۰:۳۰	پذیرایی و بازدید از نمایشگاه	
۱۲:۳۰	۱۱	نشست ۵: مبانی رمزنگاری، پیاده سازی الگوریتم ها و پروتکل های رمزنگاری و حملات مرتبط سخنرانی مدعو: پیاده سازی کارای رمزنگاری خم بیضوی ۲۵۵۱۹ سخنران: خانم دکتر راضیه سالاری فرد، دانشگاه صنعتی شریف نشست ۶: نهران سازی اطلاعات	
۱۲:۳۰	۱۱	نشست ارائه های پوستری مسئول نشست: آقای دکتر محمدرضا هوشمند	
۱۲:۳۰	۱۱	نشست طرح مساله «امنیت اتوماسیون صنعتی و اینترنت اشیا»	
۱۲:۳۰	۱۱	رویداد شاخه های دانشجویی انجمن رمز ایران (گردهمایی سالانه شاخه های دانشجویی)	
۱۴	۱۲:۳۰	اقامه نماز و صرف ناهار	
۱۵:۳۰	۱۴	نشست ۷: مبانی رمزنگاری سخنرانی مدعو: رمزنگاری کاربردی، افقهای پیش رو سخنران: آقای دکتر محمدعلی ارومیه چی ها، پژوهشگاه خواجه نصیرطوسی نشست ۸: امنیت رایانش	
۱۶	۱۵:۳۰	پذیرایی	
۱۷:۳۰	۱۶	مراسم پایانی کنفرانس و تقدیر	

مشهد، میدان آزادی، پردیس دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر

تلفن: ۰۵۱-۳۸۸۰۶۱۲۶ شماره: ۰۵۱-۳۸۸۰۷۱۸۱

<http://iscisc2019.um.ac.ir> 2019@isc.org.ir

جدول زمان بندی ارائه مقالات

شماره نشست	عنوان نشست	مسئول نشست	سخنران مدعو	کد مقاله
۱	امنیت اینترنت اشیاء و سامانه های صنعتی و جرم یابی	دکتر محمدرضا هوشمند دکتر رضا ابراهیمی آتانی	دکتر حسین قرائی	۱۵۷۰۵۶۱۸۵۱
				۱۵۷۰۵۶۱۴۸۷
				۱۵۷۰۵۵۴۱۴۱
۲	پروتکل های امنیتی ۱	دکتر هادی سلیمانی دکتر محمود احمدیان	-	۱۵۷۰۵۱۶۹۷۸
				۱۵۷۰۵۶۰۳۷۵
				۱۵۷۰۵۵۸۸۰۰
۳	امنیت شبکه	دکتر مرتضی امینی دکتر حمید ملا	مهندس مرتضی نوفرستی	۱۵۷۰۵۵۹۳۳۳
				۱۵۷۰۵۱۵۸۰۵
				۱۵۷۰۵۵۹۹۱۲
۴	پروتکل های امنیتی ۲	دکتر جواد مهاجری دکتر منصور باقری	-	۱۵۷۰۵۶۱۳۰۳
				۱۵۷۰۵۱۹۷۸۹
				۱۵۷۰۵۶۱۴۰۸
۵	مبانی رمزنگاری، پیاده سازی الگوریتم ها و پروتکل های رمزنگاری و حملات مرتبط	دکتر محمود احمدیان دکتر زهرا احمدیان	دکتر راضیه سالاری فرد	۱۵۷۰۵۶۱۴۶۲
				۱۵۷۰۵۶۱۴۹۰
				۱۵۷۰۵۶۱۵۲۰
۶	نهان سازی	دکتر محمدعلی اخایی دکتر رضا ابراهیمی آتانی	-	۱۵۷۰۵۶۱۲۲۱
				۱۵۷۰۵۶۱۷۳۱
				۱۵۷۰۵۶۱۴۳۳
۷	مبانی رمزنگاری	دکتر هادی سلیمانی دکتر محمود احمدیان	دکتر محمدعلی ارومیه چی ها	۱۵۷۰۵۵۳۰۴۴
				۱۵۷۰۵۵۳۸۱۵
۸	امنیت رایانش	دکتر بهروز ترک لادانی دکتر علیرضا کشاورز	-	۱۵۷۰۵۱۶۹۲۲
				۱۵۷۰۵۶۱۴۴۸
				۱۵۷۰۵۶۱۵۰۳

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

** مدت زمان سخنرانی مدعو ۳۰ دقیقه می باشد.

مشهد، میدان آزادی، پردیس دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر

تلفن: ۰۵۱-۳۸۸۰۶۱۲۶ نامبر: ۰۵۱-۳۸۸۰۷۱۸۱

<http://iscisc2019.um.ac.ir> 2019@isc.org.ir

انجمن رمز ایران
پیش از سخنرانی
شماره ۱۳۹۸

۶ و ۷ شهریور ۱۳۹۸

دانشگاه فردوسی مشهد



مرکز استنادی علوم اسلامی جهان



Sponsored and Indexed by
CIVILICA
We Respect the Science



عنوان مقالات	کد مقاله	شماره نشست
طرح زنجیره قالب با قابلیت تغییرپذیری تراکنشها	۱۵۷۰۵۶۱۸۵۱	۱
Assessing Derived Attacks from MITM Attack in Industrial Control Systems with Respect to DNP3 Protocol	۱۵۷۰۵۶۱۴۸۷	
Blind Multipurpose Image Watermarking Based on Secret Sharing	۱۵۷۰۵۵۴۱۴۱	
Improvement of Digest Based Authentication for Biometric Verification	۱۵۷۰۵۱۶۹۷۸	۲
GSLHA: Group-based Secure Lightweight Handover Authentication Protocol for M2M Communication	۱۵۷۰۵۶۰۳۷۵	
A New RF-PUF Based Authentication of Internet of Things Using Random Forest Classification	۱۵۷۰۵۵۸۸۰۰	
An Ultra-Lightweight RFID Mutual Authentication Protocol	۱۵۷۰۵۶۰۸۸۱	۳
Website Fingerprinting: Attacking Popular Tor Privacy Enhancing Technology Using Stream Mining Methods	۱۵۷۰۵۵۹۳۳۳	
فانوس: راهکار مقابله با حملات انگشت نگاری وب سایت	۱۵۷۰۵۱۵۸۰۵	
شناسایی روبات های وب با استفاده از ترکیب رویکردهای مبتنی بر ماشین های بردار پشتیبان فازی	۱۵۷۰۵۵۹۹۱۲	۴
A Lightweight Anonymous Authentication Protocol for IoT Wireless Sensor Networks	۱۵۷۰۵۶۱۳۰۳	
Evaluation of P2P Botnet Detection Methods Against Mimicry Attacks	۱۵۷۰۵۱۹۷۸۹	
π -یک تمایزگر تفاضلی برای دو دور الگوریتم رمزگذاری احراز اصالت شده	۱۵۷۰۵۶۱۴۰۸	۵
ارائه مدل عملی حفظ حریم خصوصی در قراردادهای هوشمند مبتنی بر زنجیره بلوکی با کاهش سربرار	۱۵۷۰۵۶۱۴۳۲	
یک طرح تسهیم راز مقاوم در برابر تقلب مبتنی بر گراف	۱۵۷۰۵۶۱۴۶۲	۶
Cryptanalysis of $sp\pi\pi d\alpha s$ and πPDA , Two Data Aggregation Schemes for Smart Grid	۱۵۷۰۵۶۱۴۹۰	
ارائه ی یک روش نوین در بهبود پیاده سازی حمله ی زمانی برن اشتاین	۱۵۷۰۵۶۱۵۲۰	۶
A Novel Steganography Algorithm Using Edge Detection and MPC Algorithm	۱۵۷۰۵۶۱۲۲۱	
Blind Image Watermarking Based on Area Quantization	۱۵۷۰۵۶۱۷۳۱	

عنوان مقالات	کد مقاله	شماره نشست
کاربرد یادگیری عمیق و شبکه عصبی پیچشی در پنهان شکنی	۱۵۷۰۵۶۱۴۳۳	
Lightweight Involutive Components for Symmetric Cryptography	۱۵۷۰۵۵۳۰۴۴	۷
Cryptanalysis of a Certificateless Signcryption Scheme	۱۵۷۰۵۵۳۸۱۵	
Ransomware Detection Using Process Mining and Classification Algorithms	۱۵۷۰۵۱۶۹۲۲	۸
Inferring API Correct Usage Rules: A Tree-based Approach	۱۵۷۰۵۶۱۴۴۸	
An Anonymous Attribute-based Access Control System Supporting Access Structure Update	۱۵۷۰۵۶۱۵۰۳	

انجمن رمز ایران
پیش ازین
کنفرانس
شامگاه
شامگاه

۶ و ۷ شهریور ۱۳۹۸
دانشگاه فردوسی مشهد



Sponsored and Indexed by
CIVILICA
We Respect the Science