به نام خدا

برنامه زمان‌بندی هشتمین کنفرانس بین‌المللی انجمن رمز ایران
ISCISC 2011

دانشگاه فردوسی مشهد – ۲۳ و ۲۴ شهریور ۱۳۹۰

چهارشنبه ۲۳ شهریور ۱۳۹۰	
۷:۳۰ – ۸:۳۰	ثبت‌نام و پذیرش
۸:۳۰ – ۹:۳۰	مراسم افتتاحیه
۹:۳۰ – ۱۰	پذیرایی
۱۰ – ۱۱	سخنرانی کلیدی Prof. Rogaway
۱۱ – ۱۲	جلسه مجمع عمومی انجمن رمز ایران (مخصوص اعضاء)
۱۲ – ۱۴	نماز و پذیرایی ناهار
۱۴ – ۱۶:۱۵	نشست‌های ارائه مقاله (AX, AY, AZ)
۱۶:۱۵ – ۱۶:۴۵	پذیرایی
۱۶:۴۵ – ۱۸:۴۵	میزگرد

پنج‌شنبه ۲۴ شهریور ۱۳۹۰	
۸:۳۰ – ۹:۳۰	سخنرانی کلیدی دکتر سلیمان فلاح
۹:۳۰ – ۱۰	پذیرایی
۱۰ – ۱۲	نشست‌های ارائه مقاله (BX, BY, BZ)
۱۲ – ۱۴	نماز و پذیرایی ناهار
۱۴ – ۱۶	نشست‌های ارائه مقاله (CX, CY, CZ)
۱۶ – ۱۶:۳۰	پذیرایی
۱۶:۳۰ – ۱۸	مراسم اختتامیه و تقدیر از برگزیدگان

برنامه‌های جانبی	
۲۲ شهریور ۱۳۹۰	کارگاه‌های آموزشی
۲۲ الی ۲۴ شهریور ۱۳۹۰ (ساعت ۸:۳۰ الی ۱۸)	نمایشگاه افتا
۲۳ شهریور ۱۳۹۰ (ساعت ۱۷ – ۱۴)	مسابقه کشف آسیب‌پذیری در برنامه‌های کاربردی تحت وب

محل برگزاری نشست‌ها	
مراسم افتتاحیه، اختتامیه، مجمع عمومی انجمن رمز و میزگرد	سالن فردوسی دانشکده مهندسی دانشگاه فردوسی مشهد
نشست‌های AX , BX & CX	سالن فردوسی دانشکده مهندسی دانشگاه فردوسی مشهد
نشست‌های AY , BY & CY	سالن خوارزمی دانشکده مهندسی دانشگاه فردوسی مشهد
نشست‌های AZ , BZ & CZ	سالن عطار دانشکده مهندسی دانشگاه فردوسی مشهد

نشست	عنوان نشست	کد مقاله‌ها
AX	رمزشناسی (مبانی و پیاده‌سازی)	۲۹۱، ۳۲۱، ۳۱۹، ۲۸۲، ۳۲۸، ۴۹
AZ	پروتکل‌های رمزنگاری و امنیتی (۱)	۱۹۲، ۲۲۲، ۳۰۷، ۳۴۷، ۳۶۹
BY	امنیت سیستم‌ها و کاربردها (۱)	۶۶، ۱۷۴، ۲۶۰، ۱۸۱، ۳۸۰
BZ	پروتکل‌های رمزنگاری و امنیتی (۲)	۳۱۷، ۳۷۷، ۳۶۷، ۳۶۸، ۲۷۱
CY	امنیت سیستم‌ها و کاربردها (۲)	۱۲، ۹۳، ۴۰۳، ۳۷۲، ۱۹۱
CZ	مهندسی امنیت و رمزشناسی	۲۸۵، ۳۶۲، ۱۶۷، ۲۶۲، ۳۷۵

Session	Title	Paper Code
AY	Security of Systems & Applications	316, 149, 171, 265, 247
BX	Cryptology (Fundamentals & Implementation)	225, 299, 210, 313, 224
CX	Information Hiding	202, 302, 333, 310, 160

برنامه زمان‌بندی ارائه شفاهی

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

نشست AX – رمزشناسی (مبانی و پیاده‌سازی)

چهارشنبه ۲۳ شهریور ۱۳۹۰ – ساعت ۱۶-۱۴ سالن فردوسی

مدیران نشست: دکتر منصفی، مهندس مهاجری

کد ارائه کد مقاله	عنوان مقاله	نویسندگان	زمان ارائه
AX1 ۴۹	ویژگی‌های رمزنگاری عملگر جمع پیمانه‌ای، به هنگ توانی از ۲	سید مجتبی دهنوی اکبر محمودی ریشکانی حمیدرضا میمنی	۱۴ – ۱۴:۲۰
AX2 ۳۲۸	تحلیل لغزشی متن منتخب با احتمال ۱	اکبر شاهسواران هادی سلیمانی	۱۴:۲۰ – ۱۴:۴۰
AX3 ۲۸۲	حمله توانی الگو بر روی الگوریتم رمز A5/1	محمد عجمی علی پاینده محمدرضا عارف	۱۴:۴۰ – ۱۵
AX4 ۳۱۹	رمزنگاری تصویر با کانتورلت و فوق آشوب	محمدجعفر دهقان سید علی موسوی احمد رضا دهقان مهدی یعقوبی	۱۵ – ۱۵:۲۰
AX5 ۳۲۱	یک روش ترکیبی برای رمزنگاری تصویر با استفاده از توابع فوق آشوب و عملگرهای تکاملی	سیدعبدالحمید اصفهانی داوود بخشش	۱۵:۲۰ – ۱۵:۴۰
AX6 ۲۹۱	تسریع رمزنگاری تصویر با استفاده از الگوریتم‌های موازی آشوبی بر روی پردازش‌گرهای گرافیکی	احسان خان‌میرزا محسن نساجی عبد اله چاله چاله مهرداد احمدزاده راجی	۱۵:۴۰ – ۱۶

AY Session – Security of Systems & Applications

Kharazmi Hall **Wed, September 14, 2011 – Time: 14 – 16**

Session Chair: Dr. Jalili, Dr. HajiAbolhassan

Present Code Paper Code	Paper Title	Authors	Present Time
AY1 316	Trust Modeling and Verification Using Colored Petri Nets	Amir Jalali Bidgoli Behrouz Tork Ladani	14 – 14:20
AY2 149	RTBIMS: Accuracy Enhancement in Iterative Multiplication Strategy for Computing Propagated Trust	Hassan Shakeri Abbas Ghaemi Bafghi	14:20 – 14:40
AY3 171	Computing Trust Resultant using Intervals	Hassan Shakeri Abbas Ghaemi Bafghi Hadi Sadoghi Yazdi	14:40 - 15
AY4 265	Hybrid Rule Threshold Adjustment System for Intrusion Detection	Mohammad Mahdi Moghimi Mohammad Saraee	15 – 15:20
AY5 247	Security Analyzing and Designing GUI with the Resources Model	Maryam Mehrnejad Ehsan Toreini Abbas Ghaemi Bafghi	15:20 – 15:40

نشست AZ – پروتکل‌های رمزنگاری و امنیتی (۱)

چهارشنبه ۲۳ شهریور ۱۳۹۰ – ساعت ۱۶-۱۴ سالن عطار

مدیران نشست: دکتر گردشی، دکتر لادانی

کد ارائه کد مقاله	عنوان مقاله	نویسندگان	زمان ارائه
AZ1 ۳۶۹	ارائه‌ی مدل صوری طرح امضای کور با استفاده از روش استقرایی	نجمه سادات میرامیرخانی حمیدرضا محروقی رسول جلیلی	۱۴ – ۱۴:۲۰
AZ2 ۳۴۷	سامانه توأم رمزنگاری متقارن–کدگذاری کانال مبتنی بر کدهای بررسی توازن کم چگال منظم	رضا هوشمند ترانه اقلیدس محمدرضا عارف	۱۴:۲۰ – ۱۴:۴۰
AZ3 ۳۰۷	گمنام‌سازی مسیرهای حرکت اشیا متحرک با سطوح متفاوت حریم خصوصی	سمانه مهدوی‌فر مهدی آبادی محسن کاهانی	۱۴:۴۰ – ۱۵
AZ4 ۲۲۲	کشف و حذف حمله سیاهچاله جمعی درمسیریابی AODV در شبکه‌های ویژه ادهاک	مهدی مدادیان خسرو فرداد احمد معبادی	۱۵ – ۱۵:۲۰
AZ5 ۱۹۲	همه پخشی و تک پخشی ذاتاً امن در شبکه‌های حسگر بی‌سیم	حسن نصیرایی بندپی جمشید باقرزاده محمد اهدائی	۱۵:۲۰ – ۱۵:۴۰

BX Session – Cryptology (Fundamentals & Implementation)

Ferdowsi Hall **Thu, September 15, 2011 – Time: 10 – 12**

Session Chair: Prof Rogaway, Dr. Eghlidos

Present Code Paper Code	Paper Title	Authors	Present Time
BX1 225	On the Period of GSM's A5/1 Stream Cipher and Its Internal State Transition Structure	Vahid Amin Ghaffari Ali Vardasbi	10 – 10:20
BX2 299	An Improved Attack on A5/1	Vahid Amin Ghafari Javad Mohajeri	10:20 – 10:40
BX3 210	An Entanglement-based Quantum Key Distribution Protocol	Monireh Houshmand Saied Hosseini-khayat	10:40 - 11
BX4 313	Cryptanalysis and Improvement on a New RFID Mutual Authentication Protocol Compatible with EPC Standard	Mohammad Hassan Habibi Mahmud Gardeshi	11 – 11:20
BX5 224	Multiple-Chi-square Tests and Their Application on Distinguishing Attacks	Ali Vardasbi Mahmoud Salmasizadeh Javad Mohajeri	11:20 – 11:40

نشست BY – امنیت سیستم‌ها و کاربردها (۱)

پنج‌شنبه ۲۴ شهریور ۱۳۹۰ – ساعت ۱۲-۱۰ سالن خوارزمی

مدیران نشست: دکتر هاشمی، دکتر نقیب‌زاده

کد ارائه کد مقاله	عنوان مقاله	نویسندگان	زمان ارائه
BY1 ۳۸۰	جستجوی مبتنی بر کلید خصوصی در داده‌های متنی رمز شده	حماد افضلی ننیز بهنام نیکبخت رضا عزمی	۱۰ – ۱۰:۲۰
BY2 ۱۸۱	روشی کارآ و امن جهت پرس‌وجوی بازه‌ای روی داده رمز شده XML	مریم کریمی رسول جلیلی	۱۰:۲۰ – ۱۰:۴۰
BY3 ۲۶۰	ارائه‌ی شاخصی امن در پایگاه داده‌های رابطه‌ای رمزشده‌ی چند کاربره	محسن رضاییان مجید غیوری مصطفی حق جو	۱۰:۴۰ – ۱۱
BY4 ۱۷۴	ارائه یک فایل سیستم امن مبتنی بر TPM با پشتیبانی گروه	امین سرده مقدم رضا عزمی	۱۱ – ۱۱:۲۰
BY5 ۶۶	چارچوب شبیه‌سازی سطح بالای حملات سایبری به منظور ارزیابی دسترس‌پذیری	مهرداد آشتیانی محمد عبدالهی ازگمی	۱۱:۲۰ – ۱۱:۴۰

نشست BZ – پروتکل‌های رمزنگاری و امنیتی (۲)

پنج‌شنبه ۲۴ شهریور ۱۳۹۰ – ساعت ۱۲-۱۰ سالن عطار

مدیران نشست: دکتر مالک، دکتر برنجکوب

کد ارائه کد مقاله	عنوان مقاله	نویسندگان	زمان ارائه
BZ1 ۲۷۱	حمله به یک پروتکل احراز اصالت در سامانه‌های RFID	محمدحسن حبیبی محمود گردشی	۱۰ – ۱۰:۲۰
BZ2 ۳۶۸	اِعمال کنترل دسترسی نوشتن در سناریوی برونسپاری داده‌ها با استفاده از مدیریت کلید رمزنگاری	سجاد امیدی حمیدرضا شهریاری	۱۰:۲۰ – ۱۰:۴۰
BZ3 ۳۶۷	تشخیص دستکاری در داده های برچسب RFID با استفاده از نشانه‌گذاری شکننده	صادق سلیمانی پریسا کاغذگران	۱۰:۴۰ – ۱۱
BZ4 ۳۷۷	یک مدل اعتماد مبتنی بر شهرت در تور اعتماد	نرجس میرزاپور احمد براآنی دستجردی	۱۱ – ۱۱:۲۰
BZ5 ۳۱۷	مدل اعتماد مبتنی بر شهرت در اجتماعات تجارت الکترونیک همتا به همتا با قابلیت تشخیص و مقابله با حملات بدخواهان	رضا عزمی معصومه کردیان	۱۱:۲۰ – ۱۱:۴۰

CX Session – Information Hiding

Ferdowsi Hall **Thu, September 15, 2011 – Time: 14 – 16**

Session Chair: Dr. Salmasizade, Dr. Sheikhzadegan

Present Code Paper Code	Paper Title	Authors	Present Time
CX1 202	A Secure and Robust Video Watermarking Based on Chaotic Maps	Somayyeh Mohammadi Siamak Talebi Ahmad Hakimi	14 – 14:20
CX2 302	Watermarking in Farsi/Arabic binary document images using fractal coding	Fatemeh Daraee Saeed Mozaffari	14:20 – 14:40
CX3 333	An efficient buyer-seller watermarking protocol based on proxy signatures	Mohammad KazemNasab Haji Ziba Eslami	14:40 - 15
CX4 310	A Reversible Data Embedding Scheme Based on Search Order Coding for VQ Index Tables	Peyman Rahmani Gholamhossein Dastghaibyfard Ehsan Rahmani	15 – 15:20
CX5 160	Cryptographic Keys Management for H.264 Scalable Coded Video Security	Mamoona Asghar Mohammed Ghanbari	15:20 – 15:40

نشست CY – امنیت سیستم‌ها و کاربردها (۲)

پنج‌شنبه ۲۴ شهریور ۱۳۹۰ – ساعت ۱۶-۱۴ سالن خوارزمی

مدیران نشست: دکتر سلیمان فلاح، دکتر کوزه‌کنانی

کد ارائه کد مقاله	عنوان مقاله	نویسندگان	زمان ارائه
CY1 ۱۹۱	رویکردی ترکیبی مبتنی بر الگوریتم‌های انتخاب منفی و کلونی زنبورهای مصنوعی برای تشخیص ناهنجاری در شبکه‌های اقتضایی متحرک	فاطمه بارانی برواتی مهدی آبادی	۱۴ – ۱۴:۲۰
CY2 ۳۷۲	روشی برای تشخیص بات‌نت‌ها در مرحله فرمان و کنترل با استفاده از خوشه‌بندی برخط	موسی یحیی‌زاده مهدی آبادی	۱۴:۲۰ – ۱۴:۴۰
CY3 ۴۰۳	تشخیص نفوذ مبتنی بر ناظر، بر اساس رویکرد سیستم‌های ایمنی مصنوعی	رضا عزمی بشری پیشگو حامد نعمتی	۱۴:۴۰ – ۱۵
CY4 ۹۳	FAPSWPP : یک پروتکل خرید امن کالای الکترونیکی مبتنی بر APSWPP	سمانه لایقیان جوان عباس قائمی بافقی	۱۵ – ۱۵:۲۰
CY5 ۱۲	همبسته‌سازی هشدارها در یک سیستم تشخیص نفوذ بر اساس سیستم ایمنی مصنوعی	مهدی باطنی احمد براآنی دستجردی	۱۵:۲۰ – ۱۵:۴۰

نشست CZ – مهندسی امنیت و رمزشناسی

پنج‌شنبه ۲۴ شهریور ۱۳۹۰ – ساعت ۱۶-۱۴ سالن عطار

مدیران نشست: دکتر ابراهیمی، دکتر شاه‌حسینی

کد ارائه کد مقاله	عنوان مقاله	نویسندگان	زمان ارائه
CZ1 ۳۷۵	نهان‌نگاری تهی و نیمه‌شکننده تصاویر دیجیتال با استفاده از استخراج ویژگی در حوزه ویولت و SVM	مینا باقری حبیب‌اله دانیالی محمدصادق هل‌فروش	۱۴ – ۱۴:۲۰
CZ2 ۲۶۲	معیار کمّی آسیب‌پذیری شبکه‌های کامپیوتری با استفاده از گراف حمله و سیستم امتیازدهی آسیب‌پذیری	الهه سمیع حمیدرضا شهریاری	۱۴:۲۰ – ۱۴:۴۰
CZ3 ۱۶۷	ارائه روشی مناسب برای بهبود و توسعه شاخص‌های مدیریت امنیت اطلاعات جهت طراحی و پیاده‌سازی در سازمان‌ها	مجتبی بهرامی	۱۴:۴۰ – ۱۵
CZ4 ۳۶۲	تحلیل صوری ویژگی وارسی‌پذیری میکس‌نت با استفاده از حساب پی کاربردی	بنیامین تختائی حمیدرضا محروقی رسول جلیلی	۱۵ – ۱۵:۲۰
CZ5 ۲۸۵	آزمون تصویری بازشناسی انسان از ماشین مبتنی بر تبدیلات هندسی	مریم مهرنژاد عباس قائمی بافقی احد هراتی احسان تورینی	۱۵:۲۰ – ۱۵:۴۰

سخنرانی‌های کلیدی

عنوان	سخنران کلیدی	زمان
Constructing Cryptographic Definitions	Prof. Phillip Rogaway	September 14, 2011 10 – 11 AM
امنیت زبان ـ مبنا: نتایج و چالش‌ها	دکتر مهران سلیمان‌فلاح	۲۴ شهریور ۱۳۹۰ ۸:۳۰ – ۹:۳۰

میزگرد

عنوان	زمان
تحقق بندهای ۳ و ۴ سیاست‌های کلان نظام در زمینه افتا • ارتقاء سطح دانش و ظرفیت‌های علمی، پژوهشی، آموزشی و صنعتی کشور برای تولید علم و فناوری مربوط به امنیت فضای اطلاعاتی و ارتباطی (افتا) • تکیه بر فناوری بومی و توان‌مندی‌های تخصصی داخلی در توسعه زیرساخت‌های علمی و فنی امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی	**چهارشنبه ۲۳ شهریور** **۱۶:۴۵-۱۸:۴۵**

مسابقه

عنوان	زمان
کشف آسیب‌پذیری در برنامه‌های کاربردی تحت وب	**چهارشنبه ۲۳ شهریور** **۱۴-۱۷**