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 شهیور 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

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	عنوان مقاله	نویسندگان	زمان ارائه
AX1	خواص عملگر جمع پیمانه ای به هنگ توانی از ۲، از منظر رمزنگاری	سید مجتبی دهنوی اکبر محمودی ریشکانی حمیدرضا میمنی	۱۴ – ۱۴:۲۰
AX2	تحلیل لغزشی متن منتخب با احتمال ۱	اکبر شاهسواران هادی سلیمانی	۱۴:۲۰ – ۱۴:۴۰
AX3	حمله توانی الگو بر روی الگوریتم رمزA5/1	محمد عجمی علی پاینده محمدرضا عارف	۱۴:۴۰ – ۱۵
AX4	رمزنگاری تصویر با کانتورلت و فوق آشوب	محمدجعفر دهقان سید علی موسوی احمد رضا دهقان مهدی یعقوبی	۱۵ – ۱۵:۲۰
AX5	یک روش ترکیبی برای رمزنگاری تصویر با استفاده از توابع فوق آشوب و عملگرهای تکاملی	سیدعبدالحمید اصفهانی داوود بخشش	۱۵:۲۰ – ۱۵:۴۰
AX6	تسریع رمزنگاری تصویر با استفاده از الگوریتم های موازی آشوبی بر روی پردازش گرهای گرافیکی	احسان خان‌میرزا محسن نساجی عبد اله چاله چاله	۱۵:۴۰ – ۱۶

AY Session – Security of Systems & Applications

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

Session Chair: Dr. Jalili, Dr. HajiAbolhassan

Present Code	Paper Title	Authors	Present Time
AY1	Trust Modeling and Verification Using Colored Petri Nets	Amir Jalali Bidgoli Behrouz Tork Ladani	14 – 14:20
AY2	RTBIMS: Accuracy Enhancement in Iterative Multiplication Strategy for Computing Propagated Trust	Hassan Shakeri Abbas Ghaemi Bafghi	14:20 – 14:40
AY3	Computing Trust Resultant using Intervals	Hassan Shakeri Abbas Ghaemi Bafghi Hadi Sadoghi Yazdi	14:40 - 15
AY4	hybrid rule threshold adjustment system for intrusion detection	Mohammad Mahdi Moghimi Mohammad Saraee	15 – 15:20
AY5	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	عنوان مقاله	نویسندگان	زمان ارائه
AZ1	ارائه‌ی مدل صوری طرح امضای کور با استفاده از روش استقرایی	نجمه سادات میرامیرخانی حمیدرضا محروقی رسول جلیلی	۱۴ – ۱۴:۲۰
AZ2	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	گمنام‌سازی مسیرهای حرکت اشیا متحرک با سطوح متفاوت حریم خصوصی	سمانه مهدوی‌فر مهدی آبادی محسن کاهانی	۱۴:۴۰ – ۱۵
AZ4	کشف و حذف حمله سیاهچاله جمعی درمسیریابی AODV در شبکه‌های ویژه ادهاک	مهدی مدادیان خسرو فرداد احمد معبادی	۱۵ – ۱۵:۲۰
AZ5	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)

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

Session Chair: Prof Rogaway, Dr. Eghlidos

Present Code	Paper Title	Authors	Present Time
BX1	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	An Improved Attack on A5/1	Vahid Amin Ghafari Javad Mohajeri	10:20 – 10:40
BX3	An Entanglement-based quantum key distribution protocol	Monireh Houshmand Saied Hosseini-khayat	10:40 - 11
BX4	Attacks and Improvement to an RFID Authentication Protocol Conforming to EPC C-1 G-2 Standard	Mohammad Hassan Habibi Mahmud Gardeshi	11 – 11:20
BX5	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	عنوان مقاله	نویسندگان	زمان ارائه
BY1	جستجوی مبتنی بر کلید خصوصی در داده‌های متنی رمزشده	حماد افضلی ننیز بهنام نیکبخت رضا عزمی	۱۰ – ۱۰:۲۰
BY2	روشی کارآ و امن جهت پرس‌وجوی بازه‌ای روی داده رمز شده XML	مریم کریمی رسول جلیلی	۱۰:۲۰ – ۱۰:۴۰
BY3	ارائه‌ی شاخصی امن در پایگاه داده‌های رابطه‌ای رمزشده ی چند کاربره	محسن رضاییان مصطفی حق جو مجید غیوری	۱۰:۴۰ – ۱۱
BY4	ارائه یک فایل سیستم امن مبتنی بر TPM با پشتیبانی گروه	امین سرده مقدم رضا عزمی	۱۱ – ۱۱:۲۰
BY5	شبیه سازی چندسطحی حملات سایبری با شبکه های پتری رنگی به منظور ارزیابی دسترس پذیری	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	عنوان مقاله	نویسندگان	زمان ارائه
BZ1	حمله به یک پروتکل احراز اصالت در سامانه‌های RFID	محمدحسن حبیبی محمود گردشی	۱۰ – ۱۰:۲۰
BZ2	اِعمال کنترل دسترسی نوشتن در سناریوی برونسپاری داده‌ها با استفاده از مدیریت کلید رمزنگاری	سجاد امیدی حمیدرضا شهریاری	۱۰:۲۰ – ۱۰:۴۰
BZ3	تشخیص دستکاری در داده های برچسب RFID با استفاده از نشانه گذاری شکننده	صادق سلیمانی پریسا کاغذگران	۱۰:۴۰ – ۱۱
BZ4	یک مدل اعتماد مبتنی بر شهرت در تور اعتماد	نرجس میرزاپور احمد براآنی	۱۱ – ۱۱:۲۰
BZ5	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

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

Session Chair: Dr. Salmasizade, Dr. Sheikhzadegan

Present Code	Paper Title	Authors	Present Time
CX1	A Secure and Robust Video Watermarking Based on Chaotic Maps	Somayyeh Mohammadi Siamak Talebi Ahmad Hakimi	14 – 14:20
CX2	Watermarking in Farsi binary document images using fractal coding	Fatemeh Daraee Saeed Mozaffari	14:20 – 14:40
CX3	An efficient buyer-seller watermarking protocol based on proxy signatures	Mohammad KazemNasab Haji Ziba Eslami	14:40 - 15
CX4	A Reversible Data Embedding Scheme Based on Search Order Coding for VQ Index Tables	Peyman Rahmani Gholamhossein Dastghaibyfard Ehsan Rahmani	15 – 15:20
CX5	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	عنوان مقاله	نویسندگان	زمان ارائه
CY1	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	روشی برای تشخیص بات‌نت‌ها در مرحله فرمان و کنترل با استفاده از خوشه‌بندی برخط	موسی یحیی‌زاده مهدی آبادی	۱۴:۲۰ – ۱۴:۴۰
CY3	تشخیص نفوذ مبتنی بر ناظر، بر اساس رویکرد سیستم‌های ایمنی مصنوعی	رضا عزمی بشری پیشگو حامد نعمتی	۱۴:۴۰ – ۱۵
CY4	FAPSWPP : یک پروتکل خرید امن کالای الکترونیکی مبتنی بر APSWPP	سمانه لایقیان جوان عباس قائمی بافقی	۱۵ – ۱۵:۲۰
CY5	همبسته سازی 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	عنوان مقاله	نویسندگان	زمان ارائه
CZ1	نهان‌نگاری تهی و نیمه‌شکننده تصاویر دیجیتال با استفاده از استخراج ویژگی در حوزه ویولت و SVM	مینا باقری حبیب الله دانیالی محمدصادق هل‌فروش	۱۴ – ۱۴:۲۰
CZ2	معیار کمّی آسیب‌پذیری شبکه‌های کامپیوتری با استفاده از گراف حمله و سیستم امتیازدهی آسیب‌پذیری	الهه سمیع حمیدرضا شهریاری	۱۴:۲۰ – ۱۴:۴۰
CZ3	ارائه روشی مناسب برای بهبود و توسعه شاخص‌های مدیریت امنیت اطلاعات جهت طراحی و پیاده‌سازی در سازمان‌ها	مجتبی بهرامی	۱۴:۴۰ – ۱۵
CZ4	تحلیل صوری ویژگی وارسی‌پذیری میکس‌نت با استفاده از حساب پی کاربردی	بنیامین تختائی حمیدرضا محروقی رسول جلیلی	۱۵ – ۱۵:۲۰
CZ5	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**