به نام خدا

برنامه زمان‌بندی ارائه شفاهی
هشتمین کنفرانس بین‌المللی انجمن رمز ایران

دانشگاه فردوسی مشهد – ۲۳ و ۲۴ شهریور ۱۳۹۰
http://iscisc2011.um.ac.ir

توضیح ضروری: احتمال تغییر در این برنامه زمانی وجود دارد.

عصر روز اول

عنوان نشست : مبانی رمزشناسی

کد مقاله	عنوان مقاله	نویسندگان
۴۹	خواص عملگر جمع پیمانه ای به هنگ توانی از ۲، از منظر رمزنگاری	سید مجتبی دهنوی اکبر محمودی ریشکانی حمیدرضا میمنی
۳۲۸	تحلیل لغزشی متن منتخب با احتمال ۱	اکبر شاهسواران هادی سلیمانی
۲۸۲	حمله توانی الگو بر روی الگوریتم رمزA5/1	محمد عجمی علی پاینده محمدرضا عارف
۳۱۹	رمزنگاری تصویر با کانتورلت و فوق آشوب	محمدجعفر دهقان مهدی یعقوبی سید علی موسوی احمد رضا دهقان
۳۲۱	یک روش ترکیبی برای رمزنگاری تصویر با استفاده از توابع فوق آشوب و عملگرهای تکاملی	سیدعبدالحمید اصفهانی
۲۹۱	تسریع رمزنگاری تصویر با استفاده از الگوریتم های موازی آشوبی بر روی پردازش گرهای گرافیکی	احسان خان‌میرزا محسن نساجی عبد اله چاله چاله

First Day (Afternoon)

Security of Systems & Applications

Authors	Paper Title	Paper Code
Amir Jalali Bidgoli Behrouz Tork Ladani	Trust Modeling and Verification Using Colored Petri Nets	316
Hassan Shakeri Abbas Ghaemi Bafghi	RTBIMS: Accuracy Enhancement in Iterative Multiplication Strategy for Computing Propagated Trust	149
Hassan Shakeri Abbas Ghaemi Bafghi Hadi Sadoghi Yazdi	Computing Trust Resultant using Intervals	171
Mohammad Mahdi Moghimi Mohammad Saraee	hybrid rule threshold adjustment system for intrusion detection	265
Mohammad Hassan Habibi Mahmud Gardeshi	Attacks and Improvement to an RFID Authentication Protocol Conforming to EPC C-1 G-2 Standard	313
Maryam Mehrnejad Ehsan Toreini Abbas Ghaemi Bafghi	Security Analyzing and Designing GUI with the Resources Model	247

عصر روز اول

عنوان نشست : پروتکل‌های رمزنگاری و امنیتی (۱)

نویسندگان	عنوان مقاله	کد مقاله
نجمه سادات میرامیرخانی حمیدرضا محروقی رسول جلیلی	ارائه‌ی مدل صوری طرح امضای کور با استفاده از روش استقرایی	۳۶۹
رضا هوشمند ترانه اقلیدس محمدرضا عارف	سامانه توأم رمزنگاری متقارن-کدگذاری کانال مبتنی بر کدهای بررسی توازن کم چگال منظم	۳۴۷
سمانه مهدوی‌فر	گمنام‌سازی مسیرهای حرکت اشیا متحرک با سطوح متفاوت حریم	۳۰۷

	خصوصی	مهدی آبادی محسن کاهانی
۹۳	FAPSWPP : یک پروتکل خرید امن کالای الکترونیکی مبتنی بر APSWPP	سمانه لایقیان جوان عباس قائمی بافقی
۱۹۲	همه پخشی و تک پخشی ذاتا امن در شبکه های حسگر بی سیم	حسن نصیرایی بندپی جمشید باقرزاده محمد اهدائی

Second Day (morning)

Fundamentals of Cryptology

Paper Code	Paper Title	Authors
225	On the Period of GSM's A5/1 Stream Cipher and Its Internal State Transition Structure	Vahid Amin Ghaffari Ali Vardasbi
299	An Improved Attack on A5/1	Vahid Amin Ghafari Javad Mohajeri
354	New Color Image Encryption Based on Hyper Chaos	Mohammad Jafar Dehghan Iman Dehghan Ebrahimi AhmadReza Dehghan Mahdi Yaghoobi Saeed Toosizadeh
224	Multiple-Chi-square Tests and Their Application on Distinguishing Attacks	Ali Vardasbi Mahmoud Salmasizadeh Javad Mohajeri
210	An Entanglement-based quantum key distribution protocol	Monireh Houshmand Saied Hosseini-khayat

صبح روز دوم

عنوان نشست : امنیت سیستم‌ها و کاربردها (۱)

کد مقاله	عنوان مقاله	نویسندگان
۳۸۰	جستجوی مبتنی بر کلید خصوصی در داده‌های متنی رمزشده	حماد افضلی ننیز بهنام نیکبخت علیرضا عزمی
۱۸۱	روشی کارآ و امن جهت پرس‌وجوی بازه‌ای روی داده رمز شده XML	مریم کریمی رسول جلیلی
۲۶۰	ارائه‌ی شاخصی امن در پایگاه داده‌های رابطه‌ای رمزشده ی چند کاربره	محسن رضاییان مصطفی حق جو مجید غیوری
۱۷۴	ارائه یک فایل سیستم امن مبتنی بر TPM با پشتیبانی گروه	امین سرده مقدم رضا عزمی
۶۶	شبیه سازی چندسطحی حملات سایبری با شبکه های پتری رنگی به منظور ارزیابی دسترس پذیری	مهرداد آشتیانی محمد عبدالهی ازگمی

صبح روز دوم

عنوان نشست : پروتکل‌های رمزنگاری و امنیتی (۲)

کد مقاله	عنوان مقاله	نویسندگان
۳۶۸	اِعمال کنترل دسترسی نوشتن در سناریوی برونسپاری داده‌ها با استفاده از مدیریت کلید رمزنگاری	سجاد امیدی حمیدرضا شهریاری
۲۷۱	حمله به یک پروتکل احراز اصالت در سامانه‌های RFID	محمد حسن حبیبی محمود گردشی
۳۶۷	تشخیص دستکاری در داده های برچسب RFID با استفاده از نشانه گذاری شکننده	صادق سلیمانی پریسا کاغذگران
۳۷۷	یک مدل اعتماد مبتنی بر شهرت در تور اعتماد	نرجس میرزاپور

		احمد براآنی
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

Second Day (afternoon)

Information Hiding

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

عصر روز دوم

عنوان نشست : امنیت سیستم‌ها و کاربردها (۲)

کد مقاله	عنوان مقاله	نویسندگان
۱۹۱	رویکردی ترکیبی مبتنی بر الگوریتم‌های انتخاب منفی و کلونی زنبورهای مصنوعی برای تشخیص ناهنجاری در شبکه‌های اقتضایی متحرک	فاطمه بارانی برواتی مهدی آبادی
۳۷۲	روشی برای تشخیص باتنت‌ها در مرحله فرمان و کنترل با استفاده از خوشه‌بندی برخط	موسی یحیی‌زاده مهدی آبادی
۴۰۳	تشخیص نفوذ مبتنی بر ناظر، بر اساس رویکرد سیستم‌های ایمنی مصنوعی	رضا عزمی بشری پیشگو

		حامد نعمتی
۲۲۲	کشف و حذف حمله سیاهچاله جمعی درمسیریابی AODV در شبکه های ویژه ادهاک	مهدی مدادیان خسرو فرداد احمد معبادی
۱۲	همبسته سازی هشدارها در یک سیستم تشخیص نفوذ بر اساس سیستم ایمنی مصنوعی	مهدی باطنی احمد براآنی دستجردی

عصر روز دوم

عنوان نشست : مهندسی و مدیریت امنیت

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