

This file has been cleaned of potential threats.

If you confirm that the file is coming from a trusted source, you can send the following SHA-256 hash value to your admin for the original file.

8d2e835c3357b97956d2b456ddb5719d877adaa9f7d9c6f88b14d4f7f237f570

To view the reconstructed contents, please SCROLL DOWN to next page.

In The Name of God

Technical Program

8th International ISC Conference

on Information Security and Cryptology (ISCISC'11)

September 14-15, 2011 - Ferdowsi University of Mashhad

<http://iscisc2011.um.ac.ir>

عصر روز اول

عنوان نشست : مبانی رمزشناسی

نویسندگان	عنوان مقاله	کد مقاله
سید مجتبی دهنوی اکبر محمودی ریشکانی حمیدرضا میمنی	خواص عملگر جمع پیمانان ای به هنگ توانی از ۲، از منظر رمزنگاری	۴۹
اکبر شاهسواران هادی سلیمانی	تحلیل لغزشی متن منتخب با احتمال ۱	۳۲۸
محمد عجمی علی پاینده محمد رضا عارف	حمله توانی الگو بر روی الگوریتم رمز A5/1	۲۸۲
محمد جعفر دهقان مهدی یعقوبی سید علی موسوی احمد رضا دهقان	رمزنگاری تصویر با کانتورلت و فوق آشوب	۳۱۹
سید عبدالحمید اصفهانی	یک روش ترکیبی برای رمزنگاری تصویر با استفاده از توابع فوق آشوب و عملگرهای تکاملی	۳۲۱
احسان خان میرزا محسن نساجی عبداله چاله چاله	تسریع رمزنگاری تصویر با استفاده از الگوریتم های موازی آشوبی بر روی پردازش گرافیکی	۲۹۱

First Day (Afternoon)

Security of Systems & Applications

Authors	Paper Title	Paper Code
Amir Jalali Bidgoli Behrouz TorkLadani	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 محمد رضا عارف	سامانه توأم رمزنگاری متقارن-کدگذاری کانال مبتنی بر کدهای بررسی توازن کم چگال منظم	۳۴۷
سمانه مهدوی فر	گمنام‌سازی مسیرهای حرکت اشیا متحرک با سطوح متفاوت حریم	۳۰۷

مهدي آبادي محسن كاهاني	خصوصي	
سمانه لايقيان جوان عباس قائمي بافقي	FAPSWPP : يك پروتكل خريد امن كالاي الكترونيكي مبتني بر APSWPP	۹۳
حسن نصيرايي بنديبي جمشيد باقرزاده محمد اهدائي	همه پخشي و تك پخشي ذاتا امن در شبكه هاي حسگر بي سيم	۱۹۲

Second Day (morning)

Fundamentals of Cryptology

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

صبح روز دوم

عنوان نشست : امنیت سیستم‌ها و کاربردها (۱)

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

صبح روز دوم

عنوان نشست : پروتکل‌های رمزنگاری و امنیتی (۲)

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

احمد برآنی		
رضا عزمی معصومه کردیان	مدل اعتماد مبتنی بر شهرت در اجتماعات تجارت الکترونیک همتا به همتا با قابلیت تشخیص و مقابله با حملات بدخواهان	۳۱۷

Second Day (afternoon)

Information Hiding

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

عصر روز دوم

عنوان نشست : امنیت سیستمها و کاربردها (۲)

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

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

عصر روز دوم

عنوان نشست : مهندسی و مدیریت امنیت

نویسندگان	عنوان مقاله	کد مقاله
الهه سمیع حمیدرضا شهرباری	معیار کمی آسیب پذیری شبکه های کامپیوتری با استفاده از گراف حمله و سیستم امتیازدهی آسیب پذیری	۲۶۲
مجتبی بهرامی	ارائه روشی مناسب برای بهبود و توسعه شاخص های مدیریت امنیت اطلاعات جهت طراحی و پیاده سازی در سازمان ها	۱۶۷
بنیامین تختائی حمیدرضا محروقی رسول جلیلی	تحلیل صوری ویژگی واریسی پذیری میکسنت با استفاده از حساب پی کاربردی	۳۶۲
مریم مهرنژاد عباس قائمی بافقی احد هراتی احسان تورینی	آزمون تصویری بازشناسی انسان از ماشین مبتنی بر تبدیلات هندسی	۲۸۵
مینا باقری حبیب الله دانیالی	نهان نگاری تھی و نیمه شکننده تصاویر دیجیتال با استفاده از استخراج ویژگی در حوزه ویولت و SVM	۳۷۵