برنامه زمان‌بندی ارائه مقالات

چهارشنبه ۱۷ شهریورماه ۱۳۹۵، ساعت ۱۳:۴۵ الی ۱۵:۱۵، سالن شیخ بهایی		
نشست ۱: مبانی رمزشناسی ۱		
روسای نشست	خانم دکتر ترانه اقلیدس	دانشگاه صنعتی شریف
	خانم دکتر زیبا اسلامی	دانشگاه شهید بهشتی

Session Speech (13:45-14:05)
Public Key Encryption with Keyword Search and Keyword Guessing Attack
Dr. Nasrollah Pakniat

Paper No. 1570282127 (14:05-14:25)
Biclique Cryptanalysis of Twine-128
Seyed Reza Hoseini Najarkolaei; Mohammad Zare Ahangarkolaei; Siavash Ahmadi; Mohammad Reza Aref

Paper No. 1570282198 (14:25-14:45)
FMNV Continuous Non-malleable Encoding Scheme is More Efficient Than Believed
Seyyed Amir Mortazavi; Mahmoud Salmasizadeh; Amir Daneshgar

چهارشنبه ۱۷ شهریورماه ۱۳۹۵، ساعت ۱۳:۴۵ الی ۱۵:۱۵، سالن علامه طباطبایی	
نشست ۲: پروتکل‌های امنیتی	
روسای نشست	خانم دکتر مهتاب میرمحسنی دانشگاه صنعتی شریف خانم دکتر فرخ لقا معظمی دانشگاه شهید بهشتی

Session Speech (13:45-14:05)
Typing Authentication Protocols in the Presence of Compromised Principals
Dr. Behnam Sattarzadeh

Session Speech (14:05-14:25)
How to Protect a Distance Bounding Protocol against a Terrorist Fraud Attack?
Dr. Hoda Jannati

Paper No. 1570282260 (14:25-14:45)
PapiaPass: Sentence-based Passwords Using Dependency Trees
Habibollah Yajam; Younes Karimi Ahmadabadi; Mohammad Ali Akhaee

Paper No. 1570284630 (14:45-15:05)
An Improved Certificateless Signcryption Scheme
Parvin Rastegari; Mehdi Berenjkoub

پنجشنبه ۱۸ شهریورماه ۱۳۹۵، ساعت ۰۸:۳۰ الی ۱۰:۱۵، سالن شیخ بهایی		
نشست ۳: مبانی رمز شناسی ۲		
روسای نشست	دکتر محمود سلماسی زاده	دانشگاه صنعتی شریف
	دکتر عبدالرسول میرقدری	دانشگاه امام حسین (ع)

Session Speech (08:30-08:50)
On the Indifferentiability of Hash Functions
Dr. Nasour Bagheri

Session Speech (08:50-09:10)
Code based Cryptography as a Post Quantum Cryptography Candidate
Dr. Masoumeh Koochak Shooshtari

Paper No. 1570281942 (09:10-09:30)
A Secret Key Encryption Scheme Based on 1-Level QC-LDPC Lattices
Khadijeh Bagheri; Mohammad-Reza Sadeghi; Taraneh Eghlidos; Daniel Panario

کد مقاله: ۱۵۷۰۲۸۲۲۶۳ (۰۹:۵۰ – ۰۹:۳۰)
ثبات های انتقالی کلاک کنترلی با دوره تناوب اثبات پذیر
اکبر محمودی ریشکانی، سید مجتبی دهنوی، محمدرضا میرزایی شمس آباد

پنجشنبه ۱۸ شهریورماه ۱۳۹۵، ساعت ۰۸:۳۰ الی ۱۰:۱۵، سالن علامه طباطبایی		
نشست ۴: نهان‌سازی اطلاعات + مهندسی امنیت		
روسای نشست	دکتر مهدی خرازی	دانشگاه صنعتی شریف
	دکتر محسن ابراهیمی مقدم	دانشگاه شهید بهشتی

Paper No. 1570282116 (08:30-08:50)
Feature Extraction for Detection of Watermarking Algorithm
Zahra Hatefi; Mojtaba Mahdavi; Pegah Nikbakht

Paper No. 1570282322 (08:50-09:10)
Video Watermarking in the DT-CWT Domain Using Hyperbolic Function
Milad Ghalejughi; Mohammad Ali Akhaee

Paper No. 1570285918 (09:10-09:30)
Spread Spectrum Watermarking Robust to SILK Vocoder
Ali Sattari; Mohammad Ali Akhaee

کد مقاله: ۱۵۷۰۲۸۴۴۳۴ (۰۹:۵۰ – ۰۹:۳۰)
پیشنهاد مدل تعالی برای مدیریت امنیت اطلاعات در سازمان ها
صدیقه اولین چهارسوقی، بهنام رفیعی مهر، حمیدرضا عطاییان، زینب کاموسی، حبیب رستمی

سیزدهمین کنفرانس بین المللی انجمن رمز ایران
۱۷ الی ۱۸ شهریورماه ۱۳۹۵، دانشگاه شهید بهشتی
13th International ISC Conference on
Information Security and Cryptology (ISCISC2016)
September 7-8, 2016; Shahid Beheshti University – Tehran

پنجشنبه ۱۸ شهریورماه ۱۳۹۵، ساعت ۰۸:۳۰ الی ۱۰:۱۵، سالن خوارزمی	
نشست ۵: پیاده‌سازی الگوریتم‌های رمزنگاری	
روسای نشست	دکتر مرتضی صاحب‌الزمانی — دانشگاه صنعتی امیرکبیر دکتر بیژن علیزاده — دانشگاه تهران

Session Speech (08:30-08:50)
An Analytical Approach to Trust-Driven Placement
Dr. Seyed Mohammad Hossein Shekarian

Paper No. 1570282117 (08:50-09:10)
A New CPA Resistant Software Implementation for Symmetric Ciphers with Smoothed Power Consumption
Morteza Safaeipour; Mahmoud Salmasizadeh

کد مقاله: ۱۵۷۰۲۸۲۲۰۴ (۰۹:۳۰ – ۰۹:۱۰)

پیاده‌سازی بهینه‌ی نرم‌افزاری الگوریتم رمزنگاری احراز اصالت شده‌ی AEGIS

محسن رضایی، رضا ابراهیمی آتانی

پنجشنبه ۱۸ شهریورماه ۱۳۹۵، ساعت ۱۳:۴۵ الی ۱۵:۳۰، سالن علامه طباطبایی		
نشست ۶: امنیت شبکه		
روسای نشست	دکتر مقصود عباسپور	دانشگاه شهید بهشتی
	خانم دکتر زهرا احمدیان	دانشگاه شهید بهشتی

Session Speech (13:45-14:05)
Smart Grid Security Challenges
Dr. Majid Bayat

Paper No. 1570281977 (14:05-14:25)
XABA: A Zero-Knowledge Anomaly-Based Behavioral Analysis Method to Detect Insider Threats
Abolfazl Zargar; Alireza Nowroozi; Rasool Jalili

کد مقاله: ۱۵۷۰۲۸۲۰۸۹ (۱۴:۴۵ – ۱۴:۲۵)
روتبن: تشخیص ترافیک فرمان و کنترل بات‌های نظیر به نظیر با ترکیب اطلاعات میزبان و شبکه
احمدرضا اسکندری، علیرضا نوروزی

کد مقاله: ۱۵۷۰۲۸۲۰۹۶ (۱۵:۰۵ – ۱۴:۴۵)
تشخیص نفوذ مبتنی بر جریان بر اساس خوشه‌بندی گراف پراکندگی ترافیک
رویا راستگار، آیاز عیسی زاده، جابر کریم پور

کد مقاله: ۱۵۷۰۲۸۲۲۷۵ (۱۵:۲۵ – ۱۵:۰۵)
استخراج ساختار پیام های ارسالی توسط برنامه های کاربردی شبکه
نیره مومنیان، محسن احمدی، بهروز ترک لادانی

پنجشنبه ۱۸ شهریورماه ۱۳۹۵، ساعت ۱۳:۴۵ الی ۱۵:۳۰، سالن شیخ بهایی		
نشست ۷: امنیت رایانش		
روسای نشست	دکتر عباس قائمی بافقی	دانشگاه فردوسی مشهد
	دکتر بهروز ترک لادانی	دانشگاه اصفهان

Session Speech (13:45-14:05)
Privacy Engineering
Dr. Sadegh Dorri Nogoorani

Paper No. 1570282245 (14:05-14:25)
Fine-Grained Access Control for Hybrid Mobile Applications in Android Using Restricted Paths
Shahrooz Pooryousef; Morteza Amini

کد مقاله: ۱۵۷۰۲۸۲۲۲۸ (۱۴:۴۵ – ۱۴:۲۵)
روشی برای کشف جریان های اطلاعاتی در نرم افزار به منظور تشخیص آسیب پذیری تزریق نویسه ذخیره شده از طریق وب گاه
حامد سلیمانی، محمدعلی هادوی، حسن مختاری سنگچی

چهارشنبه ۱۷ شهریورماه ۱۳۹۵، ساعت ۱۷:۳۰ الی ۱۸:۳۰، لابی گلبرگ ۱

نشست پوستر ۱

Paper No. 1570281511
Construction of New S-boxes Via Permuting the Inverse Mapping on Special Subsets
Mojtaba Dehnavi; Mohammadreza Mirzaee Shamsabad; Akbar Mahmoodi Rishakani

Paper No. 1570281848
An Identity-Based Digital Signature Scheme to Detect Pollution Attacks in Intra-Session Network Coding
Sogand SadrHaghighi; Siavash Khorsandi

Paper No. 1570282148
A New Lightweight Authenticated Key Exchange Protocol for Internet of Things
Sima Arasteh; Seyed Farhad Aghili; Hamid Mala

Paper No. 1570282168
Preserving Privacy in Location Based Mobile Coupon Systems Using Anonymous Authentication Scheme
Mohsen Ahmadi; Behrooz Shahgholi Ghahfarokhi

Paper No. 1570282186
Zero Correlation Linear Attack on Reduced Round Piccolo-80
Mohammad Zare Ahangarkolaei; Seyed Reza Hoseini Najarkolaei; Siavash Ahmadi; Mohammad Reza Aref

چهارشنبه ۱۷ شهریورماه ۱۳۹۵، ساعت ۱۷:۳۰ الی ۱۸:۳۰، لابی گلبرگ ۱

نشست پوستر ۱

کد مقاله: ۱۵۷۰۲۸۲۱۱۵

تشخیص بدون نظارت بات نت های نظیر به نظیر، بر اساس رویکرد سیستمهای ایمنی مصنوعی

حامد شجاعی یاس، رضا عزمی، محمدامین عراقی زاده

کد مقاله: ۱۵۷۰۲۸۲۱۵۰

تشخیص حملات خاص شبکه سلولی موبایل با استفاده از رویکرد همبسته سازی هشدارها

حسین امینی، علیرضا نوروزی، رسول جلیلی

کد مقاله: ۱۵۷۰۲۸۲۲۱۹

تحلیل یک پروتکل امن اشتراک گذاری داده (SeDS) جدید در ارتباطات D2D مبتنی بر شبکه های LTE-A

امیرحسین آداوودی جلفائی، عاطفه محسنی اژیه، مائده عاشوری تلوکی، سید فرهاد عقیلی

کد مقاله: ۱۵۷۰۲۸۲۲۳۹

مدل اعتماد پویا و آگاه از کیفیت سرویس برای مسیریابی در شبکه MANET

محبوبه مدبر عزیزی، عباس قائمی بافقی

پنجشنبه ۱۸ شهریورماه ۱۳۹۵، ساعت ۱۳:۴۵ الی ۱۵:۳۰، لابی گلبرگ ۱

نشست پوستر ۲

Paper No. 1570281931
Counterfeiting Attack on Adjusted Expanded-bit Multiscale Quantization-based Semi-fragile Watermarking Technique
Samira Hosseini; Mojtaba Mahdavi

Paper No. 1570282205
2entFOX: A Framework for High Survivable Ransomwares Detection
Mohammad Mehdi Ahmadian; Hamid Reza Shahriari

Paper No. 1570282373
Security Improvement of FPGA Configuration File Against the Reverse Engineering Attack
Sharareh ZamanZadeh; Shahram Shahabi; Ali Jahanian

Paper No. 1570284633
A New Approach for Effective Malware Detection in Android-based Devices
Mahmood Deypir

کد مقاله: ۱۵۷۰۲۸۱۲۹۰

پیاده سازی روشی جدید مبتنی بر SLSB جهت ارتقاء امنیت الگوریتم نهان نگاریLSB

سیده فاطمه هاشمی طبالوندانی، جواد شیخ زادگان، علی محمد نوروز زاده گیل ملک

پنجشنبه ۱۸ شهریورماه ۱۳۹۵، ساعت ۱۳:۴۵ الی ۱۵:۳۰، لابی گلبرگ ۱
نشست پوستر ۲

کد مقاله: ۱۵۷۰۲۸۱۴۹۸

ارائه یک الگوریتم مقاوم نشان گذاری تصویر دیجیتال در فضای رنگی YCoCg-R با استفاده از الگوریتم ژنتیک و ارتباط ضرایب DCT

محمد موسی زاده، غلامحسین اکباتانی فرد

کد مقاله: ۱۵۷۰۲۸۲۲۱۵

طراحی و پیاده سازی الگوریتم RC5 با مسیرداده ۸ بیتی به منظور دست یابی به سربار سخت افزاری کمینه

یحیی ارزانی بیرگانی، سمیه تیمارچی

کد مقاله: ۱۵۷۰۲۸۲۲۳۸

نهان نگاری کور مقاوم در برابر حملات هندسی مبتنی بر شناسایی مختصات نقاط ویژگی SURF

پگاه قدک، کریم فائز

کد مقاله: ۱۵۷۰۲۸۲۲۹۶

نشان گذاری سیگنال صدا بر اساس تغییر در دامنه ضرایب تبدیل فوریه سریع با قابلیت کور و همزمان سازی

مهدی جیحون، محمد عسگری، لیلی احسان

سیزدهمین کنفرانس بین المللی انجمن رمز ایران
۱۷ الی ۱۸ شهریورماه ۱۳۹۵، دانشگاه شهید بهشتی
13th International ISC Conference on
Information Security and Cryptology (ISCISC2016)
September 7-8, 2016; Shahid Beheshti University – Tehran

پنجشنبه ۱۸ شهریورماه ۱۳۹۵، ساعت ۱۳:۴۵ الی ۱۵:۳۰، لابی گلبرگ ۱
نشست پوستر ۲

کد مقاله: ۱۵۷۰۲۸۴۷۳۷

پیاده سازی مقاوم الگوریتم RSA در مقابل حمله کانال جانبی تحلیل توان با استفاده از محاسبات نامتعارف

سعید گرگین، حسین کریمی خوشرو