زیبا

اسلامی

شماره تماس: ۲۹۹۰۳۰۰۷
رایانامه: Z_Eslami@sbu.ac.ir
وب سایت: http://facultymembers.sbu.ac.ir/eslami
پروفایل علم سنجی: http://scimet.sbu.ac.ir/Ziba_Eslami

علوم ریاضی / علوم داده ها و کامپیوتر

تحصیلات

■ کارشناسی: دانشگاه تهران، ریاضی کاربردی، ۱۳۶۲←۱۳۶۶

■ کارشناسی ارشد: دانشگاه تهران، ریاضی کاربردی، ۱۳۷۱←۱۳۷۴

■ دکتری: دانشگاه تهران، ریاضی – کاربردی، ۱۳۷۴←۱۳۷۸

علایق پژوهشی

■ مبانی نظری و همچنین پروتکلهای رمزنگاری

فعالیت‌های اجرایی

■ عضو هیات تحریریه نشریه کد، رمز و امنیت سایبری، ۱۳۹۶←تا زمان حال

■ ادیتور مهمان برای شماره ویژه مجله در حوزه تخصصی، ۱۳۹۵←۱۳۹۶

■ معاون آموزشی پژوهشکده فضای مجازی، ۱۳۹۵←۱۳۹۷

■ سرپرست معاون آموزشی پژوهشکده فضای مجازی، ۱۳۹۴←۱۳۹۵

■ سرپرست گروه پژوهشی رمز و امنیت شبکه، ۱۳۹۲←۱۳۹۶

■ فرصت مطالعاتی، ۱۳۹۱←۱۳۹۲

■ استاد راهنما، ۱۳۹۰←۱۳۹۱

کتب

■ نظریه کذاری

زیبا اسلامی

دانشگاه شهیدبهشتی – تهران، ایران، ۱۳۸۷، شابک: ۹۴۶–۴۵۷–۱۴۹–۵

ارتباط با صنعت

■ تحقیق و امکان سنجی، پیاده سازی و تحلیل یک الگوریتم رمز قالبی اختصاصی

۱۳۹۷

مقالات علمی چاپ شده در مجلات

■ Certificate-based authenticated encryption with keyword search: Enhanced security model and a concrete construction for Internet of Things
Danial Shiraly, Ziba Eslami, Nasrollah Pakniat
Journal of Information Security and Applications, Vol.80, pp. 103683-103693, 2024

■ An Efficient Ramp Secret Sharing Scheme Based on Zigzag-Decodable Codes
saeideh Kabirirad, Sorour Sheidani, Ziba Eslami
Journal of Computer and Knowledge Engineering, Vol.6, pp. 15-24, 2023

■ Designated-Server Hierarchical Searchable Encryption in Identity-Based Setting
Danial Shiraly, Nasrollah Pakniat, Ziba Eslami
ISeCure-ISC International Journal of Information Security, Vol.15, pp. 1-16, 2023

■ A generic construction to build simple oblivious transfer protocols from homomorphic encryption schemes
Saeid Esmaeilzade, Nasrollah Pakniat, Ziba Eslami
JOURNAL OF SUPERCOMPUTING, Vol.78, pp. 72-92, 2022

■ Pairing-free certificateless authenticated encryption with keyword search
Danial Shiraly, Nasrollah Pakniat, Mahnaz Noroozi, Ziba Eslami
JOURNAL OF SYSTEMS ARCHITECTURE, Vol.124, 2022

■ Public key encryption with distributed keyword search
Ziba Eslami, Mahnaz Noroozi, Kobra Amirizirtol
JOURNAL OF DISCRETE MATHEMATICAL SCIENCES & CRYPTOGRAPHY, pp. 1-25, 2021

■ Blind multipurpose image watermarking with perfect security
Sorour Sheidani, Ziba Eslami
ISeCure-ISC International Journal of Information Security, Vol.13, pp. 145-156, 2021

■ CPA-Secure Privacy-Preserving Reversible Data Hiding for JPEG Images
Sorour Sheidani, Ahmad Mahmoudi-Aznaveh, Ziba Eslami
IEEE Transactions on Information Forensics and Security, Vol.16, pp. 3647-3661, 2021

■ Blind multipurpose watermarking with insertion of a single watermark: a generic construction based on verifiable threshold secret sharing
Sorour Sheidani, Ziba Eslami
IET Image Processing, Vol.14, pp. 4766-4773, 2020

■ Public-key encryption with keyword search: a generic construction secure against online and offline keyword guessing attacks
Mahnaz Noroozi, Ziba Eslami
Journal of Ambient Intelligence and Humanized Computing, Vol.11, pp. 879-890, 2020

■ Cryptanalysis and improvement of a group RFID authentication protocol
Nasrollah Pakniat, Ziba Eslami
WIRELESS NETWORKS, Vol.26, pp. 3363-3372, 2020

■ Certificateless authenticated encryption with keyword search: Enhanced security model and a concrete construction for industrial IoT
Nasrollah Pakniat, Danial Shiraly, Ziba Eslami
Journal of Information Security and Applications, Vol.53, 2020

■ Improvement of (n, n)-multi-secret image sharing schemes based on Boolean operations

Saeideh Kabirirad, Ziba Eslami
Journal of Information Security and Applications, Vol.47, pp. 16-27, 2019

■ High-speed GPU implementation of a secret sharing scheme based on cellular automata
Saeideh Kabirirad, Mahmood Fazlali, Ziba Eslami
JOURNAL OF SUPERCOMPUTING, Vol.75, pp. 7314-7336, 2019

■ On the Security of a Privacy-Preserving Ranked Multi-Keyword Search Scheme
Ziba Eslami, Mahnaz Noroozi, joonsang baek
Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol.10, pp. 75-85, 2019

■ Public key authenticated encryption with keyword search: revisited
Mahnaz Noroozi, Ziba Eslami
IET Information Security, Vol.13, pp. 336-342, 2019

■ A verifiable threshold secret sharing scheme based on lattices
Bahman Rajabi Kafshgar, Ziba Eslami
INFORMATION SCIENCES, pp. 655-661, 2019

■ Comments on a chaos-based public key encryption with keyword search scheme
Mahnaz Noroozi, Ziba Eslami, Nasrollah Pakniat
NONLINEAR DYNAMICS, Vol.94, pp. 1127-1132, 2018

■ Designing a secure designated server identity-based encryption with keyword search scheme: still unsolved
Mahnaz Noroozi, Iman Karoobi, Ziba Eslami
Annals of Telecommunications, Vol.73, pp. 769-776, 2018

■ A (t,n) -multi secret image sharing scheme based on Boolean operations
Saeideh Kabirirad, Ziba Eslami
JOURNAL OF VISUAL COMMUNICATION AND IMAGE REPRESENTATION, Vol.57, pp. 39-47, 2018

■ A CCA2-Secure Incomparable Public Key Encryption Scheme
Bahman Rajabi Kafshgar, Ziba Eslami
Journal of Computing and Security, Vol.3, pp. 3-12, 2017

■ Cryptanalysis of a multiparty quantum key agreement protocol based on commutative encryption
Razieh Mohajer, Ziba Eslami
Quantum Information Processing, Vol.16, pp. 1-9, 2017

■ Verifiable Social Multi-Secret Sharing Secure in Active Adversarial
Nasrollah pakniat, Ziba Eslami
Journal of Computing and Security, Vol.4, pp. 3-12, 2017

■ Provably Secure Group Key Exchange Protocol in the Presence of Dishonest Insiders
Ziba Eslami, Mahnaz Noroozi, Saeideh Kabirirad
International Journal of Network Security, Vol.18, pp. 33-42, 2016

■ Reducing multi-secret sharing problem to sharing a single secret based on cellular automata
Nasrollah Pakniat, Mahnaz Noroozi, Ziba Eslami
the csi journal of computer science and engineering, Vol.14, pp. 38-43, 2016

■ Ideal social secret sharing using Birkhoff interpolation method
Ziba Eslami, Nasrollah Pakniyat, mehrdad nojoumian
Security and Communication Networks, Vol.9, pp. 4973-4982, 2016

■ Distributed key generation protocol with hierarchical threshold access structure
Nasrollah Pakniyat, Mahnaz Noroozi, Ziba Eslami
IET Information Security, pp. 1-8, 2015

■ Algorithmic Aspects of Trades
Ziba Eslami
ARS COMBINATORIA, Vol.120, pp. 245-253, 2015

■ A note on Selling multiple secrets to a single buyer
Nasrollah Pakniyat, Ziba Eslami, Ali Miri
INFORMATION SCIENCES, Vol.279, pp. 889-892, 2014

■ Secret image sharing scheme with hierarchical threshold access structure
Nasrollah Pakniyat, Mahnaz Noroozi, Ziba Eslami
JOURNAL OF VISUAL COMMUNICATION AND IMAGE REPRESENTATION, Vol.25, pp. 1093-1101, 2014

■ Proxy signatures and buyer seller watermarking protocols for the protection of multimedia content
Ziba Eslami, Mohammad Kazem Nasab Haji, Narges Mirehi
MULTIMEDIA TOOLS AND APPLICATIONS, Vol.72, pp. 2723-2740, 2014

■ Cryptanalysis of an Attribute-based Key Agreement Protocol
Ziba Eslami, Nasrollah Pakniat, Mahnaz Noroozi
international journal of computer and information technologies, Vol.2, pp. 351-358, 2014

■ Certificateless aggregate signcryption Security model and a concrete construction secure in the random oracle model
Ziba Eslami, Nasrollah Pakniyat
journal of king university-computer and information sciences, Vol.26, pp. 276-286, 2014

■ An authenticated image encryption scheme based on chaotic maps and memory cellular automata
Atieh Bakhshandeh Kapoorchali, Ziba Eslami
OPTICS AND LASERS IN ENGINEERING, pp. 665-673, 2013

■ An improvement over an image encryption method based on total shuffling
Ziba Eslami, Atieh Bakhshandeh Kapoorchali
OPTICS COMMUNICATIONS, pp. 51-55, 2013

■ A new verifiable multi-secret sharing scheme based on bilinear maps
Ziba Eslami, Saeedeh Kabirirad
WIRELESS PERSONAL COMMUNICATIONS, pp. 459-467, 2012

■ Data security in unattended wireless sensor networks through aggregate signcryption
Faezeh Sadat Babamir, Ziba Eslami
KSII Transactions on Internet and Information Systems, Vol.6, pp. 2940-2955, 2012

■ SECRET IMAGE SHARING BASED ON CELLULAR AUTOMATA AND STEGANOGRAPHY
Ziba Eslami, Seyyed Hossein Razzaghi, Jamal Zarepour Ahmadabadi
PATTERN RECOGNITION, Vol.43, pp. 397-404, 2011

■ a proxy e- raffle protocol based on proxy signatures
Nasrollah Pakniyat, Ziba Eslami
Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol.2, pp. 74-84, 2011

■ A new untraceable off-line electronic cash system
mehdi talebi, Ziba Eslami
Electronic Commerce Research and Applications, Vol.10, pp. 59-66, 2011

■ Secret image sharing with authentication-chaining and dynamic embedding
Ziba Eslami, Jamal Zarepour Ahmadabadi
JOURNAL OF SYSTEMS AND SOFTWARE, Vol.84, pp. 803-809, 2011

■ A verifiable multi-secret sharing scheme based on cellular automata
Ziba Eslami, Jamal Zarepour Ahmadabadi
INFORMATION SCIENCES, Vol.180, pp. 2889-2894, 2010

■ On the possible automorphisms of a 3-(16 7 5) design
Ziba Eslami
ARS COMBINATORIA, Vol.95, pp. 217-224, 2010

■ Another security weakness in an authenticated group key agreement
Ziba Eslami, Saeideh Kabirirad

Journal of Internet Technology, Vol.11, pp. 573-576, 2010

■ Classification of trades by large sets
Ziba Eslami
ARS COMBINATORIA, Vol.82, 2007

■ Classification of Designs with nontrivial Automorphism groups
Ziba Eslami
JOURNAL OF COMBINATORIAL DESIGNS, pp. 479-489, 2006

■ Some New 4-Designs
Ziba Eslami, G.B Khosro Shahi, M.M Noori, B Tayfeh Rezaiie
ARS COMBINATORIA, pp. 225-229, 2004

■ Enumeration of t-Designs Through Intserction Matrices
Ziba Eslami, G.B Khosro Shahi, M.M Noori
DESIGNS CODES AND CRYPTOGRAPHY, pp. 185-191, 2004

■ LS 7 (3 5 11)Exists
Ziba Eslami
JOURNAL OF COMBINATORIAL DESIGNS, pp. 312-316, 2003

■ On the indecomposable partition problem Ipp(10)
Ziba Eslami
DISCRETE MATHEMATICS, pp. 255-264, 2002

■ Some New 6-(14 7 4)Designs
Ziba Eslami, G.B Khosro Shahi
JOURNAL OF COMBINATORIAL THEORY SERIES A, pp. 141-152, 2001

■ On Classification of 2(8 3)and 2-(9 3)Trades
Ziba Eslami, G.B Khosro Shahi, B Tayfeh Rezaiie
Journal of Combinatorial Mathematics and Combinatorial Computing, pp. 231-242, 2001

■ On Halvings of The 2-(10 3 8) Design
Ziba Eslami, G.B Khosro Shahi, B Tayfeh Rezaiie
JOURNAL OF STATISTICAL PLANNING AND INFERENCE, pp. 411-419, 2000

■ Classification of Some Large Sets and Designs
Ziba Eslami, G.B Khosro Shahi
JOURNAL OF GEOMETRIC ANALYSIS, pp. 105-110, 2000

■ A Complete Classification of 3-(11 4 4) Designs with nontrivial automorphism group
Ziba Eslami, G.B Khosro Shahi
JOURNAL OF COMBINATORIAL DESIGNS, pp. 419-425, 2000

■ On 2-(v 3)Trades of Minimum Volume
Ziba Eslami, B Tayfeh Rezaiie
Australasian Journal of Combinatorics, pp. 239-245, 1999

■ تحلیل امنیت و بهبود یک سامانه حمل ونقل هوشمند مبتنی بر امضای تجمعی فاقد گواهینامه
نصرالله پاک نیت، زیبا اسلامی
پدافند الکترونیکی و سایبری، نسخه ۸، صفحات: ۲۵-۳۳، ۱۳۹۸

مقالات علمی ارائه شده در همایش‌ها

■ Forgery attack on an outsourced attribute-based signature scheme
saideh kabiri rad, Ziba Eslami
27th international computer conference

■ Accelerating Robust Watermarking through Parallelization
Sorour Sheidani, Mahmood Fazlali, Ziba Eslami
CSICC 2020, pp.1-6

■ A Block-Based Image Encryption Scheme UsingCellular AutomataWith Authentication Capability
Ziba Eslami, Saeideh Kabirirad
THIRD INTERNATIONAL CONFERENCE OF MATHEMATICAL SCIENCES (ICMS 2019)

■ Quantum Secret Sharing using single states
Razieh Mohajer, Ziba Eslami
8th International Symposium on Telecommunictions

■ issuer-free oblivious transfer with threshold access control policy
PARISA MOMENI, Ziba Eslami
2nd international conference on knowledge-base engineering and innovation

■ proactive multi-secret sharing scheme
Davood Faramarzi Filabadi, Ziba Eslami
2nd international conference on knowledge-base engineering and innovation

■ multi-user searchable encryption scheme with general access structure
Kobra Amirizirtol, Mahnaz Noroozi, Ziba Eslami
2nd international conference on knowledge-base engineering and innovation

■ social multi-secret sharing scheme
Abdolkarim Mohammadi, Ziba Eslami
2nd international conference on knowledge-base engineering and innovation

■ Hierarchical Threshold Multi-Secret Sharing Scheme Based on Birkhoff Interpolation and Cellular Automata
Ziba Eslami, Nasrollah Pakniyat, Mahnaz Noroozi
18th CSI International Symposium on Computer Architecture Digital Systems (CADS 2015)

■ improving a coding method in unattended wireless sensor networks
Faezeh Sadat Babamir, Ziba Eslami
5th Conference on Algebraic Combinatorics and Graph Theory

■ an aggregate signcryption based on elliptic curves in unattended environments
Ziba Eslami
international congress on applied analysis and algebra

■ A certificateless proxy signature scheme secure in
Ziba Eslami, Nasrollah Pakniyat
international conference on latest computational technologies

■ secret image sharing with high quality stego images
Ziba Eslami, Jamal Zarepour Ahmadabadi
6 international isc confrrence on information security and cryptology(iscisc09)

■ a simple protocol for selling multiple secrets to a single buyer without a trusted party
Ziba Eslami, Nasrollah Pakniat
6 international isc confrrence on information security and cryptology(iscisc09)

■ Application of Trades in Construction/Enumeration of Combinatorial Objects
Ziba Eslami
ICM 2002

■ Classification of Some Large Sets and Designs
Ziba Eslami
2nd Pythagorean Conf.

■ تحلیل امنیت یک امضای فاقد گواهینامه جهت دار
نصرالله پاک نیت، مجتبی گودرزی، زیبا اسلامی

سومین کنفرانس ملی پژوهش های نوین در مهندسی و علوم کاربردی

■ Blind Multipurpose Image Watermarking Based onSecret Sharing
سرور شیدانی، زیبا اسلامی
شانزدهمین کنفرانس بین المللی انجمن رمز ایران، صفحات: ۱-۸

■ تحلیل امنیت یک طرح رمزنگاری با قابلیت جست و جوی رتبه بندی شده ی چند کلمه ی کلیدی و دارای چند صاحب داده
پوریا زنداکبری، زیبا اسلامی
چهارمین کنفرانس موضوعات نوین در علوم کامپیوتر و اطلاعات، صفحات:۲۱۷-۲۲۰

■ بهبود یافته یک روش تسهیم راز آستانه ای بر مبنای الگوریتم های پخش اطلاعات
سعیده کبیری راد، زیبا اسلامی
چهارمین کنفرانس موضوعات نوین در علوم کامپیوتر و اطلاعات

■ رمزگذاری کلید عمومی با قابلیت جستجوی کلیدواژه
مهناز نوروزی، نصراللّه پاک نیت، زیبا اسلامی
چهاردهمین کنفرانس بین المللی انجمن رمز ایران، صفحات: ۱-۶

■ پروتکل انتقال فراموشکار ۱ از ۲ مبتنی بررمزگذاری دوحالته تعمیم یافته
سیدمحمود موسوی، زیبا اسلامی
چهل و هشتمین کنفرانس ریاضی ایران، صفحات:۱۷۰۳-۱۷۰۷

■ پروتکل توافق کلید گروهی مقاوم در برابرتقلب با ویژگی تصحیح خطای ناشی از اختلال کانال
زیبا اسلامی، مهناز نوروزی
هفتمین کنفرانس بین المللی فناوری اطلاعات دانش و توسعه

■ پروتکل واترمارکینگ فروشنده-خریدار غیرخطی بدون شخص سوم معتمد
غلامرضا هجرودی، زیبا اسلامی
هفتمین کنفرانس بین المللی فناوری اطلاعات دانش و توسعه

■ یک روش رمزنگاری تصویر بلوک-مبنا با استفاده از آتاماتای سلولی و نگاشت آشوب
سعیده کبیری راد، زیبا اسلامی
بیستمین کنفرانس ملی سالانه انجمن کامپیوتر ایران

■ Cryptanalysis of an Attribute-based Key Agreement Protocol
نصراله پاک نیت، زیبا اسلامی، مهناز نوروزی
کنفرانس بین المللی ، فناوری اطلاعات و رسانه های دیجیتال، صفحات:۱۷۹-۱۸۲

■ پایداری داده ها در شبکه های حسگر بی سیم بی ملازم
فائزه سادات بابامیر، زیبا اسلامی
نهمین کنفرانس بین المللی انجمن رمز ایران

■ an efficient buyer- seller watermarking protcol based on proxy signatures
محمد کاظم نسب حاجی، زیبا اسلامی

■ یک طرح انتخابات الکترونیک امن و کار آمد مبتنی بر امضای کور
زیبا اسلامی، هدی قوامی پور
یازدهمین کنفرانس انجمن کامپیوتر ایران

پایان‌نامه‌ها و رساله‌های دکتری

■ امنیت در برون سپاری محتوای چندرسانه ای
سرور شیدانی
۱۴۰۰

■ طرح های های تسهیم راز بر مبنای عملگرهای بولی
سعیده کبیری راد
۱۳۹۸

■ ذخیره سازی داده های رمز گذاری شده بر روی ابر با قابلیت جستجو
مهناز نوروزی
۱۳۹۸

■ رمزگذاری کلیدعمومی; کلیدهای عمومی غیر قابل مقایسه و رمزگشایی گروهی پیام
بهمن رجبی کفشگر
۱۳۹۶

■ رمزنگاری آستانه ای سلسه مراتبی
نصراله پاک نیت
۱۳۹۴

پایان‌نامه‌های کارشناسی‌ارشد

■ پروتکل‌های احراز هویت سبک مبتنی بر اینترنت اشیاء
مجتبی گودرزی
۱۴۰۰

■ تجزیه و تحلیل امنیتی طرح‌های رمزنگاری قابل جستجوی اصالت سنجی شده در تنظیمات فاقد گواهی
دانیال شیرالی
۱۳۹۹

■ امضاهای فاقد گواهینامه تحلیل امنیت و بهبود برخی از طرح های موجود
شادی فرزان کیا
۱۳۹۹

■ تسریع رمزنگاری تصویر با استفاده از موازی سازی شبکه عصبی سلولی
امیرحسین علی حسینی

۱۳۹۸

■ ارائه یک مدل کنترل دسترسی برای رایانش مه در اینترنت اشیاء
حمید شمس الهی
۱۳۹۸

■ رمزگذاری قابل جتسجوی سبک وزن برای ابرهای سلامت
الناز نادریان
۱۳۹۷

■ تطابق الگو روی داده های رمز شده در فضای ابری
سهراب ابوذرخانی فرد
۱۳۹۷

■ طراحی یک چهارچوب برای انتقال فراموشکار مبتنی بر رمزنگاری‌های هم‌ریخت
سعید اسماعیل زاده
۱۳۹۷

■ جست و جوی رتبه بندی شده ی کلمه ی کلیدی بر روی داده های رمز شده
پوریا زنداکبری
۱۳۹۷

■ جستجوی مبتنی بر صفات کلمه کلیدی روی داده ی رمز شده
وهاب قمری
۱۳۹۷

■ حملات ملاقات در میانه بر روی رمزهای قالبی
امیرحسین ابراهیمی مقدم
۱۳۹۶

■ جستجوی عطفی کلمه ی کلیدی بر روی داده های رمز شده
ایمان کروبی
۱۳۹۶

■ رمزنگاری تصویر مبتنی بر روش های نهان نگاری
مهدیه شادفر
۱۳۹۶

■ بررسی و تحلیل پروتکل های توزیع کلید در رمزنگاری کوانتومی
راضیه مهاجر
۱۳۹۵

■ ایمن در برابر حمله حدس کلمه کلیدی (PEKS)طرح رمزگذاری کلید عمومی با جستجوی کلمات کلیدی
ندا حسین پوردهکردی

۱۳۹۵

■ طرح های تسهیم راز پویا
داود فرامرزی فیل آبادی
۱۳۹۴

■ تسهیم راز اجتماعی و کاربردهای آن
عبدالکریم محمدی
۱۳۹۴

■ پروتکل های انتقال فراموشکار در رمزنگاری
پریسا مومنی
۱۳۹۴

■ طرح های رمزگذاری با قابلیت جستجو
کبری امیری زیرتل
۱۳۹۴

■ مقیاس پذیری در طرح تسهیم تصویر محرمانه
حامد نوربخش
۱۳۹۳

■ بررسی پروتکل های واتر مارکینگ فروشنده – خریدار ناشناس
غلامرضا هجرودی
۱۳۹۳

■ تسهیم تصویر محرمانه آستانه ای سلسله مراتبی
فوءاد جنت بابائی
۱۳۹۲

■ رمز گذاری مبتنی بر ویژگی
سیدهاتف حسینیان برزی
۱۳۹۲

■ مدل های امنیتی و اثبات امنیت در پروتکل های توافق کلید گروهی
مهناز نوروزی
۱۳۹۱

■ رمزنگاری تصاویر با استفاده از توابع آشوب
عطیه بخشنده کپورچالی
۱۳۹۱

■ کدهای احراز هویت پیام برای چندین پیام
حکیمه فرخ

۱۳۹۱

■ بررسی طرح های امضائ – رمز مبتنی بر شناسه و کاربردهای آن
فائزه سادات بابامیر
۱۳۹۱

■ کدهای زنجیره ای و تشخیص الگو با استفاده از آن
مجید مددی گوگدرقی
۱۳۹۰

■ GSM تحلیل امنیت ارتباطات رمز شده
توحید سرابچی
۱۳۹۰

■ رمزنگاری تصاویر با استفاده اتوماتای سلولی
محمدوحید زنگنه مقدم
۱۳۹۰

■ طرح های امضاء_رمز فاقد گواهی نامه
نصراله پاک نیت
۱۳۸۹

■ پروتکل های واتر مارکینگ خریدار–فروشنده
محمد کاظم نسب حاجی
۱۳۸۹

■ روش های تسهیم راز آستانه ای و توافق کلید گروهی بر مبنای خم بیضوی
سعیده کبیری راد
۱۳۸۹

■ سیستم های انتخابات الکترونیک مبتنی بر امضای کور
هدی قوامی پور
۱۳۸۸

■ طرحی جدید برای تسهیم چندین –راز بر اساس اتوماتای سلولی
جمال زارع پور احمدآبادی
۱۳۸۸

■ پول الکترونیکی
مهدی طالبی
۱۳۸۸

■ پنهان نگاری و تسهیم راز در عکسهای استتار
سیدحسین رزاقی

۱۳۸۸

جوایز و افتخارات

■ مقاله برتر کنفرانس ملی

۱۳۹۷

■ مقاله برتر مجله بین المللی انجمن رمز ایران در سال ۹۶

۱۳۹۵

■ پژوهشگر برتر (پژوهشکده فضای مجازی) سال ۹۴

۱۳۹۳