به نام خدا

نصراله پاک‌نیت

کارنامک . خرداد ۱۴۰۴

تهران . صندوق پستی ۱۳۷۱- ۱۳۱۸۵ تلفن (داخلی ۴۲۳) ۶۶۹۵۱۴۳۰ (۰۲۱) دورنگار ۶۶۴۶۲۲۵۴ (۰۲۱)
https://irandoc.ac.ir/u/n-pakniat Pakniat[at]irandoc[dot]ac[dot]ir

◻ دانش‌آموخته

۱۳۹۴ دکتری ریاضی (علوم کامپیوتر). دانشگاه شهید بهشتی.

۱۳۸۹ کارشناسی ارشد علوم کامپیوتر. دانشگاه شهید بهشتی.

۱۳۸۷ کارشناسی علوم کامپیوتر. دانشگاه شهید باهنر کرمان.

۱۳۸۲ دیپلم ریاضی فیزیک. دبیرستان امام خمینی استهبان.

◻ پیشینهٔ کار

۱۴۰۱- رئیس مرکز فناوری اطلاعات و امنیت فضای مجازی . پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)*.

۱۴۰۱-۱۴۰۰ رئیس گروه ارتباطات علمی . ایرانداک.

۱۳۹۵- استادیار گروه زبان‌شناسی رایانشی، پژوهشکده علوم اطلاعات. ایرانداک.

◻ مجری پروژه

۱۴۰۳- سامانه اشاعه منابع علمی دانشگاهی ایرانیان. ایرانداک.

۱۴۰۳- توسعه سامانه نشریات دسترسی آزاد ایران (دوآجی) با طراحی و پیاده‌سازی خزشگرهای مقاله‌ها و داشبوردهای مدیریتی. ایرانداک

۱۴۰۳ طراحی و توسعه سامانه مدیریت اسناد راهبردی وزارت علوم، تحقیقات و فناوری. وزارت علوم، تحقیقات و فناوری

۱۴۰۳ طراحی و توسعه یک سامانه واژه‌نامه جدید با به کارگیری کلیدواژه‌های پایان‌نامه‌ها و رساله‌های فارسی‌زبان. ایرانداک.

۱۴۰۳ طراحی و توسعه پایگاه نمایه‌سازی نشریه‌های علمی دسترسی آزاد ایران (دوآجی). ایرانداک.

۱۴۰۲ طراحی و ساخت سامانه/ خدمت احراز هویت یکپارچه پژوهشگاه علوم و فناوری اطلاعات ایران. ایرانداک

---

* «پژوهشگاه علوم و فناوری اطلاعات ایران» پیش از سال ۱۳۸۴، «مرکز اطلاعات و مدارک علمی ایران»، تا سال ۱۳۸۸ «پژوهشگاه اطلاعات و مدارک علمی ایران»، و از سال ۱۳۸۸ به این سو «پژوهشگاه علوم و فناوری اطلاعات ایران» نام داشته است و در همهٔ این سال‌ها نیز با نام کوتاه «ایرانداک» خوانده می‌شود.

۱۴۰۱ طراحی و ساخت یک ماژول نرم‌افزاری برای استخراج و بازنمایی خودکار پیشنهادهای پژوهش از پایان‌نامه‌ها و رساله‌های پایگاه اطلاعات علمی ایران (گنج). ایرانداک.

۱۳۹۹ ارائه یک ماژول نرم‌افزاری در راستای ایجاد شبکه استنادی پارساهای موجود در پایگاه اطلاعات علمی ایران (گنج). ایرانداک

۱۳۹۷ طراحی یک روش هوشمند تجزیه رشته‌های مرجع در زبان فارسی. ایرانداک.

۱۳۹۶ طراحی یک الگوریتم همانندجو برای تشخیص متون بازنویسی شده در زبان فارسی. ایرانداک.

□ همکار پروژه

۱۴۰۳ مفهوم‌سازی، طراحی، و ساخت نظام رتبه‌بندی رویت‌پذیری موسسه‌های آموزش عالی. وزارت علوم، تحقیقات و فناوری.

۱۴۰۳ ارزیابی دسترس‌پذیری و کاربردپذیری سامانه‌های پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) از دید کاربران با آسیب بینایی. ایرانداک.

۱۴۰۰ ساخت پیکره متنی از مقاله‌های پژوهش‌نامه پردازش و مدیریت اطلاعات. ایرانداک.

۱۴۰۰ استخراج فراداده در پارساها با رویکرد الگوریتم‌های دسته‌بندی. ایرانداک.

۱۳۹۹ طراحی روشی هوشمند برای دسته‌بندی نوشتارهای علمی فارسی. ایرانداک.

□ ناظر پروژه

۱۴۰۴ بهینه‌سازی یک الگوریتم نویسه‌خوان نوری برای پایان‌نامه‌ها و رساله‌های فارسی . ایرانداک.

۱۴۰۴ امکان‌سنجی و استقرار سامانه فهرستگان کتابخانه‌های دانشگاهی . ایرانداک.

۱۴۰۳ طراحی چارچوب مدیریت تداوم کسب‌وکار پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) . ایرانداک.

۱۴۰۳ ایجاد هستی‌شناسی از اصطلاح‌نامه کشاورزی ایرانداک (اگرووک) . ایرانداک.

۱۴۰۳ بررسی دیدگاه دانشجویان کاربر سامانه ملی ثبت پایان‌نامه، رساله، و پیشنهاده در زمینه چگونگی اشاعه فراداده‌ها، داده‌ها، و متن آن‌ها . ایرانداک.

۱۴۰۲ طراحی گویه‌های ارزیابی سامانه‌های پرکاربرد پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) و بهبود سامانه نظرسنجی ایرانداک (سنا) در چارچوب نیازمندی‌های دولت الکترونیک . ایرانداک.

۱۴۰۰ تحلیل عرضه و تقاضای پایان‌نامه‌ها و رساله‌های حوزه انرژی در پایگاه گنج . ایرانداک.

۱۴۰۰– توسعه سیستم پیشنهاددهنده کلیدواژه برای مستندات علمی فارسی بر پایه اطلاعات اصطلاح‌نامه‌های تخصصی. ایرانداک.

۱۴۰۰ طراحی یک روش برای برچسب‌زدن تصاویر استخراج‌شده از پارساهای موجود در پایگاه اطلاعات علمی ایران (گنج). ایرانداک.

۱۴۰۰ تهیه مجموعه داده استاندارد فارسی برای مساله استخراج خودکار کلیدواژه از اسناد علمی. ایرانداک.

مقالهٔ ژورنال

Shiraly, D., Z. Eslami, and N. Pakniat. 2024. Designated-tester Identity-Based Authenticated Encryption with Keyword Search with applications in cloud systems. Journal of Systems Architecture 152: 103181.

Shiraly, D., N. Pakniat, and Z. Eslami. 2024. Hierarchical Identity-Based Authenticated Encryption with Keyword Search over encrypted cloud data. Journal of Cloud Computing 13 (1): 112.

Goodarzi, M., Z. Eslami, and N. Pakniat. 2024. Certificateless directed signature scheme without bilinear pairing. Information Security Journal: A Global Perspective 33 (3): 268-284.

Shiraly, D., Z. Eslami, and N. Pakniat. 2024. Certificate-based authenticated encryption with keyword search: Enhanced security model and a concrete construction for Internet of Things. Journal of Information Security and Applications 80: 103683.

Shiraly, D., N. Pakniat, and Z. Eslami. 2024. Designated-Server Hierarchical Searchable Encryption in Identity-Based Setting. The ISC International Journal of Information Security 15 (3): 1-17.

Ebrahimi Kiasari, M. E., N. Pakniat, A. Mirghadri, and M. Nazari. 2023. A new Social multi-secret sharing scheme using Birkhoff interpolation and Chinese remainder theorem. The ISC International Journal of Information Security 15 (1): 125-135.

Shiraly, D., N. Pakniat, M. Noroozi, and Z. Eslami. 2022. Pairing-free certificateless authenticated encryption with keyword search. Journal of Systems Architecture 124: 102390.

Esmaeilzade, S., N. Pakniat, and Z. Eslami. 2022. A generic construction to build simple oblivious transfer protocols from homomorphic encryption schemes. The Journal of Supercomputing 78(1): 72-92.

Pakniat, N., D. Shiraly, and Z. Eslami. 2020. Certificateless authenticated encryption with keyword search: Enhanced security model and a concrete construction for industrial IoT. Journal of Information Security and Applications 53: 102525.

Pakniat, N., and Z. Eslami. 2020. Cryptanalysis and improvement of a group RFID authentication protocol. Wireless Networks 26(5): 3363-3372.

Pakniat, N. 2019. Designated tester certificateless encryption with keyword search. Journal of Information Security and Applications 49: 102394.

Pakniat, N. 2018. Security Analysis of Two Lightweight Certificateless Signature Schemes. Journal of Computing and Security 5(2): 59-65.

Noroozi, M., Z. Eslami, and N. Pakniat. 2018. Comments on a chaos-based public key encryption with keyword search scheme. Nonlinear Dynamics 94(2): 1127-1132.

Pakniat, N., and Z. Eslami. 2017. Verifiable social multi-secret sharing secure in active adversarial model. Journal of Computing and Security 4(1): 3-12.

Eslami, Z., N. Pakniat, and M. Nojoumian. 2016. Ideal social secret sharing using Birkhoff interpolation method. Security and Communication Networks 9(18): 4973-4982.

Pakniat, N., M. Noroozi, and Z. Eslami. 2016. Reducing Multi-Secret Sharing Problem to Sharing a Single Secret Based on Cellular Automata. CSI Journal on Computer Science and Engineering 14: 38-43.

Pakniat, N., M. Noroozi, and Z. Eslami. 2015. Distributed key generation protocol with hierarchical threshold access structure. IET Information Security 9(4): 248-255.

Pakniat, N., Z. Eslami, and A. Miri. 2014. A note on “Selling multiple secrets to a single buyer”. Information Sciences 279: 889-892.

Eslami, Z., and N. Pakniat. 2014. Certificateless aggregate signcryption: Security model and a concrete construction secure in the random oracle model. Journal of King Saud University-Computer and Information Sciences 26(3): 276-286.

Pakniat, N., M. Noroozi, and Z. Eslami. (2014). Secret image sharing scheme with hierarchical threshold access structure. Journal of Visual Communication and Image Representation 25(5): 1093-1101.

Pakniat, N., and Z. Eslami. 2011. A Proxy E-Raffle Protocol Based on Proxy Signatures. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 2(3): 74-84.

Parand, K., Z. Delafkar, N. Pakniat, A. Pirkhedri, and M. K. Haji. 2011. Collocation method using Sinc and Rational Legendre functions for solving Volterra’s population model. Communications in Nonlinear Science and Numerical Simulation 16(4): 1811-1819.

Parand, K., N. Pakniat, and Z. Delafkar. 2011. Numerical solution of the Falkner-Skan equation with stretching boundary by collocation method. International Journal of Nonlinear Science 11(3): 275-283.

محمد ابراهیم ابراهیمی کیاسری، عبدالرسول میرقدری، مجتبی نظری، نصراله پاک‌نیت. ۱۴۰۳. بررسی و تحلیل چند طرح تسهیم راز مبتنی بر روش‌های درون‌یابی. پدافند الکترونیک و سایبری ۱۲(۱): ۱۱-۲۰.

پاک‌نیت، نصراله، و جلال‌الدین نصیری. ۱۴۰۰. تجزیه متون استنادی در زبان فارسی با استفاده از ماشین بردار پشتیبان. پژوهشنامه پردازش و مدیریت اطلاعات ۳۷ (۴): ۱۲۴۵-۱۲۶۸.

علایی ابوذر، الهام، نصراله پاک‌نیت، علی‌اصغر حجت‌پناه، مجتبی زالی، و محمدهادی آقالویی آغمیونی. ۱۴۰۰. معرفی یک پیکره متنی تخصصی: پیکره پژوهش‌نامه. پژوهش‌های زبان‌شناسی تطبیقی ۱۱(۲۲): ۲۷۱-۲۸۹.

پاک‌نیت، نصراله، و زیبا اسلامی. ۱۳۹۹. تحلیل امنیت و بهبود یک سیستم حمل‌ونقل هوشمند مبتنی بر امضای تجمعی فاقد گواهینامه. پدافند الکترونیکی و سایبری ۸: ۲۵-۳۳.

ابراهیمی کیاسری، محمد ابراهیم، عبدالرسول میرقدری، نصراله پاکنیت، و مجتبی نظری. ۱۳۹۹. تسهیم چندراز پیشنگر با استفاده از درونیابی لاگرانژ و قضیه باقیمانده چینی. پژوهش‌های نوین در ریاضی ۶: ۱۴۵ - ۱۵۶.

پاک‌نیت، نصراله، و آزاده محبی. ۱۳۹۸. همانندجویی در متون فارسی بازنویسی شده با استفاده از روش‌های معنایی و احتمالاتی. پژوهشنامه پردازش و مدیریت اطلاعات ۳۴(۴): ۱۸۱۱ – ۱۸۳۶.

□ مقالهٔ همایش

Pakniat, N., and B. A. Vanda. 2018. Cryptanalysis and improvement of a pairing-free certificateless signature scheme. In 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), Tehran, Iran.

Pakniat, N. 2018. On the Security of a Certificateless Strong Designated Verifier Signature Scheme. In 3th International Conference on Computer Engineering - Information Technology and Data Processing, Tehran, Iran.

Pakniat, N., and M. Noroozi. 2016. Cryptanalysis of a certificateless aggregate signature scheme. In 9th National Conference of Command, Control, Communication and Computers & Intelligence (C4I), Tehran, Iran.

Pakniat, N. 2016. Public key encryption and keyword guessing attack: a survey. In 13th International ISC Conference on Information Security and Cryptology (ISCISC'16), Tehran, Iran.

Eslami, Z., N. Pakniat, and M. Noroozi. 2015. Hierarchical threshold multi-secret sharing scheme based on birkhoff interpolation and cellular automata. In 18th CSI International Symposium on Computer Architecture and Digital Systems (CADS), Tehran, Iran.

Pakniat, N., M. Noroozi, and Z. Eslami. 2013. Cryptanalysis of an Attribute-based Key Agreement Protocol. In Proceedings of the International Conference on Computer, Information Technology and Digital Media, Tehran, Iran.

Eslami, Z., and N. Pakniat. 2012. A certificateless proxy signature scheme secure in standard model. In International Conference on Latest Computational Technologies (ICLCT), Bangkok Thailand.

Eslami, Z., and N. Pakniat. 2009. A simple protocol for selling multiple secrets to a single buyer without a trusted party. In 6th International ISC Conference on Information Security and Cryptology (ISCISC'09), Isfahan, Iran.

پاک‌نیت، نصراله، و بهنام عباسی وندا. ۱۳۹۷. تحلیل امنیت یک طرح امضا انبوه فاقد گواهینامه. اولین کنفرانس ملی پیشرفت‌های اخیر در مهندسی و علوم نوین، تهران، ایران.

نوروزی، مهناز، نصراله پاک‌نیت، و زیبا اسلامی. ۱۳۹۶. رمزگذاری کلید عمومی با قابلیت جستجوی کلیدواژه: ارائه یک ساخت کلی امن در برابر حملات حدس کلیدواژه برخط و غیربرخط. چهاردهیمن کنفرانس بین‌المللی انجمن رمز ایران، شیراز، ایران.

☐ آموزش

۱۴۰۳-	روش‌های یادگیری ماشین در پردازش زبان طبیعی . ایرانداک. پژوهشکده علوم اطلاعات.
۱۴۰۳	آشنایی با زبان‌شناسی رایانشی . ایرانداک. پژوهشکده علوم اطلاعات.
۱۳۹۹	امنیت شبکه پیشرفته. کارشناسی ارشد شبکه‌های کامپیوتری. دانشگاه علم و صنعت ایران. دانشکدهٔ مهندسی کامپیوتر.
۱۳۹۶-۰۰	سیستم‌های کامپیوتری امن. کارشناسی ارشد مهندسی فناوری اطلاعات. دانشگاه علم و صنعت ایران. دانشکدهٔ مهندسی کامپیوتر.
۱۳۹۶	رمزنگاری. کارشناسی علوم کامپیوتر. دانشگاه شهید بهشتی. دانشکده علوم ریاضی.

☐ راهنمایی/مشاوره پایان‌نامه/رساله

۱۴۰۳	مشاوره رساله دکتری با عنوان: رمزگذاری داده‌ها بر روی ابر با قابلیت جستجو در بستر رمزنگاری شناسه-مبنا. دانشگاه شهید بهشتی.
۱۴۰۳	مشاوره پایان‌نامه کارشناسی ارشد با عنوان: امنیت در اینترنت اشیاء پزشکی با استفاده از پروتکل های احراز هویت مبتنی بر RFID . دانشگاه الزهرا (س).

۱۴۰۲ مشاوره رساله دکتری با عنوان: طرح تسهیم راز آستانه‌ای کارآمد مبتنی بر درونیابی . دانشگاه آزاد اسلامی واحد خرم‌آباد

۱۴۰۱ مشاوره پایان‌نامه کارشناسی ارشد با عنوان: پروتکل های استقرار کلید گروهی مبتنی بر تسهیم راز . دانشگاه الزهرا (س).

◻ داوری مقالات

- Journal of Systems Artichecture
- Journal of Information Security and Applications
- Computer Networks
- Wireless Personal Communications
- Journal of King Saud University - Computer and Information Sciences
- Journal of Franklin Institute
- Wireless Networks
- Journal of Computing and Security
- ISC International Journal of Information Security
- IEEE Access
- IEEE Internet of Things
- IEEE Transactions on Information Forensics and Security
- Signal Processing
- Journal of Supercomputing
- International Journal of Information
- Science and Management
- Information Processing Letters
- Frontiers of Computer Science

- مدیریت اطلاعات
- پدافند الکترونیکی و سایبری
- پردازش و مدیریت اطلاعات

◻ عضویت‌ها (کمیته علمی همایش‌ها)

- پنجمین همایش ملی مدیران فناوری اطلاعات. ۱۳۹۶.
- ششمین همایش ملی مدیران فناوری اطلاعات. ۱۳۹۷.
- هفتمین همایش ملی مدیران فناوری اطلاعات. ۱۳۹۸
- چهارمین کنفرانس بین‌المللی شهر هوشمند ایران. ۱۴۰۲

- پنجمین کنفرانس بین‌المللی شهر هوشمند ایران. ۱۴۰۳
- هشتمین جایزه ملی فناوری اطلاعات. ۱۴۰۳
- ششمین کنفرانس بین‌المللی شهر هوشمند و هوش مصنوعی ایران. ۱۴۰۴

عضویت‌ها (اجرایی)

- عضو حقیقی شورای پژوهش پژوهشگاه. ایرانداک: از سال ۱۳۹۸ تا سال ۱۴۰۳
- عضو کمیته پدافند غیرعامل پژوهشگاه. ایرانداک: از سال ۱۴۰۲
- عضو کمیته بهره‌وری پژوهشگاه. ایرانداک: از سال ۱۴۰۱
- عضو شورای نظارت، ارزیابی، و تضمین کیفیت پژوهشگاه. ایرانداک: از سال ۱۴۰۲
- عضو شورای راهبردی پژوهشگاه: ایرانداک: از سال ۱۴۰۳
- عضو کمیته توسعه دولت الکترونیک و هوشمندسازی پژوهشگاه: از سال ۱۴۰۳

افتخارات

- مدیر برگزیده فناوری اطلاعات. وزارت علوم، تحقیقات و فناوری: ۱۴۰۳
- مقاله برتر Journal of Computing and Security: ۱۳۹۷
- رساله شایسته تقدیر رمزنگاری و امنیت شبکه: ۱۳۹۵
- عضو دفتر استعدادهای درخشان دانشگاه شهید بهشتی: ۱۳۹۰
- دانش‌آموخته رتبه اول کارشناسی ارشد علوم کامپیوتر دانشگاه شهید بهشتی: ۱۳۸۹