Curriculum Vitae January 2019

Nasrollah Pakniat

Contact

Address: Information science research center, Iranian Research Institute for Information Science and Technology (IRANDOC)

Phone : +98 21 66951430 (ext. 422) and +98 930 0575566

Email: [my last name](at)irandoc(dot)ac(dot)ir

Education

[1]. Ph.D. in Mathematics (Computer Science), Shahid Beheshti University, 2015. Thesis Title: Hierarchical Threshold Cryptography, Supervisor: Dr. Ziba Eslami.

[2]. M.Sc. in Computer Science, Shahid Beheshti University, 2011. Thesis Title: Certificateless Signcryption Schemes, Supervisor: Dr. Ziba Eslami.

[3]. B.Sc. Degree in Computer Science, Shahid Bahonar University of Kerman. Thesis Title: Wireless Networks, Supervisor: Dr. Faramarz Sadeghi.

Publications

Research projects:

[۱]. **نصراله پاک‌نیت**، طراحی یک الگوریتم همانندجو برای تشخیص متون بازنویسی شده در زبان فارسی، پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، ۱۳۹۶.

[۲]. **نصراله پاک‌نیت**، جلال‌الدین نصیری، عمار جلالی‌منش، طراحی یک روش هوشمند تجزیه رشته‌های مرجع در زبان فارسی، پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، در دست انجام.

[۳]. جلال‌الدین نصیری، **نصراله پاک‌نیت**، طراحی روشی هوشمند برای دسته‌بندی نوشتارهای علمی فارسی، پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، در دست انجام.

Journals:

[۱]. **نصراله پاک‌نیت**، آزاده محبی، همانندجویی در متون فارسی بازنویسی شده با استفاده از روش‌های معنایی و احتمالاتی، پژوهش‌نامه پردازش و مدیریت اطلاعات، در دست چاپ.

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

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

[4]. Z. Eslami, **N. Pakniat**, M. Nojoumian, Ideal social secret sharing using Birkhoff interpolation method, Security and Communication Networks, 9 (2016) 4973–4982.

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

[6]. **N. Pakniat**, M. Noroozi, Z. Eslami, A Distributed Key Generation Protocol with Hierarchical Threshold Access Structure, IET information Security, 9 (2015) 248-255.

[7]. **N. Pakniat**, M. Noroozi, Z. Eslami, Secret image sharing scheme with hierarchical threshold access structure, Journal of Visual Communication and Image Representation, 25 (2014) 1093–1101.

[8]. **N. Pakniat**, Z. Eslami, A. Miri, A Note on "Selling Multiple Secrets to a Single Buyer", Information Sciences, 279 (2014) 889–892.

[9]. **N. Pakniat**, Z. Eslami, 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 (2014) 276–286.

[10]. **N. Pakniat**, Z. Eslami, A proxy e-raffle protocol based on proxy signatures. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2 (2012) 74-84.

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

[12]. K. Parand, Z. Delafkar, **N. Pakniat**, A. Pirkhedri, M. Kazemnasab Haji, Collocation Method Using Sinc And Rational Legendre Functions For Solving Volterra's Population Model, Communications in Nonlinear Science and Numerical Simulation, 16 (2011) 1811–1819.

Conferences:

[1]. **N. Pakniat**, B. Abasi Vanda, Cryptanalysis and improvement of a pairing-free certificateless signature scheme, 15th International ISC Conference on Information Security and Cryptology (ISCISC'18), 2018, Tehran, Iran.

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

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

[4]. **N. Pakniat**, M. Noroozi, Z. Eslami, Hierarchical Threshold Multi-Secret Sharing Scheme Based on Birkhoff Interpolation and Cellular Automata, The 18th CSI International Symposium on Computer Architecture & Digital Systems (CADS 2015), October 7-8, 2015, Tehran, Iran.

[5]. **N. Pakniat**, M. Noroozi, Z. Eslami, Cryptanalysis of an Attribute-based Key Agreement Protocol, Proceedings of the International Conference on Computer, Information Technology and Digital Media, October 13-18 2013, Tehran, Iran.

[6]. Z. Eslami, **N. Pakniat**, A certificateless proxy signature scheme secure in standard model, International conference on latest computational technologies (ICLCT 2012), 2012, Bangkok, Thailand.

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

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

[۹]. مهناز نوروزی، **نصراله پاک‌نیت**، زیبا اسلامی، 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، ۱۳۹۶، شیراز، ایران.

Translations:

[۱]. زیبا اسلامی، **نصراله پاک‌نیت**، مهناز نوروزی، رمزنگاری تابعی: دیدگاهی جدید در رمزنگاری. فضای دوم، شماره ۲، ۱۳۹۴، ۵-۱۵.

Reviewer

- Journal of Computer Security (IOS press)
- Optics and Lasers in Engineering (Elsevier)
- Expert Systems With Applications (Elsevier)
- Journal of the Franklin Institute (Elsevier)

- Wireless Personal Communications (Springer)
- Journal of Computing and Security
- Iranian Journal of Information Processing and Management
- Iranian Journal of Information Management
- International Journal of Advanced Computer Science and Applications (Taylor & Francis)
- International Journal of Network Security
- Journal of Computer Networks and Communications (hidawi)
- Journal of the Institution of Engineers (India): Series B (Springer)
- Journal of Applied Mathematics (hindawi)
- The Scientific World Journal (hindawi)
- 13th International ISC Conference on Information Security and Cryptology (ISCISC'16)
- 14th International ISC Conference on Information Security and Cryptology (ISCISC'17)
- 15th International ISC Conference on Information Security and Cryptology (ISCISC'18)
- 16th International ISC Conference on Information Security and Cryptology (ISCISC'19)
- 5th IT Managers National Conference (ITManC17)
- 6th IT Managers National Conference (ITManC18)

Teaching

Spring 2018: Secure Computer Systems (graduate), Iran University of Science & Technology, Tehran, Iran

Fall 2017: Secure Computer Systems (graduate), Iran University of Science & Technology, Tehran, Iran.

Spring 2017: Secure Computer Systems (graduate), Iran University of Science & Technology, Tehran, Iran

Spring 2017: Cryptography, Shahid Beheshti University, Tehran, Iran.

Fall 2016: Basic mathematics, Shahid Beheshti University, Tehran, Iran.

Fall 2013: Mathematics for chemists, Shahid Beheshti University, Tehran, Iran.

Spring 2013: Basic mathematics, Shahid Beheshti University, Tehran, Iran.

Fall 2012: Mathematics 1, Shahid Beheshti University, Tehran, Iran.

Fall 2012: Mathematics 2, Shahid Beheshti University, Tehran, Iran.

Spring 2010: Web Designing Workshop, Fakhr Razi University, Saveh, Iran.

Teaching Assistance

[1]. Cryptography, Department of Computer Science, Shahid Beheshti University, Tehran, Iran.

[2]. Advanced Cryptography, Department of Computer Science, Shahid Beheshti University, Tehran, Iran.

[3]. Coding Theory, Department of Computer Science, Shahid Beheshti University, Tehran, Iran.

[4]. Linear algebra, Department of Computer Science, Shahid Beheshti University, Tehran, Iran.

Honors

[1]. 2nd place in ISC (Iranian Society of Cryptology) Doctoral Dissertation Award in cryptology and network security, summer 2016.

[2]. Recognized as an Exceptional Talent and Admitted to the graduate programs without an entrance exam, Shahid Beheshti University, Summer 2011

[3]. Ranked first among all M.Sc. graduate students of Computer Science of Shahid Beheshti University in 2011.

Miscellaneous

[1]. My Erdös number is 3 through (N. Pakniat→M. Nojoumian→ D. R. Stinson→P. Erdös)