رزومه

فروردین ۱۴۰۰

مهناز نوروزی

رایانامه: m.noroozi@alzahra.ac.ir

اشتغال

- استادیار، گروه علوم کامپیوتر، دانشکده علوم ریاضی، دانشگاه الزهرا (س)، تهران، ایران.

تحصیلات

- دکتری، علوم کامپیوتر، دانشگاه شهید بهشتی، تهران، ایران.

  عنوان رساله: ذخیره‌سازی داده‌های رمزگذاری شده بر روی ابر با قابلیت جستجو، استاد راهنما: دکتر زیبا اسلامی.

  فرصت مطالعاتی: دانشگاه ولونگونگ، استرالیا، استاد راهنما: پروفسور ویلی سوسیلو.

- کارشناسی ارشد، علوم کامپیوتر، دانشگاه شهید بهشتی، تهران، ایران.

  عنوان پایان‌نامه: مدل‌های امنیتی و اثبات امنیت در پروتکل‌های توافق کلید گروهی، استاد راهنما: دکتر زیبا اسلامی.

- کارشناسی، علوم کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران.

  پروژه کارشناسی: برنامه‌نویسی چندعاملی، استاد راهنما: دکتر رسول رمضانیان.

- پیش‌دانشگاهی و دبیرستان، ریاضی و فیزیک، فرزانگان، سازمان ملی پروش استعدادهای درخشان، تهران، ایران.

مقالات

نشریات علمی:

[1]. Z. Eslami, **M. Noroozi,** K. Amirizirtol, Public Key Encryption with Distributed Keyword Search, Journal of Discrete Mathematical Sciences & Cryptography, in press (DOI : 10.1080/09720529.2020.1859797).

[2]. D. Shiraly, N. Pakniat, **M. Noroozi**, Z. Eslami, Paring-free Certificateless Encryption with Keyword Search Secure against Keyword Guessing Attacks, submitted.

[3]. **M. Noroozi**, Z. Eslami, Public-key encryption with keyword search: a generic construction secure against online and offline keyword guessing attacks, Journal of Ambient Intelligence and Humanized Computing, 11, 879-890, 2020.

[4]. **M. Noroozi**, Z. Eslami, J Baek, On the Security of a Privacy-Preserving Ranked Multi-Keyword Search Scheme, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 10 (1), 75-85, 2019.

[5]. **M. Noroozi**, Z. Eslami, Public key authenticated encryption with keyword search: revisited, IET Information Security, 13 (4), 336-342, 2018.

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

[7]. **M. Noroozi**, I. Karoubi, Z. Eslami, Designing a secure designated server identity-based encryption with keyword search scheme: still unsolved, Annals of Telecommunications, 73 (11), 769-776, 2018.

[8]. 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 (1), 38-43, 2016.

[9]. Z Eslami, **M Noroozi**, SK Rad, Provably Secure Group Key Exchange Protocol in the Presence of Dishonest Insiders, International Journal of Network Security, 18 (1), 33-42, 2016.

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

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

همایش‌ها:

[۱]. **م. نوروزی**، ز. اسلامی، حفظ محرمانگی و قابلیت جستجو در ذخیره‌سازی ابری، هفدهمین کنفرانس بین المللی انجمن رمز ایران، تهران، ایران، شهریور ۱۳۹۹.

[۲]. **م. نوروزی**، ن. پاک نیت، ز. اسلامی، رمزگذاری کلید عمومی با قابلیت جستجوی کلید واژه: ارایه یک ساخت کلی امن در برابر حملات حدس کلید واژه برخط و غیربرخط، چهاردهمین کنفرانس بین المللی انجمن رمز ایران، شیراز، ایران، شهریور، ۱۳۹۶.

[3]. N. Pakniat, **M. Noroozi**, Cryptanalysis of a certificateless aggregate signature scheme, 9th National Conference of Command, Control, Communication and Computers & Intelligence (C4I), Tehran, Iran, December 15-16, 2016.

[4]. KA Zirtol, **M Noroozi**, Z Eslami, Multi-user searchable encryption scheme with general access structure, 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, Iran, November 5-6, 2015.

[۵]. **م. نوروزی**، ز. اسلامی، پروتکل توافق کلید گروهی مقاوم در برابر تقلب با ویژگی تصحیح خطای ناشی از اختلال کانال، هفتمین کنفرانس بین المللی فناوری اطلاعات و دانش، ارومیه، ایران، ۱۳۹۴.

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

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

داوری مقالات

[1]. Security and communication Networks (Wiley)

[2]. Journal of Information Security and Applications (Elsevier)

[3]. The ISC International Journal of Information Security (ISeCure)

[4]. Biannual Journal Monadi for Cyberspace Security (AFTA)

[5]. 13th International ISC Conference on Information Security and Cryptology

[6]. 14th International ISC Conference on Information Security and Cryptology

تدریس

[۱]. رمزنگاری (کارشناسی ارشد)، دانشگاه الزهرا، تهران، ایران.

[۲]. نظریه کدگذاری، دانشگاه الزهرا، تهران، ایران.

[۳]. برنامه‌سازی پیشرفته، دانشگاه الزهرا، تهران، ایران.

[۴]. اصول سیستم‌های کامپیوتری، دانشگاه الزهرا، تهران، ایران.

[۵]. ساختمان داده‌ها و الگوریتم‌ها، دانشگاه الزهرا، تهران، ایران.

[۶]. مبانی کامپیوتر و برنامه‌سازی، دانشگاه الزهرا، تهران، ایران.

[۷]. کارگاه کامپیوتر، دانشگاه الزهرا، تهران، ایران.

[۸]. رمزنگاری، دانشگاه شهید بهشتی، تهران، ایران.

دستیاری آموزشی

[۱]. رمزنگاری (کارشناسی ارشد)، دانشگاه شهید بهشتی، تهران، ایران.

[۲]. رمزنگاری پیشرفته (کارشناسی ارشد)، دانشگاه شهید بهشتی، تهران، ایران.

[۳]. نظریه کدگذاری (کارشناسی ارشد)، دانشگاه شهید بهشتی، تهران، ایران.

افتخارات و فعالیت‌ها

- برنده جایزه شهید تهرانی مقدم از بنیاد ملی نخبگان ایران، ۱۳۹۹.
- دانش‌آموخته برتر، بنیاد ملی نخبگان ایران.
- سخنران مدعو، هفدهمین کنفرانس بین المللی انجمن رمز ایران، تهران، ایران، شهریور ۱۳۹۹.
- درجه ممتاز در جلسه دفاع از رساله دکتری (نمره ۲۰ از ۲۰).
- رتبه اول در میان فارغ التحصیلان کارشناسی ارشد رشته علوم کامپیوتر دانشگاه شهید بهشتی، ۱۳۹۱، (معدل ۱۸,۸۲ از ۲۰).
- عضویت در تیم اجرایی سیزدهمین کنفرانس بین‌المللی انجمن رمز ایران، ۱۳۹۵.
- رئیس شاخه دانشجویی انجمن رمز ایران در دانشگاه شهید بهشتی در دوره دکتری.