



به نام خدا

رزومه علمی - پژوهشی



مجتبی بهرامیان

کاشان، دانشگاه کاشان، دانشکده علوم ریاضی، گروه ریاضی محض	آدرس محل کار:
+98-31-55912327	تلفن دفتر کار:
<a href="mailto:bahramianh@kashanu.ac.ir">bahramianh@kashanu.ac.ir</a>	ایمیل:
<a href="https://faculty.kashanu.ac.ir/bahramian/fa">https://faculty.kashanu.ac.ir/bahramian/fa</a>	وبسایت:

## تحصیلات

- دکتری : رشته جبر - نظریه اعداد  
نام دانشگاه: دانشگاه کاشان  
عنوان رساله: حل مسأله لگاریتم گسسته روی خم‌های بیضوی و ژاکوبین تعمیم یافته آن‌ها  
نام استاد راهنما: دکتر حسن دقیق

- کارشناسی ارشد: رشته جبر ناجابجایی

نام دانشگاه: دانشگاه صنعتی شریف

عنوان رساله: اتحاد چندجمله‌ایها

نام استاد راهنما: دکتر سعید اکبری

- کارشناسی

- نام دانشگاه: دانشگاه کاشان

- عنوان رساله: -

- نام استاد راهنما: -

## افتخارات

- برگزیده بیست و دومین مسابقات دانشجویی ریاضی کشوری ۱۳۷۶
- برگزیده بیست و سومین مسابقات دانشجویی ریاضی کشوری ۱۳۷۷
- دانش‌آموخته رتبه اول کارشناسی دانشگاه کاشان ۱۳۷۸
- نفر اول برگزیده آزمون دکترای ریاضی
- استاد نمونه آموزشی دانشکده ریاضی دانشگاه کاشان ۱۳۹۳
- استاد نمونه آموزشی دانشکده ریاضی دانشگاه کاشان ۱۳۹۸
- استاد نمونه آموزشی دانشکده ریاضی دانشگاه کاشان ۱۴۰۱

## زمینه‌های تحقیقاتی مورد علاقه

- نظریه جبری اعداد
- رمزنگاری خم‌های بیضوی

1. Hassan Daghigh and Mojtaba Bahramian, Generalized Jacobian and Discrete Logarithm Problem on Elliptic Curves, Iranian Journal of Mathematical Sciences and Informatics Vol. 4, No. 2, 2009, 55-64.
2. Mojtaba Bahramian and Hassan Daghigh, A Generalized Fibonacci Sequence and the Diophantine Equations  $x^2 \pm kxy - y^2 \pm x = 0$ , Iranian Journal of Mathematical Sciences and Informatics Vol. 8, No. 2, 2013, 111-121.
3. Mojtaba Bahramian and Khadijeh Eslami, An Efficient Threshold Verifiable Multi-Secret Sharing Scheme Using Generalized Jacobian of Elliptic Curves, Algebraic Structures and Their Applications Vol. 4 No. 2, 2017, 45-55.
4. Mojtaba Bahramian and Khadijeh Eslami, A New Verifiable Multi-Secret Sharing Scheme based on Elliptic Curves and Pairings, Italian Journal of Pure and Applied Mathematics, N. 41, 2019 456-668.
5. Maryam Sheikhi-Garjan, Mojtaba Bahramian, Christophe Doche, A Threshold Verifiable Multi-Secret Sharing Based on Elliptic Curves and Chinese Remainder Theorem, In: IET Information Security, Vol. 13, No. 3, 2019, 278-284.
6. Kh. Eslami and M. Bahramian, An ECDLP-Based Verifiable Multi-Secret Sharing Scheme, Math. Interdisc. Res. 5(2020) 193-206.
7. Kh. Eslami and M. Bahramian, An Isogeny-based Quantum-resistant Secret Sharing Scheme, Filomat 36:10 (2022), 3249–3258.
8. M. Bahramian and E. Hajirezaei, An Identity-Based Encryption Scheme using Isogeny of Elliptic Curves, FACTA UNIVERSITATIS (NIŠ), Ser. Math. Inform., Vol. 35, No. 5, 2020, 1451-1460.
9. M. Rezaei Kashi and M. Bahramian, Proof of Knowing the Prime Factors of a Number Using Zero-Knowledge Proof, Iranian Journal of Mathematical Sciences and Informatics, (English version)

10. M. Rezaei Kashi and M. Bahramian, A Post-Quantum Zero-Knowledge Identification Scheme, Math. Interdisc. Res. 10:4 (2025) 431-446.

11. M. Rezaei Kashi and M. Bahramian, Oblivious Transfer Using Generalized Jacobian of Elliptic Curves, Isecure 15:2 (2023), 260-270.

۱۲. مجتبی بهرامیان، آشنایی با رمزنگاری خم‌های بیضوی، فرهنگ و اندیشه ریاضی، سال ۳۸، شماره ۶۴، (بهار و تابستان ۱۳۹۸)، صص. ۱۱۷ تا ۱۴۲.

۱۳. مجتبی بهرامیان و مریم رضایی کاشی، اثبات دانستن عوامل اول یک عدد با استفاده از پروتکل دانش-صفر، نشریه علوم ریاضی و انفورماتیک (IJMSI)، شماره ویژه فارسی (اسفند ۹۹)، صص. ۳۳ تا ۴۶. (نسخه فارسی)

#### مقالات ارائه شده در کنفرانسها

1. Mojtaba Bahramian, Nanoscience and Nanotechnology Conference, The Vertex Padmakar-Ivan Index of Dendrimer, Sabancı University, Istanbul, Turkey, 2011.
2. Mojtaba Bahramian, The Jacobian of graphs, 5th Conference on Algebraic Combinatorics and Graph Theory, University of Kashan, Kashan, Iran, 2012.
3. Mojtaba Bahramian and G. H. Fath-Tabar, The Szeged Eigenvalues of the Path, 5th Conference on Algebraic Combinatorics and Graph Theory, University of Kashan, Kashan, Iran, 2012.

4. Mojtaba Bahramian, Sandpile Group of Nanotubes, THE ALGERIAN-TURKISH INTERNATIONAL DAYS ON MATHEMATICS, Fatih University, Istanbul, Turkey, 2013.
5. Mojtaba Bahramian, The critical Groups of  $K_n-\{e\}$  and  $K_n-\{e,f\}$ , The 6th Conference & Workshop on Mathematical Chemistry, Persian Gulf University, Bushehr, Iran, 2013.
6. Mojtaba Bahramian, Computing the Tate Pairing using Generalized Jacobians, The 45th Annual Iranian Mathematics Conference, Semnan University, Semnan, Iran, 2014.
7. Mojtaba Bahramian, Discrete logarithm Problem, 24th Iranian Algebra Seminar, Kharazmi University, Karaj, Iran, 2014.
8. Mojtaba Bahramian, Maryam Sheikhi-Garjan and Fatemeh Seifi-Shahpar, The First Conference on Computational Group Theory, Computational Number Theory and Applications, Secret Sharing Based on Elliptic Curves, University of Kashan, Kashan, Iran, 2014.
9. Mojtaba Bahramian, Somayyeh Didari and Hassan Daghigh, Calculus on Elliptic Curves, The First Conference on Computational Group Theory, Computational Number Theory and Applications, University of Kashan, Kashan, Iran, 2014.
10. Somayyeh Didari, Hassan Daghigh and Mojtaba Bahramian, Constructing Elliptic Curves for Cryptography, The First Conference on Computational Group Theory, Computational Number Theory and Applications, University of Kashan, Kashan, Iran, 2014.
11. Hassan Daghigh, Mojtaba Bahramian and Somayyeh Didari, An Overview of Some Mathematical Problems in Cryptography, The First Conference on Computational Group Theory, Computational Number Theory and Applications, University of Kashan, Kashan, Iran, 2014.
12. Mojtaba Bahramian, Jacobian group of Cocktail Party, The Second Conference on Computational Group Theory, Computational Number Theory and Applications, University of Kashan, Kashan, Iran, 2015.

13. Mojtaba Bahramian and Maryam Sheikhi-Garjan, An identity-based encryption scheme, The Second Conference on Computational Group Theory, Computational Number Theory and Applications, University of Kashan, Kashan, Iran, 2015.
14. Mojtaba Bahramian and Khadijeh Eslami, GENERALIZED JACOBIAN CRYPTOSYSTEMS, First International Conference on Combinatorics, Cryptography and Computation, Iran University of Science and Technology, Tehran/Noor, Iran, 2016.
15. Khadijeh Eslami and Mojtaba Bahramian, Certificate-Based Encryption Scheme, First International Conference on Combinatorics, Cryptography and Computation, Iran University of Science and Technology, Tehran/Noor, Iran, 2016.
16. Khadijeh Eslami and Mojtaba Bahramian, Secret Sharing Scheme, 9-th Iranian Group Theory Conference, University of Kashan, Iran, 2017.
17. Mojtaba Bahramian, Group Theory in Cryptography, 9-th Iranian Group Theory Conference, University of Kashan, Iran, 2017.
18. Mojtaba Bahramian, RSA Scheme over the Ring of Gaussian Integers, The 48th Annual Iranian Mathematics Conference, Bu Ali Sina University, Hamedan, Iran, 2017.
19. Khadijeh Eslami and Mojtaba Bahramian, An Identity-Based Encryption Based on Pairings over Elliptic Curves, The 48th Annual Iranian Mathematics Conference, Bu Ali Sina University, Hamedan, Iran, 2017.
20. Khadijeh Eslami and Mojtaba Bahramian, A Threshold Multi-Secret Sharing Scheme Based on Shamir's Scheme, First International Conference on Modern Technologies in Sciences, Amol University of Special Modern Technologies, Amol, Iran, 2017.

21. Mojtaba Bahramian, secure Cryptography Using Elliptic Curves, First International Conference on Modern Technologies in Sciences, Amol University of Special Modern Technologies, Amol, Iran, 2017.

22. Maryam Rezaei Kash and Mojtaba Bahramian, Post-Quantum Cryptography Based on Isogeny of Elliptic Curves, The 48th Annual Iranian Mathematics Conference, University of Science and Technology, Tehran, Iran, 2018.

۲۳. مریم رضایی کاشی و مجتبی بهرامیان، کدهای رید-مولر روی میدان های متناهی و کاربرد آن ها در تسهیم راز، چهارمین کنفرانس بین المللی ترکیبیات، رمزنگاری، علوم کامپیوتر و محاسبات، دانشگاه علم و صنعت، تهران، آبان ۱۳۹۸

۲۴. الهام حاجی رضایی و مجتبی بهرامیان، رمزنگاری شناسه کاربری با استفاده از ژاکوبین تعمیم یافته خم های بیضوی، پنجاه و یکمین کنفرانس سالانه ریاضی ایران، دانشگاه کاشان، ۲۸ بهمن تا ۲ اسفند ۱۳۹۹، صص ۳۲۲ تا ۳۲۵.

۲۵. مریم رضایی کاشی و مجتبی بهرامیان، انتقال بی اطلاع با استفاده از ژاکوبین تعمیم یافته خم های بیضوی، پنجاه و یکمین کنفرانس سالانه ریاضی ایران، دانشگاه کاشان، ۲۸ بهمن تا ۲ اسفند ۱۳۹۹، صص ۱۴۸-۱۵۱.

۲۶. مریم رضایی کاشی و مجتبی بهرامیان، احراز هویت در رمزنگاری RSA، ششمین کنفرانس بین المللی ترکیبیات، رمزنگاری، علوم کامپیوتر و محاسبات، دانشگاه علم و صنعت ایران، ۲۶ آبان تا ۲۷ آبان ۱۴۰۰، صص ۴۹۳-۴۹۷.

## راهنمایی پروژه های کارشناسی

ردیف	عنوان	نام دانشجو	تاریخ ارائه
------	-------	------------	-------------

۹۱-۹۰	محمد مهدی ابراهیمی	زیر مدولهای ضعیفاً اول	۱
۹۳-۹۲	محمدسعید ملایی	قضیه پتانسیل جبری روی گرافها و ژاکوبی گرافها	۲

### راهنمایی و مشاوره پایان نامه های کارشناسی ارشد

تاریخ دفاع	نام دانشجو	عنوان پایان نامه	ردیف
۹۲/۱۰/۳۰	فریمان قائدی	مشبکه ها در نظریه جبری اعداد و کاربرد آن در رمزنگاری	۱
۹۴/۶/۳۱	محبوبه تخیر اردستانی	مولدهای خانواده ای از خمهای بیضوی با رتبه حداقل ۳	۲
۹۴/۱۰/۲۹	لیلا جاویدان	آزمونهای اول بودن بر اساس چنبره ها و خمهای بیضوی	۳
۹۴/۱۱/۲۷	مریم حبیبی زاده	محاسبه زوجیت تیت روی خمهای بیضوی	۴
۹۵/۱۱/۱۱	مریم رضایی	ساختارهای دسترسی طرحهای تسهیم راز ابربیضوی	۵
۹۶/۲/۳۱	شیمای بهزادی نژاد	کسرهای مسلسل متناوب و خمهای بیضوی روی میدانهای مربعی	۶
۹۴/۱۱/۲۷	زهرا پوردکان (استاد مشاور)	گراف مور و کاربردهای آن	۷
۹۶/۱۰/۱۸	رضا رئوفی نژاد	کلاسهای یکرخیختی خمهای دوچه-یککارت-کوهل روی میدانهای متناهی	۸
۹۴/۹/۷	محمد گندمکار رهقی (استاد مشاور)	عدد هم محیطی یک گراف	۹

۹۷/۶/۲۴	زهره صمدی کاشانی	خم‌های بیضوی روی حلقه‌های زنجیره‌ای	۱۰
۹۸/۱۱/۲۷	الهام حاجی رضایی	پروتکل انتقال بی اطلاع پساکوانتومی با استفاده از همسانی های خم بیضوی سوپرسینگولار	۱۱
۱۳۹۹/۶/۲۹	پروین باجلان	گراف‌های همسانی خم های بیضوی سوپرسینگولار روی میدان متناهی	۱۲
۱۳۹۹/۹/۹	الهام طیبی	یک الگوریتم حساب شاخص برای حل مسأله لگاریتم گسسته روی خم‌های بیضوی میدان اول	۱۳
۱۳۹۹/۹/۱۱	نفیسه شمسی	یک طرح تسهیم راز تأییدپذیر مبتنی بر شبکه ها	۱۴
۱۴۰۱/۰۹/۲۰	مسعود معماری	یک طرح امضای چندمتغیره شناسه مبنای بهبودیافته بر اساس رنگین کمان	۱۵
۱۴۰۱/۱۱/۱۱	اسما ملاحسنی	امضای گروهی ایمن و کارآمد مبتنی بر رمزنگاری کلید عمومی چندمتغیره	۱۶
۱۴۰۱/۱۱/۲۵	عطیه مؤمنی راوندی	یک الگوریتم امضای رقمی خم بیضوی مؤثر برای زنجیره ی بلوکی	۱۷
۱۴۰۱/۱۱/۳۰	مریم فرزانه	یک طرح امضای شناسه-مبنای پساکوانتومی بر اساس همسانی‌ها	۱۸

### راهنمایی و مشاوره پایان‌نامه‌های دکتری

ردیف	عنوان پایان‌نامه	نام دانشجو	تاریخ دفاع
۱	سیستم‌های رمزنگاری کلید عمومی بر اساس خم‌های بیضوی	مریم شیخی گرجان	۱۳۹۸/۴/۱۱
۲	طرح تسهیم راز مبتنی بر خم‌های بیضوی	خدیجه اسلامی	۱۳۹۹/۷/۱۴