# Mijtaba Bahramian

Assistant Professor

College: Faculty of Mathematics

Department: Pure Mathematics

## Education

| Degree | Graduated in | Major | University |
|---|---|---|---|
| BSc | 1999 | Pure Mathematics | University of Kashan |
| MSc | 2001 | Pure Mathematics-Non Commutative Algebra | Sharif University of Technology |
| Doctoral | 2010 | Pure Mathematics- Algebra | University of Kashan |

## Employment Information

| Faculty/Department | Position/Rank | Employment Type | Cooperation Type | Grade |
|---|---|---|---|---|
| University of kashan | | Tenure Track | Full Time | |

## Conferences

عضو کمیته‌ی اجرایی پنجمین کنفرانس ترکیبیات جبری و نظریه گراف (تیر 91)

عضو کمیته‌ی اجرایی اولین کنفرانس نظریه محاسباتی اعداد و کاربردهای آن (آذر 93)

عضو کمیته‌ی علمی اولین کنفرانس نظریه محاسباتی اعداد و کاربردهای آن (آذر 93)

دبیر اجرایی دومین کنفرانس نظریه محاسباتی اعداد و کاربردهای آن (مهر 94)

عضو کمیته‌ی علمی دومین کنفرانس نظریه محاسباتی اعداد و کاربردهای آن (مهر 94)

## Papers in Conferences

1. Maryam Rezaei Kashi و Mojtaba Bahramian،انتقال بی‌اطلاع با استفاده از ژاکوبین تعمیم‌یافته خم‌های
st Annual Iranian Mathematics Conference،۱۵۱-۱۴۸ شماره صفحات،Kashan،۲۰۲۱ ۰۲ ۱۶.
بیضوی،۵۱
2. Mojtaba Bahramian و Elham HajiRezaei،رمزنگاری شناسه کاربری با استفاده از ژاکوبین تعمیم یافته خم‌های
st Annual Iranian Mathematics Conference،۳۲۵-۳۲۲ شماره صفحات،Kashan،۲۰۲۱ ۰۲ ۱۶.
بیضوی،۵۱
3. Mojtaba Bahramian،۹،نظریه گروهها در رمزنگاریth Iranian Group Theory Conferenc،۲۰۱۷ ۰۲ ۰۱.

4. Hassan Daghigh, Mojtaba Bahramian, Somayyeh Didari،گاهی به برخی مسائل ریاضی در رمزنگاری،The First Conference on Computational Group Theory, Computational Number Theory and Applications،Kashan،۲۰۱۴ ۱۲ ۱۷.
5. Mojtaba Bahramian،رمزنگاری امن با خم‌های بیضوی،اولین کنفرانس بین المللی فناوریهای نوین در علوم،Amol،۰۷ ۰۹ ۲۰۱۷.
6. Khadijeh Eslami, Mojtaba Bahramian ,A Threshold Multi-Secret Sharing Scheme Based on Shamir's Scheme ,اولین کنفرانس بین المللی فناوریهای نوین در علوم ,Amol ,2017 09 07.
7. Khadijeh Eslami, Mojtaba Bahramian ,An Identity-Based Encryption Based on Pairings over Elliptic Curves ,48th Annual Iranian Mathematics Conference ,Hamedan ,2017 08 22.
8. Mojtaba Bahramian ,RSA Scheme over the Ring of Gaussian Integers ,48th Annual Iranian Mathematics Conference ,Hamedan ,2017 08 22.
9. Mojtaba Bahramian, Khadijeh Eslami ,Secret Sharing Scheme ,9th Iranian Group Theory Conferenc ,Kashan ,2017 02 01.
10. Mojtaba Bahramian, Khadijeh Eslami ,Secret Sharing Scheme ,9th Iranian Group Theory Conferenc ,Kashan ,2017 02 01.
11. Khadijeh Eslami, Mojtaba Bahramian ,GENERALIZED JACOBIAN CRYPTOSYSTEMS ,First International Conference on Combinatorics, Cryptography and Computation ,Noor ,2016 09 01.
12. Mojtaba Bahramian ,Certificate-Based Encryption Scheme ,First International Conference on Combinatorics, Cryptography and Computation ,2016 09 01.
13. Mojtaba Bahramian, Maryam Sheikhi ,An identity-based encryption scheme ,The Second Conference on Computational Group Theory, Computational Number Theory and Applications ,Kashan ,2015 10 13.
14. Mojtaba Bahramian ,Jacobian group of Cocktail Party ,The Second Conference on Computational Group Theory, Computational Number Theory and Applications ,Kashan ,2015 10 13.
15. Mojtaba Bahramian, Maryam Sheikhi, Fatemeh Seyfi ,Secret Sharing Based on Elliptic Curves ,همایش The First Conference on Computational Group Theory, Computational Number Theory and Applications ,Kashan ,2014 12 17.
16. Mojtaba Bahramian, Hassan Daghigh, Somayyeh Didari ,Constructing Elliptic Curves for Cryptography ,The First Conference on Computational Group Theory, Computational Number Theory and Applications ,Kashan ,2014 12 17.
17. Mojtaba Bahramian, Hassan Daghigh, Somayyeh Didari ,Calculus on Elliptic Curves ,The First Conference on Computational Group Theory, Computational Number Theory and Applications ,Kashan ,2014 12 17.
18. Mojtaba Bahramian ,Discrete logarithm Problem ,24th Iranian Algebra Seminar ,Tehran ,2014 11 12.
19. Mojtaba Bahramian ,Computing the Tate Pairing using Generalized Jacobians ,The 45th Annual Iranian Mathematics Conference ,Semnan ,2014 08 26.

## Papers in Journals

1. Maryam Rezaei Kashi و Mojtaba Bahramian،Proof of Knowing the Prime Factors of a Number Using Zero-Knowledge Proof،Iranian Journal of Mathematical Sciences and Informatics،شماره صفحات ۳۳-۴۶،۲۰۲۱.
2. Mojtaba Bahramian،مروری بر رمزنگاری خم‌های بیضوی،فرهنگ و اندیشه ریاضی،۰ ۰ ۰۱.
3. 6. Khadijeh Eslami ,& Mojtaba Bahramian,An ECDLP-Based Verifiable Multi-Secret Sharing Scheme,Math. Interdisc. Res.,Vol. 5,pp. 193-206,2020.
4. Mojtaba Bahramian ,& Elham Hajirezaei,An Identity-Based Encryption Scheme using Isogeny of Elliptic Curves,,FACTA UNIVERSITATIS (NI),Vol. 5,No. 35,pp. 1451-1460,2020.
5. Mojtaba Bahramian, Khadijeh Eslami,A New Verifiable Multi-Secret Sharing Scheme based on Elliptic Curves and Pairings,Italian journal of pure and applied mathematics,Vol. 41,pp. 456-468,2019 1 1.
6. Mojtaba Bahramian, Maryam Sheyki, Christophe Doche,A Threshold Verifiable Multi-Secret

Sharing Based on Elliptic Curves and Chinese Remainder Theorem,IET Research Journals (IET Information Security),2019 01 1.
7. Mojtaba Bahramian, Khadijeh Eslami,An Efficient threshold Verifiable Multi-secret Sharing Using Generalized Jacobian of Elliptic Curves,Algebraic Structures and Their Applications,Vol. 4,No. 2,pp. 45-55,2017 01 01.
8. Mojtaba Bahramian, Hassan Daghigh,A generalized fibonacci sequence and the diophantine equations,Iranian Journal of Mathematical Sciences and Informatics,Vol. 8,No. 2,pp. 111-121,2013 01 01.
9. Hassan Daghigh, Mojtaba Bahramian,Generalized Jacobian and Discrete logarithm Problem on Elliptic Curves,Iranian Journal of Mathematical Sciences and Informatics,Vol. 4,No. 2,pp. 55-64,2009 01 01.