Mojtaba Bahramian
Department of Pure Mathematics
Faculty of Mathematical Sciences
University of Kashan
Kashan, Iran
Tel.: +98-31-55912327
E-Mail: bahramianh@kashanu.ac.ir
https://faculty.kashanu.ac.ir/bahramian/fa.

1. PERSONAL Data

Name: Mojtaba
Last Name: Bahramian
D.O.B: June 12, 1976
Current Position: Assistant Professor, Department of Pure mathematics, University of Kashan
Postal Address: Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, P.O Box 87317-51167, Kashan, Iran
Email: bahramianh@kashanu.ac.ir
Phone: +98-31-55912559

2. Educational Information

Grade	Graduated At	Major	University
BSc	1999	Mathematics Education	University of Kashan
MSc	2001	Algebra	Sharif University of Technology
Doctoral	2010	Number Theory	University of Kashan

3. QUALIFICATIONS/ HONORS/ AWARDS/ ASSOCIATION MEMBERSHIP

1. Diploma in Mathematical Sciences, 1994
2. B. Sc in Pure Mathematics, 1999
3. M.Sc in Pure Mathematics (Algebra), 2001
4. Ph.D in Pure Mathematics (Representation theory of Algebras), 2010
5. Top Student in B. Sc Class
6. Ranked first in Ph.D entrance exam (University of Kashan), 2004
7. Chosen in the 22-th National Mathematics Student Competitions (University of Shahid Chamran-Ahvaz), 1997
8. Chosen in the 23-th National Mathematics Student Competitions (Sharif University of Technology-Tehran), 1998
9. Exemplary Teacher Award University, 2013
10. Exemplary Teacher Award University, 2019
11. Exemplary Teacher Award University, 2022

4. RESEARCH INTERESTS

1. Number Theory
2. Cryptography

5. Publications

5.1. Journal Publications:

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 x2 ± kxy − y2 ± 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, (submitted)

8. M. Bahramian and E. Hajirezaei, An Identity-Based Encryption Scheme using Isogeny of Elliptic Curves, FACTA UNIVERSITATIS (NIŠ), Ser. Math. Inform.

9. M. Bahramian and M. Rezaei Kashi, Proof of Knowing the Prime Factors of a Number Using Zero-Knowledge Proof, Iranian Journal of Mathematical Sciences and Informatics, (English version)

10. Khadijeh Eslami and Mojtaba Bahramian, An Isogeny-based Quantum-resistant Secret Sharing Scheme, Filomat, Vol. 36, No. 10, 2022, 3249-3258.

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

۱۲.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(اسفند۹۹)، صص. ۳۳ تا ۴۶. (نسخه فارسی)

5.2. Conference papers:

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 49th 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، ۲۹ آبان ۱۳۹۸، صص ۱۱۱۳-۱۱۲۳.

۲٤. الهام حاجی رضایی و مجتبی بهرامیان، رمزنگاری شناسه کاربری با استفاده از ژاکوبین تعمیم یافته خم‌های 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 بی‌اطلاع با استفاده از ژاکوبین تعمیم‌یافته خم‌های بیضوی، پنجاه و یکمین کنفرانس سالانه ریاضی ایران، دانشگاه کاشان، ۲۸ بهمن تا ۲ اسنفند ۱۳۹۹، صص ۱٤۸-۱٥۱.

۲٦. مریم رضایی کاشی و مجتبی بهرامیان، احراز هویت در رمزنگاریRSA ، ششمین کنفرانس بین المللی ترکیبیات، رمزنگاری، علوم کامپیوتر و محاسبات، دانشگاه علم و صنعت ایران، ۲٦ آبان تا ۲۷ آبان ۱٤۰۰، صص ٤۹۳-٤۹۷.

- **Supervision experiences**
  - **I. Ph.D. students**
    1. **Maryam Sheikhi Garjan**, Public key cryptosystems based on elliptic curves, 07.2019
    2. **Khadijeh Eslami**, Secret Sharing based on Elliptic Curves, 10.2020
    3. **Maryam Rezaei Kashi**, Zero-knowledge proof for identification in cryptographic systems, proposing and elliptic curve key exchange protocol and its application in oblivious transfer, 2023 (in the process of writing her doctoral thesis)
    4. **Elham Haji Rezaei**, (in progress).
    5. **Hoseyn Soltani**, (in progress).

  - **II. Masters Students**
    1. **Fariman Ghaedi**, Lattices in algebraic number theory and its application in cryptography, 01.2014
    2. **Mahboobeh Takhayor**, Generators for the family of elliptic curves of rank at lead three, 09.2015
    3. **Leila Javidan**, Primality tests based on elliptic curves, 01.2016
    4. **Maryam Habibizadeh**, Computation of the tate pairing on elliptic curves, 02.2016
    5. **Maryam Rezaei Kashi**, Hyperelliptic secret sharing schemes, 01.2017
    6. **Shima behzadinejad**, Continued fractions and elliptic curves, 05.2017
    7. **Reza Raoufi nejad**, Isomorphism classes of Doche-Icart-Kohel curves, 01.2018

8. **Zohre Samadi Kashi**, Elliptic curves over chain rings, 09.2018
9. **Elham Haji Rezaei**, Post-quantum oblivious transfer protocol using isogenies of supersingular elliptic curves, 02.2020
10. **Parvin Bajelan**, Isogeny graphs of supersingular elliptic curves, 09.2020
11. **Elham Tayyebi**, Index calculus algorithm and discrete logarithm on elliptic curves, 11.2020
12. **Nafiseh Shamsi**, Secret sharing scheme based on lattices, 12.2020
13. **Masoud Maemari**, Identity-based multivariate signature scheme, 12.2022
14. **Asma Mollahasani**, Group signature scheme based on multivariate public key cryptography, 01.2023
15. **Atiyeh momeni**, Elliptic Curve Digital Signature Algorithm for Blockchain, 02.2023
16. **Maryam Farzane**, Post-quantum identity-based signature scheme based on isogeny of elliptic curves, 02.2023
17. **Khatereh Reisi**, in progress.

III. Bachelor projects

1. **Mohammad Ebrahimi**, On weakly prime submodules, 02-2012.
2. **Mohammad Saeid Mollaei**, Algebraic potential theory on graphs and the Jacobian, 06-2014.