



# Kaveh Dastouri

✉ [kavehdastouri45@gmail.com](mailto:kavehdastouri45@gmail.com)

✉ [k.dastouri@bicmr.pku.edu.cn](mailto:k.dastouri@bicmr.pku.edu.cn)

☎ +8615611855483

🌐 [ResearchGate](#)

🌐 [ORCID](#)

🌐 [Personal Webpage](#)

## EDUCATION

---

PhD	Tarbiat Modares University, Tehran, Iran <i>Field:</i> Algebra <i>Thesis:</i> "Monomial characters and structure of finite groups" <i>Supervisor:</i> Prof. Ali Iranmanesh <i>Advisor:</i> Prof. Mohsen Ghasemi	2020 – 2023
MS	University of Tabriz, Tabriz, Iran <i>Field:</i> Algebra <i>Thesis:</i> "Irreducible characters of even degree and normal Sylow 2-subgroups" <i>Supervisor:</i> Prof. Kamal Aziziheris	2017 – 2020
BS	Farhangian University, Iran <i>Field:</i> Mathematics Education	2013 – 2017

## RESEARCH EXPERIENCE

---

Research Stay	RPTU Kaiserslautern-Landau, Germany Host: Prof. Günter Malle.	Jul 2026 – Dec 2026
Postdoc	Beijing International Center for Mathematical Research (BICMR), Peking University Supervisor: Prof. Jiping Zhang	Dec 2025 – present
Postdoc	Department of Pure Mathematics, Tarbiat Modares University Supervisor: Prof. Ali Iranmanesh	Jun 2024 – Sep 2025

## HONORS AND AWARDS

---

DAAD Research Grant (German Academic Exchange Service) Competitive research scholarship for a six-month research in Germany.	2026
Highest GPA among PhD Students Highest grade point average among algebra PhD students at Tarbiat Modares University.	2024
Qualified as an "Exceptional Talent" PhD Student Exempt from the entrance exam, Tarbiat Modares University.	2020

## PUBLICATIONS

---

### Journal Papers

- [1] Kaveh Dastouri. *Symmetric Group-Based Public-Key Cryptosystem with Large Prime Moduli*. Cryptology ePrint Archive, Paper 2025/1589. 2025. URL: <https://eprint.iacr.org/2025/1589>.
- [2] Kaveh Dastouri and Mohsen Ghasemi. “Groups with prime power Isaacs  $\pi$ -partial character codegrees.” (Journal of Algebra and Its Applications). 2025. URL: <https://doi.org/10.1142/S0219498827500897>.
- [3] Kaveh Dastouri and Ali Iranmanesh. “Primes and degrees of Isaacs  $\pi$ -partial characters.” In: *Communications in Algebra* 53.6 (2025), pp. 2523–2527. DOI: [10.1080/00927872.2024.2446543](https://doi.org/10.1080/00927872.2024.2446543). eprint: <https://doi.org/10.1080/00927872.2024.2446543>. URL: <https://doi.org/10.1080/00927872.2024.2446543>.
- [4] Kaveh Dastouri, Ali Iranmanesh, and Mohsen Ghasemi. “Monomial Isaacs  $\pi$ -partial characters and derived length.” In: *Journal of Algebra and Its Applications* 24.04 (2025), p. 2550108. DOI: [10.1142/S0219498825501087](https://doi.org/10.1142/S0219498825501087). eprint: <https://doi.org/10.1142/S0219498825501087>. URL: <https://doi.org/10.1142/S0219498825501087>.
- [5] Kaveh Dastouri, Ali Iranmanesh, and Mohsen Ghasemi. “Primes and Degrees of Isaacs  $\pi$ -partial Character II.” (Submitted). 2025.

## Preprints

1. K. Dastouri, “A Symmetric Group-Based Public-Key Cryptosystem with Hard-to-Factor One-Way Function,” (submitted).
2. K. Dastouri and A. Iranmanesh, “Some Combinatorial Applications of Symmetric Group Representations,” (submitted).
3. K. Dastouri, “Reconstruction of Permutation Sets from Their Decks Up to Conjugation,”
4. K. Dastouri and A. Iranmanesh, “Permutations of the Symmetric Group and Hamiltonian Cycles,” (submitted).

## Conference Papers

1. K. Dastouri, A. Molkhasi, “Pseudocomplements in free groups”, The 4th Seminar on Algebra and its Applications, August 9-11, 2016.
2. K. Dastouri, A. Iranmanesh, “Primes and degrees of Isaacs  $\pi$ -partial character”, 15th International Group Theory Conference of Iran, February 9-10, 2023.
3. K. Dastouri, A. Iranmanesh, “Some results of Isaacs  $\pi$ -partial character degrees”, 4th International Conference on Computational Algebra, Computational Number Theory and Applications, July 4-6, 2023.
4. K. Dastouri, A. Iranmanesh, “On monomial Isaacs  $\pi$ -partial characters of  $\pi$ -separable groups”, 7th Biennial International Group Theory Conference, August 7-11, 2023.
5. K. Dastouri, A. Iranmanesh, M. Ghasemi, “Groups whose all Isaacs  $\pi$ -partial characters are monomial”, 16th International Group Theory Conference of Iran, February 1-2, 2024.
6. K. Dastouri, A. Iranmanesh, “Representation theory of symmetric groups and some combinatorial results”, 12th Graph Theory and Algebraic Combinatorics, February 7-8, 2024.
7. K. Dastouri, A. Iranmanesh, “برخی نتایج در مورد نتایج درجات سرشت های مونولیتیک”, 55th Annual Iranian Mathematics Conference, August 14-16, 2024.
8. A. Iranmanesh, K. Dastouri, “ $\pi$ -structure and  $\pi$ -characters”, 17th International Group Theory Conference of Iran, January 29-30, 2025.

## RESEARCH INTERESTS

---

Representation Theory of Finite Groups: ordinary and modular cases  
Finite Groups and Their Applications  
Public-Key Cryptosystem Design: leveraging hard computational representation problems

## TEACHING EXPERIENCE

---

Teaching Assistant	Tarbiat Modares University, Tehran, Iran <i>Courses:</i> Representation Theory of Finite Groups, Abstract Algebra Lecturer: Prof. Ali Iranmanesh	2020 – 2024
High School Teacher	Various High Schools, Iran Mathematics instructor for 7 years	2013 – 2020

## COMPUTER SKILLS

---

GAP	Advanced
SageMath	Intermediate
Python (NumPy, TensorFlow, Keras)	Familiar
L <sup>A</sup> T <sub>E</sub> X	Advanced
Microsoft Office	Advanced
Linux	Familiar

## LANGUAGES

---

Persian Native  
English Upper Intermediate (C1)  
German Basic (A1)

## REFERENCES

---

### **Prof. Ali Iranmanesh**

Faculty of Mathematical Sciences, Tarbiat Modares University, Iran  
Email: [iranmana@modares.ac.ir](mailto:iranmana@modares.ac.ir)

### **Prof. Jiping Zhang**

School of Mathematical Sciences, Peking University, China  
Email: [jzhang@pku.edu.cn](mailto:jzhang@pku.edu.cn)

### **Prof. Mohammad Reza Darafsheh**

School of Mathematics, Statistics and Computer Science, University of Tehran, Iran  
Email: [darafsheh@ut.ac.ir](mailto:darafsheh@ut.ac.ir)

### **Dr. Ali Rajaei**

Faculty of Mathematical Sciences, Tarbiat Modares University, Iran  
Email: [alirajaei@modares.ac.ir](mailto:alirajaei@modares.ac.ir)