Curriculum Vitae

Omran Ahmadi

January 12, 2025

http://math.ipm.ac.ir/~emran/
oahmadid@ipm.ir

School of Mathematics, IPM
Niavaran square,
Tehran, Iran

Contents

1 Research Interests 1
2 Academic appointments 1
3 Education 2
4 Publications 2
5 Honors and Awards 4
6 Teaching Experience 5
7 Postdocs, students and graduate committees 5
8 Administrative Experience 6
9 Editorial boards, Professional Services 7
10 Research visits 7
11 Talks 8

1 Research Interests

Arithmetic algebraic geometry, Number theory, Cryptography and Combinatorics; more specifically: Distribution of points on algebraic sets and varieties, Exponential and character sums, Arithmetic of finite fields, Curve based cryptography, Algebraic graph theory, Sparse polynomials over finite fields, Extremal combinatorics

2 Academic appointments

- **Institute for research in fundamental sciences (IPM)**, Tehran, Iran.
  Associate Professor of Mathematics (with Tenure), June 2016 – present.
- **Institute for research in fundamental sciences (IPM)**, Tehran, Iran.
  Senior research fellow (tenure track), School of Mathematics, Jun. 2012 – Jul. 2016.

- **University college Dublin**, Dublin, Ireland.
  Postdoctoral research fellow, Sep. 2008 – May. 2012.

- **University of Waterloo**, Waterloo, Canada.
  Postdoctoral research fellow, Sep. 2007 – Aug. 2008.

- **University of Toronto and Fields Institute**, Toronto, Canada.
  Postdoctoral research fellow, Sep. 2006 – Aug. 2007.

3 Education

- **University of Waterloo**, Waterloo, Canada.
  Ph.D. in Mathematics, January 2002 – August 2006.
  Dissertation Topic: "Distribution of Irreducible Polynomial over Finite Fields".
  Advisor: Alfred Menezes.

- **University of Tehran**, Tehran, Iran.
  M.Sc. in Mathematics, September 1997 – August 1999.
  Dissertation Topic: "Growth Sequences in Groups".
  Advisor: Mohammad Reza Darafsheh.

- **University of Tehran**, Tehran, Iran.
  B.Sc. in Electronics Engineering, September 1993 – August 1997.

4 Publications

Invited Book Chapters

2. O. Ahmadi. *Weight distribution of irreducible polynomials over finite fields.* Handbook of Finite Fields and Their Applications, G. L. Mullen and D. Panario, Editors, CRC Press, pp 70–73, 2013.

1. O. Ahmadi and G. McGuire. *Curves over finite fields and linear recurring sequences.* Surveys in Combinatorics 2015, Cambridge University Press, pp 195–218, 2015.

Journal Papers

26. O. Ahmadi and A. Menezes. *On the number of trace-one elements in polynomial bases for* $\mathbb{F}_{2^n}$*.* Designs, Codes and Cryptography, 37, 493–507, 2005.

25. O. Ahmadi. *Self-reciprocal irreducible pentanomials over* $\mathbb{F}_2$*.* Designs, Codes and Cryptography, 38, 395–397, 2006.

24. O. Ahmadi. *On the distribution of irreducible trinomials over* $\mathbb{F}_3$*.* Finite Fields and Their Applications, 13, 659–664, 2007.

23. O. Ahmadi and A. Menezes. *Irreducible polynomials of maximum weight.* Utilitas Mathematica, 72, 111–123, 2007.

22. O. Ahmadi, D. Hankerson and A. Menezes. *Formulas for cube roots in $\mathbb{F}_{3^m}$.* Discrete Applied Mathematics, 155, 3, 260–270, 2007.

21. O. Ahmadi. *The trace spectra of polynomial bases for $\mathbb{F}_{2^n}$".* Applicable Algebra in Engineering, Communication and Computing, 18, 391–396, 2007.

20. O. Ahmadi and I. Shparlinski. *Geometric progressions in sumsets over finite fields.* Monatshefte fur Mathematik, 152, 177–185, 2007.

19. O. Ahmadi and I. Shparlinski. *Distribution of matrices with restricted entries over finite fields.* Indagationes Mathematicae, vol. 18, Issue 3, pp 327–337, 2007.

18. O. Ahmadi and G. Vega. *On the parity of the number of the irreducible factors of self-reciprocal polynomials over finite fields.* Finite Fields and Their Applications, vol. 14, Issue 1, pp 124–131, 2008.

17. O. Ahmadi, D. Hankerson and F. Rodriguez- Henriquez. *On parallel formulations of scalar multiplications on Koblitz curves.* JUCS, Special Issue on Cryptography in Computer System Security, Springer, vol 14, Issue 3, pp 481–504, 2008.

16. O. Ahmadi, N. Alon, I. Blake and I. Shparlinski. *Graphs with integral spectrum.* Linear Algebra and Its Applications, Vol. 430, Issue 1, pp 547–552, 2009.

15. O. Ahmadi, I. Shparlinski and J. F. Voloch. *Multiplicative order of Gauss periods.* International Journal of Number Theory, Vol. 6, Issue 4, pp 877–882, 2010.

14. O. Ahmadi and I. Shparlinski. *Bilinear exponential sums and sum-product problem on elliptic curves.* Proceedings of the Edinburgh Mathematical Society, Vol. 53, No. 1, pp 1–12, 2010.

13. O. Ahmadi and I. Shparlinski. *On the distribution of the number of points on algebraic curves in extensions of finite fields.* Mathematical Research Letters, Vol. 17, No 4, pp 689–699, 2010.

12. O. Ahmadi and Francisco Rodriguez-Henriquez. *Low complexity cubing and cube root computation over $\mathbb{F}_{3^m}$ in polynomial basis.* IEEE Transactions on Computers, Vol. 59, Issue 10, pp 1297–1308, 2010.

11. O. Ahmadi. *Generalization of a theorem of Carlitz.* Finite Fields and their Applications, Vol.17, Issue 5, pp 473–480, 2011.

10. O. Ahmadi and R. Granger. *On isogeny classes of Edwards curves over finite fields.* Journal of Number Theory, Vol. 132, Issue 6, pp 1337–1358, 2012.

9. O. Ahmadi, F. Luca, A. Ostafe and I. Shparlinski. *On stable quadratic polynomials.* Glasgow Mathematical Journal, Vol. 54, no. 2, pp 359–369, 2012.

8. O. Ahmadi and R. Granger. *An efficient deterministic test for Kloosterman zeros.* Mathematics of Computation, , Vol. 83, pp 347–363, 2014.

7. O. Ahmadi and I. Shparlinksi. *Exponential sums over points of elliptic curves.* Journal of Number Theory, Vol. 140, pp 299–313, 2014.

6. O. Ahmadi, G. McGuire and A. Rojas Leon. *Decomposing jacobians of curves over finite fields in the absence of algebraic structure.* Journal of Number Theory, Vol. 156 ,pp 414–431, 2015.

5. O. Ahmadi and A. Mohammadian. *Sets with many pairs of orthogonal vectors over finite fields.* Finite Fields and their Applications, Vol. 37, pp 179–192, 2016.

4. O. Ahmadi, F. Gologlu, R. Granger, G. McGuire and E. Yilmaz. *Fibre Products of Supersingular Curves and the Enumeration of Irreducible Polynomials with Prescribed Coefficients.* Finite Fields and their Application, Vol. 42, November 2016, Pages 128–164.

3. G. Adj, O. Ahmadi and A. Menezes. *On isogeny graphs of supersingular elliptic curves over finite fields.* Finite Fields and their Application, Vol. 55, January 2019, Pages 268–283.

2. O. Ahmadi and K.M. Shokri. *A note on stable trinomials over finite fields.* Finite Fields and their Application, Vol. 63, March 2020, 13 pages.

1. O. Ahmadi and M. Shafaeiabr. *Difference sets and three-weight linear codes from trinomials.* Finite Fields and their Applications, Vol. 89, August 2023, 36 pages.

Papers in Conference Proceedings

1. O. Ahmadi, D. Hankerson and A. Menezes. *Software implementation of the arithmetic in* $\mathbb{F}_{3^m}$*.* Proceedings of WAIFI 2007, LNCS, vol. 4547 Springer-Verlag, Berlin, 2007, 85–102.

Submitted papers and preprints.

- O. Ahmadi and A. Najafi. *On the Learnability of Convex Bodies.* preprint.
- O. Ahmadi. *Few weight codes from hyperovals: Resolution of a Conjecture of Cunsheng Ding.* In preparation.
- O. Ahmadi and K.M. Shokri. *BCH codes, m-sequences and intersection of Fermat hypersurfaces.* preprint.

Publications in Persian (unrefereed)

2. O.Ahmadi. *Gödl prize winners of 2013.* IPM Newsletter, Vol. 20, No. 1, pp 14–15, 2013.

1. O. Ahmadi. *Cryptography and discrete logarithm problem.* IPM Newsletter, Vol. 20, No2, pp 18–21, 2013.

5 Honors and Awards

- Outstanding Teaching Assistant Award, University of Waterloo, Canada, Spring 2006.
- Silver Medal, International Mathematical Olympiad, Istanbul, Turkey, 1993.
- Gold Medal, National Olympiad in Mathematics, Iran, 1993.

6 Teaching Experience

- **Instructor:**
  - **Courses taught at IPM, Tehran, Iran:** Post-quantum Cryptography: Code-based Cryptography, Algebraic Curves, Finite Fields, Algebraic Function Fields and Codes, Topics in Cryptography, Elliptic Curves, Introduction to Public Key Cryptography, Large Networks and Graph Limits, A Short Course on Pairing Based Cryptography, Mathematics of Public Key Cryptography.
  - **Courses taught at the university of Waterloo, Waterloo, Canada:** Introduction to Combinatorics, Linear Algebra II.
  - **Courses taught at various high schools in Iran, 1999-2001:** Elementary number theory, Geometry, Combinatorics, Real analysis.
  - Preparing high school students in Iran and Ireland for national and international mathematical Olympiads.
- **Teaching Assistant:** Responsibilities included holding office hours, grading, and tutoring. I assisted students with Algebra, Calculus, Introduction to Graph Theory, Linear Optimization, Applied Cryptography, Network Flow Theory, Mathematics of Public Key Cryptography, Deterministic Operation Research Models.

7 Postdocs, students and graduate committees

- **Postdocs**
  - Ali Mohammadi, Sep 2019–Sep 2022.
  - Farzad Aryan, Sep 2022–present.
  - Mohsen Bayat, Jan 2023–Jan 2024. Funded by Iranian National Science Foundation.
- **Graduate Students**
  - **PhD Students**
    - Supervision of Masoud Shafaeiabr, Ongoing.
    - Supervision Hassan Norouzi, Ongoing.
  - **Master Students**
    Since my employer is a research institute and we do not have an undergraduate and masters program, the master students that I have advised or co-advised have been affiliated with other institutions in Iran.
    - Soheila Sabbaghian, Thesis title: Permutation polynomials over finite fields, Isfahan University of Technology, Isfahan, Iran, 2017.
    - Tahereh Mohammadbeigi Dehghani, Thesis title: HIMMO, A key distribution scheme, Isfahan University of Technology, Isfahan, Iran, 2016.
    - Marjan Amini, Thesis title: Efficient pairing computation on elliptic curves, Isfahan University of Technology, Isfahan, Iran, 2015.

    - Rasoul Ghafarian, Thesis title: Four dimensional Gallant-Lambert-Vanstone scalar multiplication, Isfahan University of Technology, Isfahan, Iran, 2015.
    - Abolfazl Salemi, Thesis title: Lattice ideals in cryptography, University of Tehran, Tehran, Iran, 2014.
    - Mozhgan Jamali, Thesis title: Speeding up integer factorization by elliptic curve method using Edwards curves, Shahid Beheshti University, Tehran, Iran, 2014.
    - Mina Shamkani Mashhadi, Thesis title: Edwards' normal form for elliptic curves, Shahid Beheshti University, Tehran, Iran, 2013.
  - **Undergraduate Students**
    - Vladimir Soukharev, Project title: Edwards curves, University of Waterloo, Waterloo, Canada, 2008.

- **Graduate committees**
  - **PhD thesis examiner**
    - Reza Kaboli, Sharif University of Technology, Tehran, Iran, 2022.
    - Mojtaba Fadavi, Isfahan University of Technology, Isfahan, Iran, 2020.
    - Sara Sheikhi, University of Kashan, Kashan, Iran, 2019.
    - Ahmad Bourghani Farahani, Sharif University of Technology, Tehran, Iran, 2018.
  - **Master thesis examiner**
    - Mohamed Wafik Elsheikh, Sabanci University, Turkey, 2022.
    - Maedeh Ghorbani (2021), Ruhollah Mirzaei (2021), Hanieh Gheisari (2020), Peyman Shahbazi (2019), Maryam Mohammadkarimi (2019), Yusof Karimi (2019), Amirmohammad Kachkhali (2019), Simin Esteki (2018), Mohammad Ali Asadi (2016), Marzieh Ghasemi (2015), Sahel Darabi (2015), Mehran Hosseini (2015), All from Isfahan University of Technology, Tehran, Iran.

8 Administrative Experience

- **Scientific Council Member:** School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran, 2019–present.
- **Hiring Committee Member:** School of Mathematics, IPM, Tehran, Iran, 2013–present.
- **Chair of Combinatorics and Computing Group:** School of Mathematics, IPM, Tehran, Iran, 2020–present.
- **Scientific Council Member:** Algebra and Number Theory Group, School of Mathematics, IPM, Tehran, Iran, 2020–present.
- **Scientific Council Member:** IPM Combinatorics and Computing Group, School of Mathematics, IPM, Tehran, Iran, 2020–present.

9 Editorial boards, Professional Services

- **Editorial board membership**
  - Editorial board member of Designs, Codes and Cryptography, 2017 – present.
  - Section editor of Number theory, Cryptography and Combinatorics of the Bulletin of the Iranian Mathematical Society, 2022 – present.
- **Program Committees**
  - **Scientific committee Member:** Workshop on the Arithmetic of Finite Fields (WAIFI) 2008, Siena, Italy, July 6–9, 2008.
  - **Organizing and Scientific Committee Member:** IPMCCC 2015, IPM Combinatorics and Computing Conference, Apr. 29–30, 2015.
  - **Organizing and Scientific Committee Member:** IPMCCC 2017, IPM Combinatorics and Computing Conference, May 16–18, 2017.
  - **Organizing and Scientific Committee Member:** IPMCCC 2021, IPM Combinatorics and Computing Conference, May 17–20, 2021.
- **Organized Workshops**
  - **Chair of Conference:** IPMCCC 2019, IPM Combinatorics and Computing Conference, Apr. 16–18, 2019.
  - **Organizing Committee Member:** Spring School on Analytic Number Theory, May 24–31, 2016. (Co-organizer with Regis De la Breteche)
- **Refereeing**
  - **Reviewer:** Mathematical Reviews, Since 2007.
  - **Reviewer:**
    - **Mathematics Journals:** Acta Mathematica Sinica; Designs, Codes and Cryptography; Discrete Mathematics; Finite Fields and Their Applications; Graphs and Combinatorics; Journal of Number theory; Journal of Mathematical Cryptology; Linear Algebra and its Applications; Mathematics of Computation, Monatshefte fuer Mathematik; SIAM Journal on Discrete Mathematics ; Math Slovaca.
    - **Engineering and Computer Science Journals:** IEEET on Computers, IEEET on Information Theory; IEEET on Wireless Communications; Information Processing Letters; International Journal of Computers and Applications; Journal of Computational and Applied Mathematics; Journal of Computers and System Sciences; Computación y Sistemas; IJEC (Iran)
    - **Conferences:** Asiacrypt 2005; WAIFI 2007; Eurocrypt 2008; CSR 2008 (Russia); Crypto 2009; Fq9; Fq11; LATIN 2010.

10 Research visits

- **Sabanci University**, Istanbul, Turkey, Apr 16 – Apr 21, 2022.

- **University of Surrey**, Guilford, UK, Oct 07 – Oct 15, 2019.
- **University of Waterloo**, Waterloo, Canada, Feb 1– Feb 28, 2019.
- **University of Waterloo**, Waterloo, Canada, Apr 28–Aug 8, 2017.
- **University College Dublin**, Dublin, Ireland, Oct. 4–17, 2015.
- **Institute Mittag-Leffler**, Stockholm, Sweden, July. 21–31, 2015.
- **Centre de Recerca Matematica (CRM)**, Barcelona, Spain, May 19–23, 2014.
- **Centre International Recontres Mathematiques (CIRM)**, Marseille, France, Feb. 3–7, 2014.
- **Johan Radon Institute for Computational and Applied Mathematics (RICAM)**, Linz, Austria, Dec. 9–13, 2013.
- **University of Waterloo**, Waterloo, Canada, May 11–21, 2013.
- **Banff International Research Center**, Banff, Canada, May 5–10, 2013.
- **University College Dublin**, Dublin, Ireland, Feb. 14– March 05, 2013.
- **University of Waterloo**, Waterloo, Canada, May 1–10, 2012.
- **University of Waterloo**, Waterloo, Canada, July 2011.
- **University of Waterloo**, Waterloo, Canada, July 2010
- **University of Waterloo**, Waterloo, Canada, Dec. 2006–Aug. 2007.
- **Banff International Research Center**, Banff, Canada, Nov. 18–23, 2006.
- **Banff International Research Center**, Banff, Canada, Nov. 5–10, 2005.

11 Talks

Invited Talks

- *Distribution of Irreducible Polynomials over Finite Fields.* IPM math colloquium, Tehran, Iran, Feb. 21, 2024.
- *Mathematics: Protector of your valuable zeros and ones.* Online talk. Maryam Mirzakhani Foundation, Iran, Nov 9, 2021.
- *Polynomials over Finite Fields.* Algebra Day, MathHouse, Isfahan, Iran, Oct 29, 2020.
- *Supersingular isogeny graphs.* University of Surrey, Guilford, UK, Oct 09, 2019.
- *M-sequences and Some Conjectures on Exponential Sums.* Antalya Algebra Days XX, Izmir, Turkey, May 16–20, 2018.

- *M-sequences and some conjectures on exponential sums.* Spring School on Algebraic Geometry, IPM, Tehran, Iran, Apr. 8–13, 2017.
- *Elliptic curve and finite field DLP.* AKU, Tehran, Iran, May 09, 2016.
- *Algebra and Cryptography.* KNTU, Tehran, Iran, Apr. 25, 2016.
- *Elliptic curve and finite field DLP.* Workshop on Foundation of Cryptography, SBU, Jan. 6–8, 2016.
- *BCH codes, m-sequences and Fermat hypersurfaces.* UCD, Dublin, Ireland, Oct. 12, 2015.
- *Discrete Logarithm Problem in Small Characteristic Finite Fields.* Faculty of Electrical Engineering, Sharif University of Technology, Tehran, Iran, Feb. 1, 2015.
- *Discrete Logarithm Problem in Finite Fields.* Shahid Beheshti University, Tehran, Iran, Oct 28, 2014.
- *Sets with Many Pairs of Orthogonal Vectors over Finite Fields.* CRM, Barcelona, May 19, 2014.
- *Discrete Logarithm Problem and Cryptography.* Sharif University of Technology, Tehran, Iran, May 5, 2014.
- *On a Conjecture on m-Sequences.* CIRM, Luminy, Marseille, Feb 7, 2014.
- *Equations over Finite Fields.* Sharif University of Technology, Tehran, Iran, Nov. 9, 2013.
- *Algebra and Cryptography.* TMU, Tehran, Iran, Nov. 5, 2013.
- *Algebra and Cryptography.* Algebra Day, Isfahan, Iran, Oct. 31, 2013.
- *Elements of Large Orders in Finite Fields.* Antalya Algebra Days, Izmir, Turkey, May 24, 2013.
- *Distributions of Matrices over Finite Fields.* UCD, Dublin, Ireland Feb 28, 2013.
- *Algebraic Curves in Communications.* IPM, Tehran, Iran, Jan. 23, 2013.
- *On Isogeny Classes of Edwards Curves.* Frontiers of Mathematics: A conference dedicated to Siavash Shahshahani, Sharif U. of Tech., Tehran, Iran, Dec 26, 2012.
- *Curve Based Cryptography.* SBU, Tehran, Iran; May 26, 2009.
- *Curve Based Cryptography.* IPM; Tehran, Iran; November 7, 2007.
- *Curve Based Cryptography.* KNT university of technology, Tehran, Iran; October 30, 2007.
- *Curve Based Cryptography.* Forth Iranian Society of Cryptology Conference; October 18, 2007.
- *Orders of Gauss Periods in Finite Fields.* Tutte seminar, Department of C& O, University of Waterloo; July 13, 2007.

- *Quadratic Transformation of Irreducible Polynomials over Finite Fields.* in the workshop "Polynomials over Finite Fields and Applications", Banff, Alberta, Canada; November, 2006.
- *Weight Distribution of Irreducible Polynomials over Finite Fields.* in the workshop "Number Theory Inspired by Cryptography", Banff, Alberta, Canada; Nov 9, 2005.

Contributed Talks

- *The slice-rank polynomial method in combinatorics.* IPM, Tehran, Iran, Dec 14, 2022.
- *Difference sets and tri-weight linear codes from trinomials over binary fields.* IPM, Tehran, Iran, Oct. 6, 2021.
- *Difference sets from finite fields.* IPM, Tehran, Iran, Oct. 8, 2020.
- *The stability of trinomials over finite fields.* IPM, Tehran, Iran, Nov. 27, 2019.
- *Isogeny Graphs.* IPM, Tehran, Iran, May 29, 2019.
- *Supersingular isogeny based Diffie-Hellman.* IPM, Tehran, Iran, May 16, 2018.
- *Cryptocurrencies.* IPM, Tehran, Iran, Oct. 25, 2017.
- *HIMMO key pre-distribution schemes.* IPM, Tehran, Iran, Apr. 12, 2017.
- *Irreducible polynomials with prescribed coefficients.* IPM, Tehran, Iran, Dec. 14, 2016.
- *Exponential and character sums over finite fields.* IPM, Tehran, Iran, Sep. 30, 2015.
- *DLP in small characteristic finite fields.* IPM, Tehran, Iran, Feb. 18, 2015.
- *Curves over Finite Fields and Linear Recurrence Sequences.* IPM, Tehran, Iran, Oct. 08, 2014.
- *Decomposing Jacobians of Curves over Finite Fields in the Absence of Algebraic Structure.* IPM, Tehran, Iran, May 08, 2014.
- *Equations over finite fields.* IPM, Tehran, Iran, Mar. 5, 2014.
- *Weights of Irreducible Polynomials over Finite Fields.* IPM, Tehran, Iran, Oct. 02, 2013.
- *Elements of large orders in Finite Fields.* IPM, Tehran, Iran, Apr. 17, 2013.
- *Generalization of a theorem of Carlitz.* IPM, Tehran, Iran, Oct. 10, 2012.
- *On Stable Quadratic Polynomials.* Department of Mathematical Sciences, UCD, Ireland, Number Theory Seminar; March 1, 2012.
- *On isogeny classes of Edwards curves over finite fields.* Department of Mathematical Sciences, UCD, Ireland, Algebra Seminar; February 14, 2011.
- *On the Distribution of the Number of Points on Algebraic Curves in Extensions of Finite Fields.* Department of Mathematical Sciences, UCD, Ireland, Number Theory Seminar; April 7, 2010.

- *Generalization of a theorem of Carlitz.* Department of Mathematical Sciences, UCD, Ireland, Algebra Seminar; March 22, 2010.
- *Orders of Gauss Periods in Finite Fields.* Ninth Conference on Finite Fields and Their Applications, UCD, Ireland; July 17, 2009.
- *On the Number of Graphs with Integral Spectrum.* IPM 20 - Combinatorics 2009, Tehran, Iran; May 16, 2009.
- *On the Number of Graphs with Integral Spectrum.* CSI workshop,UCD, Ireland; November 7, 2008.
- *On the Number of Graphs with Integral Spectrum.* Department of Mathematical Sciences, UCD, Ireland, Algebra Seminar; October 13, 2008.
- *On the Sum-Product Problem on Elliptic Curves.* CNTA 2008, Waterloo, Canada; July 18, 2008.
- *Weight Distribution of Irreducible Polynomials over Finite Fields.* URA Seminar, Department of C&O, University of Waterloo; June 29, 2005.
- *Weight Distribution of Irreducible Polynomials over Finite Fields.* CACR Seminar, University of Waterloo; May 19, 2005.