Ayan Mahalanobis

Academic Background

- **Florida Atlantic University**, Boca Raton, FL
  Ph.D., Mathematical Sciences (GPA 3.83), **2005**
  Dissertation title: Diffie-Hellman key exchange protocol, its generalization and nilpotent groups

- **University of Canterbury**, Christchurch, New Zealand
  Graduate Student, Department of Mathematics and Statistics **1998-2000**

- **University of Calcutta**, Calcutta, India
  M.Sc., Department of Pure Mathematics **1996**

- **University of Calcutta**, Calcutta, India
  B.Sc. with Mathematics Honors, Srirampore College **1994**

Professional experience:

- **Assistant Professor** 2009 - Present
  Division of Mathematical Sciences
  Indian Institute of Science Education and Research Pune
  Dr. Homi Bhabha Road
  Pashan, Pune 411008, INDIA

- **Visiting Assistant Professor** 2005 - 2009
  Department of Mathematical Sciences
  Stevens Institute of Technology
  Hoboken, NJ 07030, U.S.A.

- **Teaching Assistant** 2000 - 2005
  Department of Mathematical Sciences
  Florida Atlantic University
  Boca Raton, FL 33431

- **Teaching Assistant** 1999 - 2000
  University of Canterbury
  Christchurch, New Zealand

Teaching experience:

Undergraduate: Calculus, the whole calculus sequence. Linear Algebra, Real Analysis, Cryptography, Probability & Statistics, Graph Theory and Algorithms.
Graduate: Algebra, both courses in the core algebra curriculum in the Ph.D. program of Stevens Institute and cryptography.

Editorial work:

Member of the editorial board:
International Mathematical Forum.

Research experience:
Cryptography, public key cryptography, finite group theory, finite p-groups, elliptic curve discrete logarithm problem, pairing based cryptosystems.

M. S. Students:
Jay Shah, M.S. IISER Pune 2012
Rahul Kumar, M.S. IISER Pune 2012
Hardik Gajera, M.S. IISER Pune 2013
Preeti, M.S. IISER Pune 2015
Krishna Hariram, M.S. IISER Pune 2015
Upendra Kapshikar, M.S. IISER Pune 2018 (Best Thesis Award)

Ph. D. Students
Pralhad Shinde, Ph. D. IISER Pune 2018
Prabhat Kushwaha, Ph. D. IISER Pune 2017

Languages: C++, HTML, LaTeX, Maple, GAP and Magma.

Operating systems: Linux, FreeBSD, MacOS X, Windows

Visiting appointments:

Visiting Scientist June & July 2006
Applied Statistics Unit
Indian Statistical Institute, Kolkata India

Academic Visitor June 2007
Centre for Interdisciplinary Research in Computational Algebra
University of St Andrews, Scotland

Publications:

- Ansari Abdullah, Ayan Mahalanobis and Vivek M. Mallick, Initial minors – a conjecture to solve the elliptic curve discrete logarithm problem, arXiv preprint, `arxiv.org/abs/2005.05039`, 2020.
- Sushil Bhunia, Ayan Mahalanobis, Pralhad Shinde and Anupam Singh, Algorithms in linear algebraic groups, Advances in applied Clifford algebras (30), 2020.
- Upendra Kapshikar, Ayan Mahalanobis, The Niederreiter cryptosystem and Quasi-Cyclic codes, arxiv preprint, `https://arxiv.org/abs/1911.00661`, 2019.
- Sushil Bhunia, Ayan Mahalanobis, Pralhad Shinde and Anupam Singh, The MOR Cryptosystem in Classical Groups with a Gaussian Elimination Algorithm for Symplectic and Orthogonal Groups, Book Chapter, Modern Cryptography - Theory, Technology, Adaptation and Integration, IntechOpen, 2019.
- Kapshikar Upendra and Mahalanobis Ayan, A Quantum-Secure Niederreiter Cryptosystem using Quasi-Cyclic Codes, Proceedings of the 15th International Joint Conference on e-Business and Telecommunications - Volume 1: SECRYPT, 506-513, 2018 `https://arxiv.org/abs/1803.07827`
- Mahalanobis Ayan, Mallick Vivek and Ansari Abdullah, A Las Vegas algorithm to solve the elliptic curve discrete logarithm problem, In Proceedings of Progress in Cryptology – INDOCRYPT 2018, LNCS, vol 11356, 215-227.
- Kushwaha Prabhat and Mahalanobis Ayan, A probabilistic baby-step giant-step algorithm, In Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT, pages 401-406

- Mahalanobis Ayan and Shinde Pralhad, Bilinear Cryptography Using Groups of Nilpotency Class 2. In: O'Neill M. (eds) Cryptography and Coding. IMACC 2017. Lecture Notes in Computer Science, vol 10655
- Sushil Bhunia, Ayan Mahalanobis, Pralhad Shinde and Anupam Singh Gaussian Elimination in Symplectic and orthogonal groups (unpublished) `http://arxiv.org/abs/1504.03794`
- Mahalanobis, Ayan and Singh Anupam Gaussian elimination in unitary groups with an application to cryptography, Journal of algebra combinatorics discrete structures and applications 4(3) 247-260, 2017
- Bhunia Sushil, Mahalanobis Ayan, Shinde Pralhad and Singh Anupam The MOR Cryptosystem in orthogonal and symplectic groups in odd characteristic, Proceedings of the 8^{th} workshop on current trends in cryptology, CTCrypt'19, Svetlogorsk, Kaliningrad region, Russia, June 4-7, 2019.
- Ansari Abdullah, Hardik Gajera and Ayan Mahalanobis On improvements of the r-adding walk in a finite field of characteristic 2, Journal of Discrete Mathematical Sciences and Cryptography 19(1) 13-38, 2016.
- Mahalanobis, Ayan The MOR cryptosystem and finite p-groups, Contemporary Mathematics Vol. 633, 81-95, 2015.
- Mahalanobis, Ayan and Shah, Jay A new guess-and-determine attack on the A5/1 stream cipher, Computer and Information Science Vol. 7, No. 1; 2014.
- Mahalanobis, Ayan Are matrices useful in public-key cryptography? International Mathematical Forum Vol. 8, no. 39, 1939-1953, 2013.
- Mahalanobis, Ayan The MOR cryptosystem and extra-special p-groups, Journal of Discrete Mathematical Sciences and Cryptography Vol. 18, No. 3, 201-208, 2015.
- Mahalanobis, Ayan The automorphism group of the group of unitriangular matrices over a field, International Journal of Algebra, Vol. 7, no. 15, 723-733; 2013.
- Mahalanobis, Ayan The discrete logarithm problem in the group of non-singular circulant matrices, Groups-Complexity-Cryptology 2(2010), 83-89.
- Mahalanobis, Ayan A simple generalization of the ElGamal cryptosystem to non-abelian groups II Communications in Algebra 40(9)2012 3583-3596.
- Mahalanobis, Ayan A note on using finite non-abelian p-groups in the MOR cryptosystem `http://arxiv.org/abs/cs/0702095` (unpublished).
- Mahalanobis, Ayan A simple generalization of the ElGamal cryptosystem to non-abelian groups, Communications in Algebra 36(10), 2008, 3878-3889.
- Mahalanobis, Ayan Abelian Groups, Homomorphisms and Central Automorphisms of Nilpotent Groups. JP Jour. Algebra, Number Theory & Appl. 7(1), 2007, 69-81
- Mahalanobis, Ayan The Diffie-Hellman key exchange and non-abelian nilpotent groups. Israel Journal of mathematics, 165, 2008, 161-187
- Mullin, Ronald; Mahalanobis, Ayan An alternate representation of finite fields, Utilitas Mathematica 67, 2005, 305-318.

- Mullin, Ronald; Mahalanobis, Ayan Dickson Bases and Finite Fields. Technical Report CORR 2005-04, Center for Applied Cryptographic Research, University of Waterloo.
- Bridges, Douglas; Mahalanobis, Ayan Bounded variation implies regulated: a constructive proof. J. Symbolic Logic 66, 2001, no. 4, 1695-1700.
- Bridges, Douglas; Mahalanobis, Ayan Increasing, nondecreasing, and virtually continuous functions. J. Autom. Lang. Comb. Vol. 6, 2001, no. 2, 139-143.
- Bridges, Douglas; Mahalanobis, Ayan Sequential continuity of functions in constructive analysis. Math. Log. Q. 46, 2000, no. 1, 139-143.

Some selected presentations:

- An alternate representation of finite fields in joint MAA-AMS Meeting, Phoenix, January 7-10 2004.
- The MOR cryptosystem, Graduate center, City University of New York, NY, March 23 2007.
- A MOR cryptosystem built on UT$(d, \mathbf{F})$, Groups Actions Computations 2010, Harish-Chandra Research Institute, Allahabad September 10-12, 2010.
- The MOR cryptosystem and extra-special p-groups, The 5th De Brún workshop, NUI Galway, Ireland, 11 April-16 April 2011.
- The MOR cryptosystem and extra-special p-groups, Finite groups and their automorphisms, Bogzici University, Istanbul, June 07-11, 2011.
- The discrete logarithm problem in semisimple group algebras, The 83$^{\text{rd}}$ Workshop on General Algebra & the 27$^{\text{th}}$ Conference of Young Algebraists, Novi Sad, Serbia, March 15-18, 2012
- The MOR cryptosystem and finite p-groups, Eighteen coast combinatorics conference, February 18-21 2013 Kailua-Kona, HI USA
- Invited speaker, Annual conference of the Ramanujan Mathematical Society, 23-27 June 2014 IISER Pune.
- Finite p-groups in cryptography, GAGTA8, July 21-25 2014, Newcastle, Australia
- Row-column operations in classical groups, in 4^{th} Alterman conference on computational and geometric algebra, 08-13 July 2019, Manipal Institute of Technology, Manipal, India.

Some awards and recognition:

1998 Waikato University, Hamilton, New Zealand, Doctoral scholarship.
2000 University of Canterbury, Christchurch, New Zealand, University of Canterbury doctoral Scholarship (declined).
2001 Florida Atlantic University, travel grant, organized and distributed by the Graduate Student Association.
2003 Florida Atlantic University, travel grant, organized and distributed by the Graduate Student Association.
2006 Indian Statistical Institute, summer support for the months of June and July 2006.
2007 Stevens Institute of Technology, travel grant, visit to Scotland, June 2006.
2007 University of St Andrews, travel grant, visit to Scotland, June 2006.
2010 NBHM Research grant for three years.
2011 NBHM Travel grant for travel to Istanbul.
2012 Awarded a certificate in recognition for his excellent service to the institute, IISER Pune
2013 DST travel grant to attend Groups St Andrews 2013, 3-11 August 2013.
2014 PI for a SERB research grant for three years(along with A. Singh and B. Balasubramanian).
2015 NBHM research grant for three years.

2019 SERB Matrix grant for three years.

Professional affiliations:

American Mathematical Society.
International Association for Cryptographic Research.

Outreach programs:

- The Ramanujan Mathematical Society Under-Graduate Teacher enrichment workshop on finite group theory and applications 7-9 February 2014, Deshbandhu College, Kalkaji, New Delhi.
- Department of Science and Technology sponsored INSPIRE science camp in HNB Garhwal University, Srinagar, Uttarkhand, June 2011.